



Intelligence Community Technical Specification

XML Data Encoding Specification for Electronic Records Management

Version 2016-JUL

July 29, 2016

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	3
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.6.3 - Terminology	3
1.6.4 - XML Namespaces	4
1.7 - Dependencies	4
1.7.1 - Standalone and Convenience Packages	7
1.8 - Conformance	7
1.9 - Version Policies	7
1.9.1 - XML Namespace Policy	7
1.9.2 - Version Numbering	8
Chapter 2 - Development Guidance	10
2.1 - Relationship to Abstract Data Definition and other encodings	10
2.2 - Additional Guidance	10
2.2.1 - Electronic Records Management Usage	10
2.2.2 - ERM Assertion and Trusted Data Objects	11
2.2.3 - ERM Structure	12
2.2.4 - ERM Elements	12
Chapter 3 - Definitions, Interfaces, and Constraints	13
3.1 - Constraint Rule Types	13
3.2 - “Living” Constraint Rules	13
3.3 - Classified or Controlled Constraint Rules	13
3.4 - Constraint Terminology	13
3.5 - Errors and Warnings	14
3.6 - Rule Identifiers	14
3.7 - Data Validation Constraint Rules	14
3.7.1 - Purpose	14
3.7.2 - Schematron	15
3.7.3 - Non-null Constraints	15
3.7.4 - Inherited Constraints	15
3.7.5 - Value Enumeration Constraints	16
3.7.6 - Additional Constraints	16
3.7.6.1 - DES Constraints	16
3.7.7 - Constraint Rules	16
3.8 - Data Rendering Constraint Rules	16
3.8.1 - Purpose	16
3.8.2 - Rendering Constraint Rules	16
Chapter 4 - Conformance Validation	18
4.1 - TDF based instances	18
4.2 - Schema Validation	18

4.3 - Business Rule Validation	18
Chapter 5 - Generated Guides	19
5.1 - Schema Guide	19
5.2 - Schematron Guide	19
Appendix A - Feature Summary	21
A.1 - ERM Feature Summary	21
Appendix B - Change History	22
Appendix C - List of Abbreviations	23
Appendix D - Bibliography	25
Appendix E - Points of Contact	29
Appendix F - IC CIO Approval Memo	30

List of Figures

Figure 1 - Related Specifications 6

Figure 2 - TDO Format Overview 11

List of Tables

Table 1 - XML Namespaces	4
Table 2 - Dependencies	4
Table 3 - Numerical Rule Identifier Ranges	14
Table 4 - Constraint Rules	17
Table 5 - ERM Dependency over time	21
Table 6 - Feature Summary Legend	21
Table 7 - ERM Feature comparison	21
Table 8 - DES Version Identifier History	22

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Electronic Records Management* (ERM.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) for Electronic Records Management data. This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing ERM concepts using XML. ERM is designed as a Trusted Data Format (TDF) assertion, and it provides guidance encoding ERM data within a TDF Object or Collection.

1.2 - Scope

This specification describes the data required for the management of electronic records including the creation, receipt, maintenance, use and disposition of records; and it defines an XML structure to contain ERM data in TDF objects and collections. This specification applies to permanent and temporary records as defined in various federal statutes, regulations, and agency directives including the Federal Records Act of 1950, the Privacy Act, and the Freedom of Information Act.

This specification applies to the Intelligence Community (IC) and information produced, stored, or shared within the IC. This 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. Records management is a subset of information management functions. ERM does not address the information management review, declassification, and release functions. However, there may be some conceptual overlaps, such as FOIA exemptions.

1.3 - Background

The Intelligence Community 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* ^[10] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, 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 Information Technology (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* ^[13] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

A DES defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* ^[2]. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID^[8] defines a plain-text format for IC Identifiers as well as an associated XML structure.

