Intelligence Community Technical Specification

Text and XML Data Encoding Specifications for Intelligence Community Identifier

Version 1

10 April 2013

Table of Contents

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This document contains two Data Encoding Specifications for Intelligence Community Identifier. The first,*Text Data Encoding Specification for Intelligence Community Identifier* (IC-ID.Text) defines detailed implementation guidance for textual identifiers to be used with a variety of text-based encodings. The second, *XML Data Encoding Specification for Intelligence Community Identifier* (IC-ID.XML), defines how to incorporate those identifiers into XML structures.

1.2 - Scope

This specification is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This Data Encoding Specification (DES) may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the DES 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* [4] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA).
- Lead the IC's identification, development, and management of IC enterprise standards.
- 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 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 ICS 500-21,[8] the extensive and consistent use of Extensible Markup Language (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.

A DES specifies how to implement the abstract data elements in the IC.ADD in a particular physical encoding (e.g., data or file format). For example:

- DESs for textual markup formats, such as Extensible Markup Language (XML) and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.
- DESs for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.
- DESs for application-specific formats, for e.g. Microsoft Word, define document properties; styles; fields; cardinalities; processing requirements; and use.

1.4 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on unique identifiers in shared intelligence. A structured, verifiable representation of unique identifiers to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions today being performed by human beings.

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.

1.4.1 - IC-ID.Text

- IC Information Technology Enterprise (IC ITE)
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[2]
- 500 Series:
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[5]

1.4.2 - IC-ID.XML;

- IC Information Technology Enterprise (IC ITE)
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[2]
- 500 Series:
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[5]

1.5 - Audience and Applicability

DESs are primarily intended to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described.

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*,[7] 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.[9] 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 Data Encoding Specification, and are normative or informative as indicated in the dependencies table.

Table 1 - Dependencies

Name	Dependency Description
Augmented Backus–Naur Form (ABNF[1]) defined by Internet Standard 68 also known as RFC 5234.	The text specification uses ABNF to define the format of the IC Identifier text string. Conformance to the structure defined with ABNF is normative, whereas use of ABNF to encode them is informative.

Name	Dependency Description
ISO Schematron[12] implementation by Rick Jelliffe (2010-04-14)	The XML specification uses Schematron to encode IC business rules for this specification. Conformance to the logic of the business rules is normative, whereas use of the schematron language to encode them is informative.

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.

The ABNF rules used to specify the format of an IC-ID are normative, the corresponding textual descriptions are informative. The remainder of this document is normative. Additionally, the use of keywords defined in IETF RFC 2119[9] is considered normative within the scope of the sentence.

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.

Chapter 2 - Development Guidance

Section 2.1 below is the entirety of IC-ID.Text which defines IC Identifiers independently of any particular technology and/or implementation. The remainder of this document is specification of IC-ID.XML.

2.1 - IC-ID.Text

2.1.1 - Overview

IC Identifiers as specified in this document are based on the GUIDE (Globally Unique Identifiers for Everything) project of the Central Intelligence Agency. For background information on GUIDE see http://intellipedia.intelink.ic.gov/wiki/GUIDE . This specification defines the structure and format for globally unique identifiers for all kinds of resources. Registration and resolution of these identifiers to locations (typically with a URL) and retrieval (subject to access controls) is typically handled by a service. While this specification makes numerous references to such a service, this specification is not intended to fully describe, nor is dependent on such a service. IC Identifiers are typically assigned to resources that are permanent and published, such as intelligence reports and other products. In contrast to common temporal URLs that can change over time and become invalid (i.e., dead links), properly maintained IC Identifiers will always refer to the resource no matter where it is stored, or subsequently moved, within the enterprise.

2.1.2 - Deployment & Usage

- IC Identifiers MUST remain completely UNCLASSIFIED so they can be used on any network, classified or unclassified.

