



Intelligence Community Technical Specification

XML Data Encoding Specification for Revision Recall

Version 2014-DEC

December 22, 2014

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	8
1.9 - Version Policies	8
1.9.1 - XML Namespace Policy	8
1.9.2 - Version Numbering	9
Chapter 2 - Development Guidance	10
2.1 - Relationship to Abstract Data Definition and other encodings	10
2.2 - Additional Guidance	10
2.2.1 - Trusted Data Format Handling Assertion	10
2.2.2 - Assertion Resource Level Markings	10
2.3 - Revision/Recall Actions	11
2.3.1 - PURGE	11
2.3.2 - RETAIN_WARN	11
2.3.3 - RETAIN_HIDE	11
2.3.4 - MANUAL_INSTRUCTION	11
Chapter 3 - Definitions, Interfaces, and Constraints	12
3.1 - Constraint Rule Types	12
3.2 - "Living" Constraint Rules	12
3.3 - Classified or Controlled Constraint Rules	12
3.4 - Terminology	12
3.5 - Errors and Warnings	13
3.6 - Rule Identifiers	13
3.7 - Data Validation Constraint Rules	13
3.7.1 - Purpose	13
3.7.2 - Schematron	13
3.7.3 - Non-null Constraints	14
3.7.4 - Value Enumeration Constraints	14
3.7.5 - Additional Constraints	14
3.7.5.1 - DES Constraints	14
3.7.6 - Constraint Rules	15
3.8 - Data Rendering Constraint Rules	15
3.8.1 - Purpose	15
3.8.2 - Rendering Constraint Rules	15
Chapter 4 - Conformance Validation	16

4.1 - Schema Validation	16
4.2 - Business Rule Validation	16
Chapter 5 - Generated Guides	17
5.1 - Schema Guide	17
5.2 - Schematron Guide	18
Appendix A - Feature Summary	19
A.1 - RevRecall Feature Summary	19
Appendix B - Change History	20
B.1 - V2014-DEC Change Summary	20
Appendix C - List of Abbreviations	22
Appendix D - Bibliography	24
Appendix E - Points of Contact	27
Appendix F - IC CIO Approval Memo	28

List of Figures

Figure 1 - Related Specifications	7
---	---

List of Tables

Table 1 - XML Namepaces	4
Table 2 - Dependencies	4
Table 3 - Constraint Rules	15
Table 4 - RevRecall Dependency over time	19
Table 5 - Feature Summary Legend	19
Table 6 - RevRecall Feature Comparison	19
Table 7 - DES Version Identifier History	20
Table 8 - Data Encoding Specification 2014-DEC Change Summary	20

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Revision Recall* (RevRecall.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode RevRecall 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 RevRecall data concepts using XML.

The specification expresses information related to the revision and recall of intelligence products. This information allows recipients to be aware of revisions and recalls and to take necessary actions in regards to previous versions.

1.2 - Scope

This specification is applicable to the Intelligence Community (IC) and information produced by, 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.

This specification is intended to meet the requirements put forth in the Memorandum for Distribution signed by Negroponte on August 5, 2005. This includes declaring the title or subject of the intelligence product being revised or recalled, type of revision or recall, the date the revision or recall was issued, the reason for its issuance, and any required actions to be taken as a result of its issuance.

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* ^[5] 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 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* ^[9] 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.

An encoding specification defines how to implement the abstract data elements in the IC Abstract Data Definition (ADD) in a particular physical encoding (e.g., data or file format). For example:

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

1.4 - Enterprise Need

Information sharing within the national intelligence enterprise is becoming increasingly reliant on machine processable and interpretable data to allow control and facilitate automated exchanges, and appropriate protection of shared intelligence. A structured, verifiable representation of revision and recall notices bound 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.

Early in the intelligence life cycle, intelligence producers need:

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

- IC Information Technology Enterprise (IC ITE):
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[3]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[5]
 - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC^[6]
- Memorandums:
 - ES 05-1963 - IC Standards and Procedures for Revised or Recalled Intel Products - (5 August 2005)^[13]

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*, [8] 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.