1.4 - Enterprise Need

Electronic Records Management (ERM) is required to control the creation, receipt, maintenance, use and disposition of records in accordance with legislation such as the Federal Records Act, Freedom of Information Act (FOIA), Privacy Act, and Executive Branch direction. This applies to permanent and temporary records. IC ITE Service Providers shall provide the means to audit, track, and manage disposition information, using agreed upon metadata tags that can be adapted to changing missions and records management practices. ERM will help automate the sharing, processing, routing, discovery, and access control of records management information. ERM enables users to quickly discover information related to FOIA and Privacy Act cases and other specialized legal requests, identify documents for mandatory declassification, and respond to other open government initiatives.

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^[6]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[10]
- Memorandums:
 - OMB Memo - Managing Government Records Directive^[18]
 - Presidential Memo - Managing Government Records^[17]
- DoD Issuances:
 - Department of Defense Instruction Number 5015.02.02, DoD Records Management Program^[3]
 - Department of Defense Instruction Number 8310.01, Information Technology Standards in the DoD^[4]
- Federal Regulations:
 - Federal Records Act^[24]
 - Freedom of Information Act^[22]
 - Privacy Act^[23]
 - Federal Community Directive 1^[5]

1.5 - Audience and Applicability

This is a data encoding specification. It defines the structure and related business rules for encoding the described data type. A DES is intended for those developing tools and services that create, modify, store, exchange, search, display, or further process the type of data being described.

The governance of this DES and the data it describes, including any requirement to use this DES or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,^[12] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,^[4] requires DoD elements to use the DoD IT Standards Registry (DISR).

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

1.6 - Conventions

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

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels.”^[14] When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.6.3 - Terminology

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

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

1.6.4 - XML Namespaces

Namespaces referenced in this document and the prefixes used to represent them are listed in the following table. The namespace prefix of any XML Qualified Name used in any example in this document should be interpreted using the information below.

Table 1 - XML Namespaces

Prefix	URI
ism	urn:us:gov:ic:ism
erm	urn:us:gov:ic:erm
xsd	http://www.w3.org/2001/XMLSchema

1.7 - Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 2](#). The dependencies listed below are directly referenced in this specification (e.g. Schema, Schematron), and are normative or informative as indicated.

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the IC CIO specifications related to this specification. The graphic depicts direct and transitive dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all transitive dependencies.

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V3+)</i> ^[9]	ERM elements as well as its dependent specifications are used in conjunction with IC-TDF objects as structured assertions or content that compose the necessary material represented by ERM.XML. The dependence of ERM.XML on IC-TDF is normative. This specification does not depend on a specific version of IC-TDF.XML; IC-TDF.XML version 3 or later MAY be used.

Name	Dependency Description
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V13+) [15]	This specification does not depend on a specific version of Information Security Marking (ISM.XML); ISM.XML version 13 or later MAY be used. The minimum version was based on the earliest non-retired version; ESB 15-2 was used for determining the version.
XML Data Encoding Specification for Enterprise Data Header (IC-EDH XML.V4+) [7]	This specification does not depend on a specific version of Enterprise Data Header (IC-EDH.XML); IC-EDH.XML version 4 or later MAY be used. The minimum version was based on the earliest non-retired version; ESB 15-2 was used for determining the version.
Schematron [20]	Schematron — ISO/IEC 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative. The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. Note: The Schematron rules in this specification use XSLT 2.0 [29] query binding.
XSLT 2.0 [29] implementation of Schematron [20] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

Name	Dependency Description
ISO 15489-1:2001, <i>Information and documentation – Records management – Part 1: General</i>	Standard that defines "records management."