The following MAY be modified by the ESB i.e., from a SHOULD to a MUST:

- References to resources (in other web pages, folders, comments, citations, etc.) should be encoded as IC-IDs.

- IC-IDs SHOULD be routinely assigned to every resource, as early in the resource’s life-cycle as possible.

- All content-creating applications assign IC-IDs to products. Downstream applications check for the existence of an IC-ID, and assign one if not found. Assign IC-IDs to legacy resources as needed.

- IC-IDs MAY be assigned to resources other than documents and digital media, e.g., people.

- Commercial data providers to the IC MAY assign IC-IDs to content.

- Creation and assignment of an IC-ID to a resource is independent of registration in an IC-ID Service.

- IC-IDs are the preferred method of identifying and retrieving resources; e.g., IC-IDs SHOULD be returned in search results.

2.1.3 - IC-ID Format and Lexicon

While this specification is useful in and of itself, the intended use is for IC Identifiers to be incorporated into other specifications. This is the primary reason this specification defines IC-IDs by use of formal language known as Augmented Backus-Naur format (ABNF) See http://en.wikipedia.org/wiki/Augmented_Backus-Naur_Form . The following ABNF rules explicitly define the content of an IC Identifier. ABNF is used to provide a formal description independent of any particular technology.

IC-ID Format

```
[1]          IC-ID ::= IC-IDscheme"://" IC-IDprefix "/" IC-IDsuffix
[2]  IC-IDscheme ::= "guide"
[3]    IC-IDprefix ::= 1*16DIGIT
[4]     IC-IDsuffix ::= 1*36(ALPHA / DIGIT / "_" / "-" / ".")
```

IC-ID Lexicon

The following vocabulary helps explain the meaning of terms used in IC-ID documentation.

IC-ID (Canonical IC-ID)

A globally unique identifier, comprised of three parts: the IC-ID Scheme, a IC-ID Prefix and a IC-ID Suffix, e.g., "guide://42/1c3". The identifier is opaque to a user, meaning that there is no embedded, encoded, or inherent meaning in a IC-ID, and by itself must remain completely UNCLASSIFIED. Once created, an IC-ID UID is immutable; both the Prefix and Suffix can never be changed. There is no theoretical limit to the size (length) of the IC-ID Prefix or Suffix, however, in order to avoid potential issues with practical software implementation and to support interoperability needs, maximum lengths have been established for prefixes and suffixes.

IC-ID scheme

IC-IDs are intended to be processed using existing URI processing techniques. To facilitate such we created an unregistered URI scheme of "guide".

IC Identifier Prefix

A positive integer (base 10), e.g., "42". Prefixes are centrally controlled and assigned by the IC-ID Prefix Governance process to "owner" agencies, programs, or projects. IC-ID Prefixes from 0 to 999 and 9000 to 999 are reserved for future use. Prefixes 999000 to 999999 are reserved for testing purposes and can be assigned to any project needing them. A prefix is limited to a maximum length of 16 digits. As the prefix is an integer, leading zeros are not permitted.

IC Identifier Suffix

An alphanumeric string, e.g., "1c3". Allowed characters include A-Z, a-z, 0-9, underscore, hyphen, and period. Length is restricted to 36 characters. Suffixes must be unique within a given Prefix. Suffix generation is the responsibility of the client. For IC usage, it is recommended that clients generate UUID (RFC 4122[10] Type 1, or ITU-T Rec. X.667 | ISO/IEC 9834-8) Suffixes. Other techniques may be used but note that some may inadvertently result in randomly generated words, which could include offensive language. There must not be embedded meaning in a Suffix.