1.6.1 - Language

The keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this technical specification are to be interpreted as described in the IETF RFC 2119.[10] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.6.3 - 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
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
Negroponte Memorandum - Subject: Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products - signed 2005-08-05 ^[13]	Policy Driver
<i>XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V2014-DEC+)</i> ^[4]	RevRecall elements are used in conjunction with TDF collections as handling assertions that indicate how objects in a trusted data collection are related. The dependence of RevRecall on TDF is normative. Any TDF version 2014-DEC or above may be used with RevRecall v2014-DEC.

Name	Dependency Description
<p><i>XML Data Encoding Specification for Information Security Markings</i> (ISM.XML.V9+) [11]</p>	<p>RevRecall elements are used in conjunction with ISM collections as structured assertions that indicate how objects in a trusted data collection are related. The dependence of RevRecall on ISM is normative. Any ISM version 9 or above may be used with RevRecall v2014-DEC.</p>
<p><i>XML Data Encoding Specification for Access Rights and Handling</i> (ARH.XML.V1+) [2]</p>	<p>RevRecall elements are used in conjunction with ARH collections as structured assertions that indicate how objects in a trusted data collection are related. The dependence of RevRecall on ARH is normative. Any ARH version 1 or above may be used with RevRecall v2014-DEC.</p>
<p>Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations (CVEs) included in this DES.</p>	<p>Specification uses CVEs to encode controlled vocabularies. The use of the RevRecall CVEs is normative.</p>
<p>Schematron [15]</p>	<p>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.</p> <p>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.</p> <p>Note: The Schematron rules in this specification use XSLT 2.0 [21] query binding.</p>

Name	Dependency Description
<p>XSLT 2.0^[21] implementation of Schematron^[15] by Rick Jelliffe (2010-04-14)</p> <p>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/.</p>	<p>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.</p> <p>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.</p>