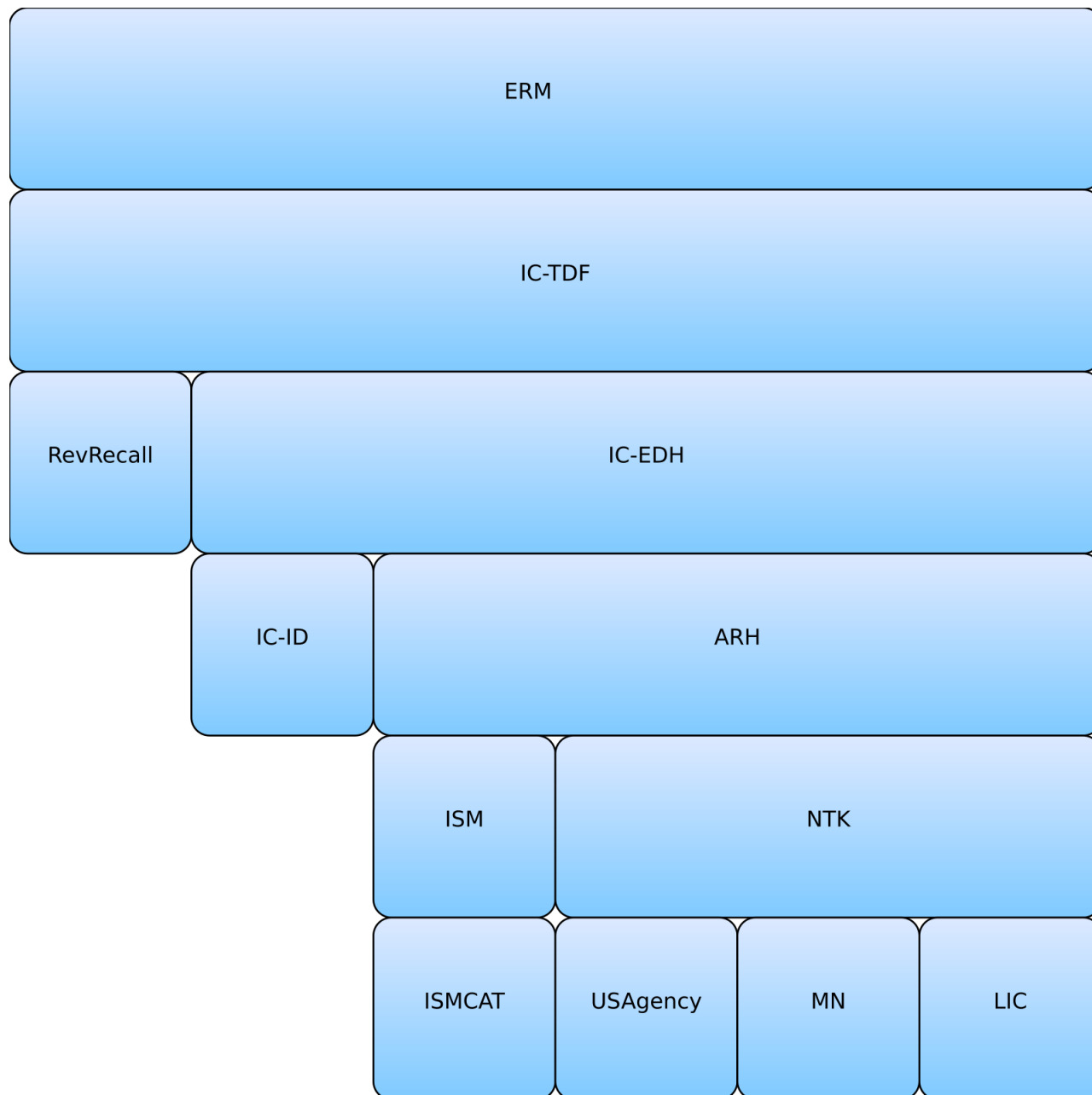


Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions of all transitive dependent specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumerations (CVEs) to validate and operate as intended.

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

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron^[20] rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[14] is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.^[27] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion='9'** to **@ism:DESVersion='10'** in the `xsd:schema` statement. The ability to specify which version of a dependent specification to import enables the configuration change control of parent specifications (such as PUBS and TDF) to be "decoupled" from the configuration change control of dependent specifications (such as ISM CVE updates). This "decoupling" method has not been in place for all versions of these parent specifications; therefore, please verify with the dependency table to ensure use of allowed dependency versions.