2.1.4 - IC-ID Governance

2.1.4.1 - Prefix Governance

- Prefixes are centrally managed by the IC-ID project team.
- Prefixes are generally assigned to participating IC agencies in blocks.
- Clients must not begin using IC-ID Prefixes until formally approved and registered by the IC-ID project team.
- Some Prefixes are reserved for special purposes within the IC-ID service:
  - The range 0-999 is reserved for IC-ID internal uses.
  - The range 9000-9999 is reserved for future uses.
  - The range 999000-999999 is reserved for testing uses. This means that "real" data should never be assigned IC-IDs in this range.
- To request a Prefix, send an email to the IC-ID project team. See http://intellipedia.intelink.ic.gov/GUIDE#.28U.29 POCs [http://intellipedia.intelink.ic.gov/GUIDE#.28U.29%20POCs] for contact details.

2.1.4.2 - Suffix Governance

In general, there is no central governance on IC-ID Suffixes, as it is the responsibility of the client to generate the Suffix. Suffixes are generated by the client and MUST be unique within a Prefix.

For more guidance, see the IC Identifier Suffix definition in the IC-ID Lexicon

2.2 - IC-ID.XML Development Guidance

The following sections and the next chapter are the documentation of the XML encoding of IC Identifiers.

2.3 - Relationship to Abstract Data Definition and other encodings

The relationship of the XML structures defined in this DES to the abstract terms defined in the IC.ADD are described using a mapping table in the IC.ADD. The mapping tables generally show the mapping to the DES where a structure is defined, not where it is used. These mappings are provided for reference only. The complete set of DES artifacts, both normative and informative, should be consulted in order to gain a complete understanding of this DES.

The mappings in the IC.ADD provide a starting point for the development of automated transformations between formats defined by the DESs. However, it should be noted that when these transformations are used between formats with different levels of detail, there might be some data loss.

2.4 - Additional guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations for which there is not clearly a single method of encoding the data are documented here. 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.

There are two ways in which a consumer requiring a IC-ID can use the IC-ID XML specification: through referencing objects defined in the schema or enforcing the format via running schematron.

2.4.1 - Usage of the IC-ID Schema

The IC-ID.XML schema defines an element (Identifier) and an attribute (identifier) that enforces the IC-ID format as defined in Section 2.1.3 - IC-ID Format and Lexicon . Consumers of the IC-ID.XML specification should import the IC-ID schema and reference the element or attribute, depending on what is needed. Note: the names for the element and the attribute are similar because the content is the same, i.e., both contain an IC-ID, but the expectation on usage is that the consumer would use one or the other. The difference in capitalization is because they follow the IC naming standards, which requires the first letter for elements to be uppercase and the first letter for attributes to be lower case.

2.4.2 - Usage of the IC-ID Schematron Library

The IC-ID.XML schematron library contains an abstract rule that enforces the IC-ID format as defined in Section 2.1.3 - IC-ID Format and Lexicon . Consumers of the IC-ID.XML specification should include the abstract rule and define an implementation for it. This allows for the consumer to define the context that triggers the rule and the value that should be matched against the IC-ID format.

Note that consumers of the IC-ID.XML schematron library also need to import the IC-ID schema within their schema. The importing schema needs to reference the DES Version for IC-ID in order to let systems reviewing the data know what schematron library to import.

Chapter 3 - Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for IC-ID.XML. They provide additional restrictions (i.e., constraints) on how the data should be structured and encoded, especially for criteria that exceed the constraints implemented in the XML Schema. These rules are written in plain English phrases; however, knowledge of the IC-ID.XML schemas is required to understand the rules. Complex constraint rules may be followed by text labeled *Human Readable*. This text is intended to inform the intent of the more formal language above it. Implementers are intended to implement the formal language, and should there be a perception of conflict, bring it to the attention of the appropriate configuration control body to be resolved.

3.1 - Basics

The IC-ID.XML schema defines the data elements, attributes, cardinalities and parent-child relationships for which Text instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified by IC elements and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints. The constraints can largely be derived from interpreting the intent of the current schemas and/or extracting guidance from the Development Guidance or the policy or guidance documents that govern that type of data.