Additional guidance that is either classified or has handling controls can be found in separate annexes 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

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from "The

Disposition of Names in an XML Namespace.”^[21] This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 “Versioning and XML namespace policy” of “Architecture of the World Wide Web, Volume One.”^[25]

There is a version attribute (e.g. **@DESVersion**, **@CESVersion**, **@TESVersion**, **@version**) for each namespace defined in an IC CIO specification. Version attributes are used to capture the specification version number the specification author intends an instance to conform to. Namespaces do not change, so the version attribute is required to fully understand an instance document.

As changes to the specification are released, the version number captured in the “version” attribute increments. See [Section 1.9.2 - Version Numbering](#) for information on the numbering scheme.

This XML namespace policy only applies to the namespaces defined in this specification, any namespaces that are included by reference should define their own namespace policy.

1.9.2 - Version Numbering

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-
MMM). This provides a temporal representation of when the specification was released. When the version number is used in the version attribute, the expression follows the Augmented Backus-Naur Form^[1] below:

Version Format when used in the version attribute:

- [1] Version ::= [Year Month](#) ["-" [CustomizationSuffix](#)]
- [2] Year ::= 4(DIGIT)
- [3] Month ::= 2(DIGIT)
- [4] Customization ::= 1*27(ALPHA / DIGIT / "_")
Suffix

Version in XML Lexicon

The following vocabulary helps explain the meaning of terms used in the version documentation, and it may further constrain the set of allowable values:

Version	The version number as it might be expressed in a DESVersion, CESVersion or other XML attribute for indicating the version being referenced.
Year	The four digit year from the version of the specification being referenced.
Month	The 2 digit month from the version of the specification being referenced.

CustomizationSuffix An optional suffix used when customizing a version of a specification. This would be used to indicate that you have extended the specification in some fashion for a particular use case.

Chapter 2 - Development Guidance

2.1 - Relationship to Abstract Data Definition and other encodings

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

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

2.2 - 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.

2.2.1 - Electronic Records Management Usage

ERM.XML is used in conjunction with TDF objects as structured assertions that contain information required for generating a Trusted Data Object (TDO) or Trusted Data Collection (TDC). The TDF.XML specification has a consistent and simple concept of Assertions and Payloads. There are two options for root elements: TDO and TDC. A TDO contains some data (the payload) and some statements about that data (the assertions). In the context of TDF, an 'assertion' is defined as a statement providing handling, discovery, or mission metadata describing a payload, TDO, or TDC depending on the scope of the assertion. Each TDO must contain at least one handling assertion, which provides the minimum information needed to protect the data. Additional discovery and mission assertions may also be provided. A TDC contains a list of TDOs (the payload) and some statements about those TDOs (the assertions). A TDO or TDC conforms to the ERM specification when it contains:

- A structured assertion with an ERM element.
 - The scope of the assertion in the TDC or TDO defines what the ERM metadata applies too. The meaning of the scope is defined in the TDF DES. This means that an ERM assertion may be used to refer to an entire TDC, an entire TDO, or a payload without regard to type of payload.
 - There may be multiple ERM assertions applied to the same data instance. When this is true, all ERM assertions MUST be respected using applicable record control schedule and ownership guidance regarding how to combine the different control schedules.

- A data payload that is a string, a file or other binary data, XML structured content, or reference to the data payload that is not embedded in the TDO but stored in a remote/external location. Linked objects classification does NOT impact the classification of the TDO. Embedded objects classification does impact the classification of the TDO.

The TDO will contain the metacard creation and security metadata for the TDO, an EDH with “payload” scope containing the security metadata for the payload, the ERM Mission Specific metadata, and a payload, which can be either the URL of the resource or the resource itself.

The diagram below shows expected use of IC specifications within a TDO and a ERM-specific metadata assertion. The use of the IC-EDH handling assertion and payload are required.

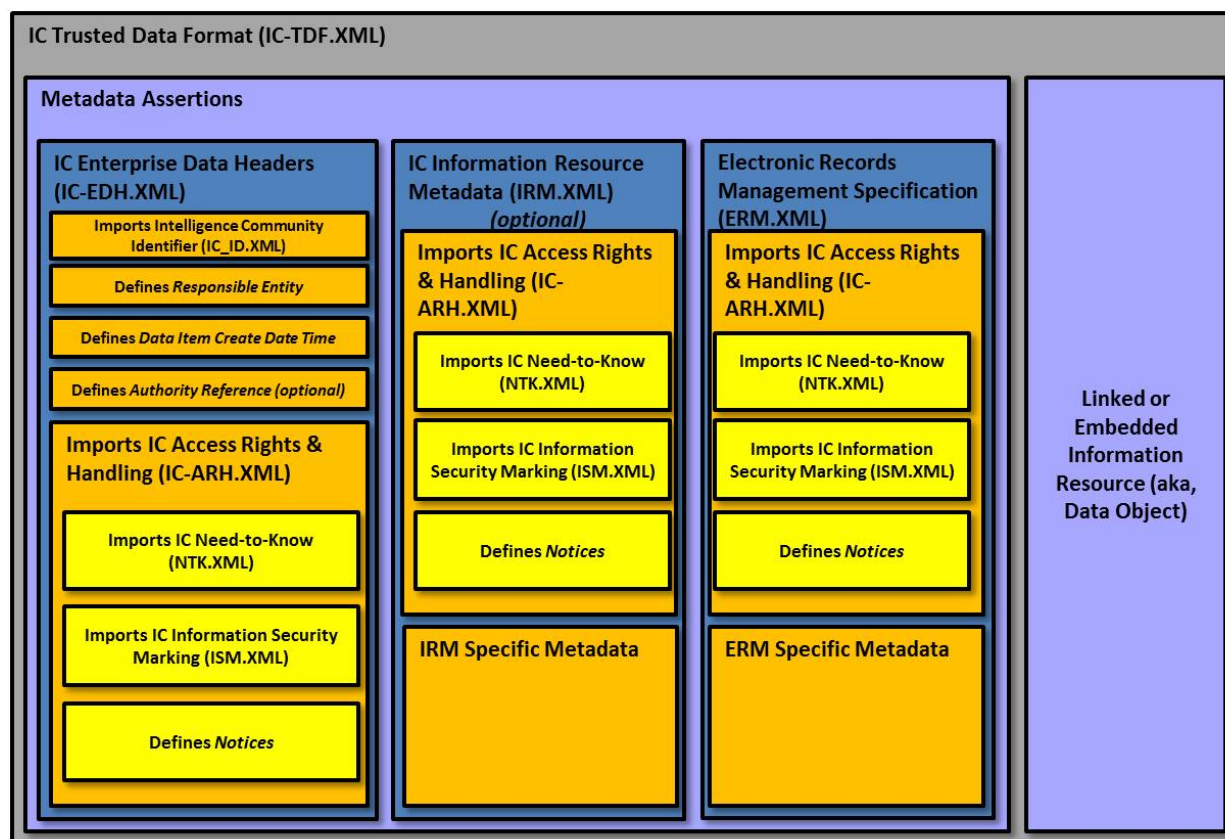


Figure 2 : TDO Format Overview

The EDH Assertion identifies the security, access rights and handling, notices, and need to know information for the TDO and the payload.

2.2.2 - ERM Assertion and Trusted Data Objects

Trusted Data Objects and Trusted Data Collections adhere to the IC Trusted Data Format XML schema, and the ERM metadata is contained in a ERM assertion within the TDO or TDC. The ERM assertion adheres to the ERM.xsd.