3.1.1 - Schematron

Schematron[12] was selected as the language in which to encode these additional rules. The provided Schematron[12] is used to define the constraint rules; it is NOT a required implementation. Implementers can use any tools at their disposal as long as the data complies with the rules expressed. To facilitate testing and understanding of the rules they are executable in either *oXygen®* [11] or the XML Stylesheet Language for Transformation (XSLT) 2.0[15] implementation of International Organization for Standardization (ISO) Schematron[12] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[14] and XSLT 2.0[15] features. According to Mr. Jelliffe, the editor of Schematron[12] for ISO:

> "By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this."

Included in the package are the ISO Schematron[12] implementation and XSLT 2.0[15] files provided as a convenience along with a compiled version of the rules.

3.1.2 - “Living” Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a starter set and do not attempt to address the full scope tradecraft and business rules addressed by multiple policy drivers including Sourcing Requirements for Disseminated Intelligence Products as defined by ICD 206.[3] These rules will be expanded and modified as the model matures, and as applicable documentation and tradecraft policies change.

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

3.1.3 - Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the DES artifacts wherever they are located.

3.1.4 - Terminology

For the purposes of this document, the following statements apply:

- The term “is specified” indicates that an attribute is applied to an element and the attribute has a non-null value.
- The term “must be specified” indicates that an attribute must be applied to an element and the attribute must have a non-null value.
- The term “is not specified” indicates that an attribute is not applied to an element, or an attribute is applied to an element and the attribute has a null value.
- The term “must not be specified” indicates that an attribute must not be applied to an element.

3.1.5 - Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are “for official use only” (FOUO). IDs from 20001 to 30000 are reserved for “Secret” rules and 30001 and above for more classified rules. IC-ID.XML data validation constraint rule IDs are prefixed with “IC-ID-ID-”.

As the constraint rules are managed over time, IDs from deleted rules will not be reused.

3.1.6 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning.” An “Error” is more severe and is indicative of a clear violation of a constraint rule, which would be likely to have a significant impact on the quality of a document. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

Each system responsible for processing a document (e.g., create, modify, transform, or exchange) must make a mission-appropriate decision about using a document with errors or warnings based on mission needs.

3.1.7 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content — which allows for empty (or null) content. According to this specification, all required elements (and certain conditional elements) must have content, other than white space. [1] Elements, which are allowed to only have text content, must have text content specified.

3.2 - Inherited Constraints

In an instance of IC-ID.XML, the use of attributes and elements from supplementary data encoding specifications must be fully conformant with the constraint rules defined in those specifications. For a full list of supplementary specifications, see Section 1.7 - Dependencies .

3.3 - Additional Constraints

3.3.1 - DES Constraints

The DES version is specified as an attribute in the IC-ID schema and constrains the allowed value. Consumers of the IC-ID should reference the IC-ID DES Version attribute at the root element of the importing schema. The **DESVersion** attribute enables systems processing an instance document to be certain which set of constraint rules, schema, CVEs and business rules are intended by the author to be used.

3.4 - Constraint Rules

The detailed constraint rules for the IC-ID.XML schema can be found in a separate document inside the SchematronGuide directory, in the IC-ID_Rules.pdf file. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron. Obsolete rule numbers are listed in the SchematronGuide.

[1] "white space" is defined in XML 1.0[13] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

Appendix A Feature Summary

The following tables summarize major features by version for IC-ID.