2.2.3 - ERM Structure

The ERM specification is composed of pieces of procedural information necessary for the management of records within the IC enterprise. These procedural pieces of information consist of an indicator stating if the record is exempted from FOIA search and publication, information about the disposition of the record, date and time the record is declared final, an indicator if the record is vital, and an office identifier identifying the agency and organization element within the agency that owns, is responsible for, and makes decisions for the record.

2.2.4 - ERM Elements

The ERM consist of five main elements specific to ERM: **FoiaOpsIndicator**, **OfficeOfRecord**, **RecordDesignationDate**, **VitalRecordsIndicator**, and **Disposition**.

- **FoiaOpsIndicator** - Indicator stating if the record is exempted from FOIA search and publication (e. g. operations exemption at CIA); each agency has specific exemptions they request and maintain. Lack of value does not mean “false”, but rather that it is not determined. Per Section 552 of Title 5, United States Code^[22] this should be “false” before it goes into a community shared resource. Does not have access control implementations; it can be discovered, but it cannot be used in a FOIA release.
- **OfficeOfRecord** - Identifies the agency and organization element within the agency that is responsible for making decisions related to the record. Also identifies which organization element within an agency owns or is responsible for the official copy of the record. If this element is reoccurring, then all dependencies need to be reoccurring and will result in multiple instances of ERM.XML. This is a single instance.
- **RecordDesignationDate** - Date that the record is declared final (e. g. cutoff, publication, creation) and starts the retention period which will be used to calculate the disposition date based on the retention schedule.
- **VitalRecordsIndicator** - Indicator stating that the record is a vital record. Vital records are those records considered essential to the continuity of operation during and after emergencies or disaster conditions. They are also known as Essential Records per Federal Continuity Directive 1^[5]. A Null does not imply false.
- **Disposition** - This element and its child elements (**AppliedBy**, **DateApplied**, **DateEligible**, **DateLimit**, **RecordControl**, **ReviewIndicator**, and **Hold**) collectively represent information about the disposition of the record.

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body for resolution. Rendering constraint rules define constraints on the display and rendering of documents. While expressed in a similar manner to the data validation constraint rules, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

3.2 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of records management business rules addressed by authoritative guidance. These rules will be expanded and modified as the model matures, tradecraft changes, and as applicable 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.

3.3 - 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 encoding specification artifacts wherever they are located.

3.4 - Constraint 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.

3.5 - 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.

3.6 - Rule Identifiers

Each constraint rule has an assigned rule identifier, indicated in brackets preceding the constraint rule description. ERM.XML data validation constraint rule identifiers are prefixed with “ERM-ID-” and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in [Section 3.6 - Rule Identifiers \[14\]](#). As the constraint rules are managed over time, IDs from deleted rules will not be reused.

Table 3 - Numerical Rule Identifier Ranges

Rule Identifier Range		Description
Start	End	
00001	09999	Reserved for Unclassified constraint rules
10001	19999	Reserved for Unclassified but For Official Use Only (FOUO) constraint rules
20001	20999	Reserved for constraint rules classified at the “Secret//REL USA, FVEY” level
21001	21999	Reserved for constraint rules classified at the “Secret//NF” level
22001	29999	Reserved for constraint rules classified at the “Secret//TBD” level
30001 and above		Reserved for constraint rules classified with other classifications

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

The ERM.XML schema defines the data elements, attributes, cardinalities and parent-child relationships for which XML 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 in applicable IC policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints.

3.7.2 - Schematron

Schematron^[20] is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document **MUST** meet, exactly as English may be used to convey normative criteria.

It is not necessary for implementers to use the specific Schematron encoding in this specification, and implementers **MAY** use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator **MUST** find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

For better understanding, the Schematron^[20] rules for this specification may be executed in *Oxygen*^[19] or with an XSLT 2.0-compliant processor using the XSLT 2.0^[29] transforms in the Schematron implementation from Rick Jelliffe (see [XSLT 2.0 implementation of Schematron by Rick Jelliffe](#) in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0^[28] and XSLT 2.0^[29] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:^[16]

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.