Table 2 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can't comply)
Cell Colors represent the same information as the Key value	

A.1. IC-ID Text Feature Summary

Table 3 - IC-ID Text Feature comparison

IC-ID Text Feature Comparison		
Required date	Feature	V1
	ABNF description of Identifier	F

A.2. IC-ID XML Feature Summary

Table 4 - IC-ID XML Feature comparison

IC-ID XML Feature Comparison		
Required date	Feature	V1
	Schema Element support	F
	Schema Attribute support	F
	Schematron support	F

Appendix B Change History

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

Table 5 - DES Version Identifier History

Version	Date	Purpose
1.0	February 2013	Initial Release

Appendix C Acronyms

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

Table 6 - Acronyms

Name	Definition
A&A	Authorization and Accreditation
ABAC	Attribute Based Access Control
ABNF	Augmented Backus-Naur Form
ADD	Abstract Data Definition
API	Applications Programming Interface
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BBOX	Bounding Box
BNF	Backus-Naur Form
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
CMS	Cryptographic Message Syntax
COMET	Completely Open Mapping Environment
CONOPS	Concept of Operations
CORBA	Common Object Request Broker Architecture
CQL	Common Catalog Query Language (CQL)
CRL	Certificate Revocation List
CSW	Catalog Service for Web
CVE	Controlled Vocabulary Enumeration
D & R	Discovery and Retrieval
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DIA	Defense Intelligence Agency

Name	Definition
DISR	DoD Information Technology Standards and Profile Registry
DNS	Domain Name System
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
EBNF	Extended Backus-Naur Form
EDH	Enterprise Data Header
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
EPR	Endpoint Reference
FOUO	For Official Use Only
FTP	File Transfer Protocol
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

Name	Definition
ICSR	Intelligence Community Standards Registry
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
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
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
LIMDIS	Limited Distribution
LNI	Library of National Intelligence
MAC	Multi Audience Collection
MCG&GIL	Mapping, Charting, and Geodesy Information Library
MCGView	Mapping, Charting, and Geodesy View
MIME	Multipurpose Internet Mail Extensions
MTOM	Message Transmission Optimization Mechanism
NARA	National Archives and Records Administration
NCES	Net-Centric Enterprise Services
NGA	National Geospatial Intelligence Agency
NGDS	Net-Centric GEOINT Discovery Services
NGT	Next Generation Trident

Name	Definition
NIPR	Non-Classified Internet Protocol Router Network
NITF	National Imagery Transmission Format
NPE	Non-Person Entity
NRO	National Reconnaisance Office
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
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
SIPR	Secret Internet Protocol Router Network
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSD	Special Security Directorate
SSL	Secure Sockets Layer
STIL	Saint Louis Information Library

Name	Definition
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
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
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] ABNF

Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.
Available online at: http://tools.ietf.org/html/std68
Also known as: http://www.ietf.org/rfc/rfc5234.txt

[2] 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 JWICS at: http://go.ic.gov/HvBHBmY

[3] ICD 206

Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Intelligence Products*. Intelligence Community Directive 206. 17 October 2007.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_206.pdf

[4] ICD 500

Director of National Intelligence Chief Information Officer. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[5] ICD 501

Director of National Intelligence Chief Information Officer. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[6] 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 JWICS at: http://go.ic.gov/fU3HML

[7] 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 IntelLinkU at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[8] 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 IntelLinkU at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[9] 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

[10] IETF-RFC 4122
Internet Engineering Task Force. *A Universally Unique IDentifier (UUID) URN Namespace*. July 2005.
Available online at: http://tools.ietf.org/html/rfc4122

[11] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. version 14.1.
Available online at: http://www.oxygenxml.com/

[12] Schematron
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.
Available online at: http://www.schematron.com/

[13] XML 1.0
World Wide Web Consortium (W3C) . *Extensible Markup Language (XML) 1.0, Second Edition*. W3C, 6 October 2000.
Available online at: http://www.w3.org/TR/2000/REC-xml-20001006

[14] XPath2
World Wide Web Consortium (W3C) . *XML Path Language (XPath) 2.0 (Second Edition)*. W3C Recommendation 14 December 2010 (Link errors corrected 3 January 2011).
Available online at: http://www.w3.org/TR/xpath20/

[15] XSLT2
World Wide Web Consortium (W3C) . *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.
Available online at: http://www.w3.org/TR/xslt20/

Appendix 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: <datastandardssupport@ugov.gov> or
<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.[7]