Note

For convenience, the specification package provides the XSLT 2.0^[29] implementation of Schematron^[20] along with a compiled version of the rules.

3.7.3 - 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, meaning elements can be empty or null. 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.

3.7.4 - Inherited Constraints

In an instance of ERM.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](#).

¹“White space” is defined in XML 1.0^[26] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

3.7.5 - Value Enumeration Constraints

Several elements and attributes of the ERM.XML model use CVEs to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE. Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

Some CVEs are not available on all networks. A subset CVE will be provided for use on networks not approved for the entire list. If the processing will occur on a network where the entire CVE is not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

As noted in the specific rules, a failure of validation against a CVE will generate an Error.

3.7.6 - Additional Constraints

3.7.6.1 - DES Constraints

The DES version is specified through attributes on the root element. The schema constrains the values of these attributes. 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.

3.7.7 - Constraint Rules

The detailed constraint rules for the ERM.XML schema can be found in a separate document inside the SchematronGuide directory, in the ERM_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.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of ERM.XML documents. The intent is to inform the development of systems capable of rendering or displaying ERM.XML data for use by individuals not familiar with the details of the ERM.XML markup. While expressed in a similar manner to the data validation constraint rules above, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

3.8.2 - Rendering Constraint Rules

The following table contains the information for the ERM.XML data rendering constraint rules.

Table 4 - Constraint Rules

Rule Number	Severity	Description	Human Readable Description
There are no Data Rendering Constraint rules at this time.			

Chapter 4 - Conformance Validation

An instance document conforms with this specification if it passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

4.1 - TDF based instances

An instance document that is based on TDF MUST use the TDF validation strategy.

- ERM Schema validation MUST be done in TDF validation step 2. Performing schema validation in TDF validation step 1 MAY not show invalid to the schema errors.
- ERM Schematron validation MUST be done in TDF validation step 1 and MUST NOT be done in TDF validation step 2. Performing ERM Schematron validation in TDF validation step 2 MAY cause inaccurate validation errors.
- TDF validation steps 3 and 4 have no ERM unique requirements.

4.2 - Schema Validation

An instance document MUST comply with the schemas for this specification and this specification's dependencies, and schema validation SHOULD occur prior to other validation steps. If schema validation fails, results from later steps may be indeterminate.

4.3 - Business Rule Validation

An instance document MUST comply with the business rules expressed in this specification. The business rules in this specification are expressed in Schematron, but it is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid if and only if the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

Chapter 5 - Generated Guides

5.1 - Schema Guide

The guide was generated using *oXygen® XML Editor*, [\[19\]](#), a commercially available product produced by SyncRO Soft.

The guide provides an interactive index to:

- Global Elements and Attributes
- Local Elements and Attributes
- Simple and Complex Types
- Groups and Attribute Groups
- Referenced Schemas

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of the master HTML file *SchemaGuide.html* with supporting graphics.

5.2 - Schematron Guide

The detailed description and reference documentation for the ERM.XML Schematron rules can be found in a separate document named *ERM_Rules.pdf*, which is located inside the

SchematronGuide directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Appendix A Feature Summary

The following table shows the version dependencies for ERM on other DES.

Table 5 - ERM Dependency over time

Dependent DES	V2016-JUL
IC-TDF	V3+
ISM	V13+
IC-EDH	V4+

The following table summarizes major features by version for this specification.

Table 6 - 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. ERM Feature Summary

Table 7 - ERM Feature comparison

ERM Feature Comparison		
Required date	Feature	V2016-JUL
	FOIA indication	F
	Record hold information	F
	Record disposition information	F
	Vital record indication	F

Appendix B Change History

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

Table 8 - DES Version Identifier History

Version	Date	Purpose
2016-JUL	29 July 2016	Initial Release

Appendix C List of Abbreviations

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

ADD	Abstract Data Definition
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EDH	Enterprise Data Header
ERM	Electronic Records Management
ESB	Enterprise Standards Baseline
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ISO	International Organization for Standardization
IT	Information Technology
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PUBS	Intelligence Publications

RFC	Request for Comments
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
URL	Uniform Resource Locator
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL 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] ADD

Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/soSC6M8>

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

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

[3] DoD Instruction 5015.02

DoD Chief Information Officer. *DoD Records Management Program*. 5015.02. 24 February 2015.

Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf>

[4] DoD Instruction 8310.01

DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.

Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf>

[5] FCD

Department of Homeland Security. *Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements*. October 2012.

Available online at: <http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf>

[6] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.

Available online Intelink-TS at: <http://go.ic.gov/4X6TOc1>

[7] IC-EDH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Data Header (IC-EDH.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/TQjVx3d>

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

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

[8] IC-ID.XML

Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/mQ4IUDk>

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

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

[9] IC-TDF.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (TDF.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/sonBSai>

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

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

[10] ICD 500

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

Available online Intelink-TS at: <http://go.ic.gov/5Ot5sbK>

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[11] ICPG 710.1

Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online Intelink-TS at: <http://go.ic.gov/0d147Ee>

Available online at: <http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf>

[12] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <http://go.ic.gov/sLKNq3N>

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[13] 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-TS at: <http://go.ic.gov/cWYv9nw>

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-21>

[14] 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>

[15] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/3oipfOY>

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

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

[16] Jelliffe

Richard Alan Jelliffe. *FAQ*. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?.

Available online at: <http://www.schematron.com>

[17] Managing Government Records

Presidential Memorandum - Managing Government Records.

Available online at: <https://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records>

[18] OMB Memo M-12-18

Managing Government Records Directive.

Available online at: <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf>

[19] Oxygen

SyncRO Soft. *<oXygen/> XML Editor.*

Available online at: <http://www.oxygenxml.com/>

[20] Schematron

International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron.* ISO/IEC 19757-3:2006.

ISO Spec Available online at: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

StyleSheets for compiling Available online at: <http://code.google.com/p/schematron/>

[21] TAG-9-Jan-2006

W3C Technical Architecture Group (TAG). *The Disposition of Names in an XML Namespace.* 9 January 2006.

Available online at: <http://www.w3.org/2001/tag/doc/namespaceState.html>

[22] USCodeT5-S552

US Code Title 5 Section 552: Public information; agency rules, opinions, orders, records, and proceedings. 25-43.

Available online at: <https://www.gpo.gov/fdsys/pkg/USCODE-2014-title5/pdf/USCODE-2014-title5-partI-chap5-subchapII-sec552.pdf>

[23] USCodeT5-S552a

US Code Title 5 Section 552a: Records Maintained on Individuals. 25-43.

Available online at: <https://www.gpo.gov/fdsys/pkg/USCODE-2014-title5/pdf/USCODE-2014-title5-partI-chap5-subchapII-sec552a.pdf>

[24] USCodeT44-C31

US Code Title 44 Chapter 31: Records Management By Federal Agencies. 97-100.

Available online at: <https://www.gpo.gov/fdsys/pkg/USCODE-2014-title44/pdf/USCODE-2014-title44-chap31.pdf> [<https://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap31.pdf>]

[25] WEBARCH-15-Dec-2004

W3C. *Architecture of the World Wide Web, Volume One.* 15 December 2004.

Available online at: <http://www.w3.org/TR/webarch>

[26] 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>

[27] XML Catalogs

The Organization for the Advancement of Structured Information Standards [OASIS]. *XML Catalogs*. Committee Specification 06 Aug 2001.

Available online at:<https://www.oasis-open.org/committees/entity/spec-2001-08-06.html>

[28] 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/>

[29] 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 the following DNI-sponsored web sites.

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

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

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

E-mail: ic-standards-support@ugov.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.^[12]