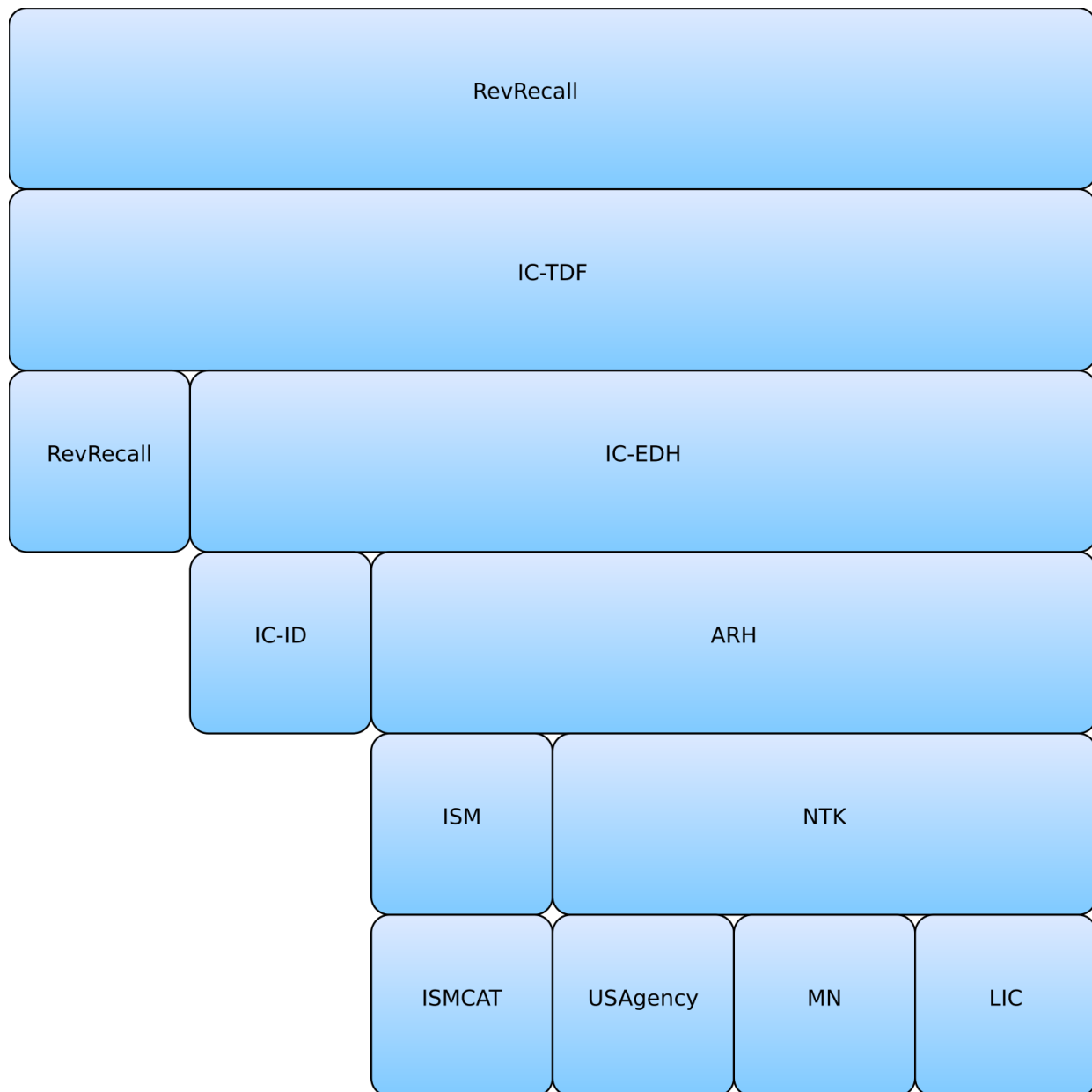


Figure 1 : Related Specifications

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 CVE 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

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.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron^[15] 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 HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[10] 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.^[19] 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 import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications such as ISM CVE updates. The decoupling of dependency versions is not retroactive; see the dependency table for 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."^[16] 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."^[17]

In a fashion similar to DocBook there is a “version” attribute (i.e., **@DESVersion**, **@CESVersion**, **@version**) defined in each namespace defined in an IC CIO specification used to capture the version number assigned to each revision of the specification. The **@DESVersion** attribute is the only indicator in an instance document as to what revision of a particular specification the author intended the instance to be valid to. Since the namespace does not change, the “version” attribute is required to fully understand the 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 - Trusted Data Format Handling Assertion

This specification is intended to be used as a handling assertion in a Trusted Data Format (TDF) which prevents the assertion from being encrypted. An instance of RevRecall is intended only to be transmitted within an instance of the TDF. The TDF structure is comprised of a data object, or payload, and the metadata describing it, or assertions. As the payload and each assertion can be optionally encrypted, TDFs have a special type of required assertion, called HandlingAssertions, that indicate the access and protection mechanisms that systems must implement to process the TDF's contents. RevRecall metadata is carried inside the TDF as a HandlingAssertion; therefore, systems processing TDFs must understand and be able to act upon Revision/Recalls that enter their system.

The revision or recall denoted in an instance of this specification refers to the payload object of the TDF that contains the RevRecall instance.

2.2.2 - Assertion Resource Level Markings

The **arh:Security** element in the Revision/Recall assertion is used to contain the resource level markings of the Revision/Recall assertion itself. Specifically, it is where the roll-up of all portions in the Revision/Recall assertion is presented. It is also where any need-to-know metadata would be placed if needed for the assertion. To ensure the proper treatment of the security and handling markings within the assertion, the **ism:resourceElement** MUST be set to true on the **arh:Security** element.

However, this assertion is not a standalone object and **MUST** live within a TDF. The resource level markings of the Revision/Recall assertion contribute to and will be reflected in the EDH within the **tdf:HandlingAssertion** with scope of [TDO] or [TDC] depending if the assertion is contained in a **tdf:TrustedDataObject** or directly within a **tdf:TrustedDataCollection**.

2.3 - Revision/Recall Actions

This section describes the actions that can be taken for a revision or recall. For additional information about the different types of revisions or recalls, please reference the *Negroponte Memorandum, Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products*. ^[13]

2.3.1 - PURGE

When the PURGE value is used for the **@action** attribute, all copies of the product and associated indexes, that have been revised or recalled, **MUST** be immediately removed and destroyed. This includes archived copies and indexes of the revised or recalled product. All recipients of the product **MUST** be notified of the purge action.

2.3.2 - RETAIN_WARN

When the RETAIN_WARN value is used for the **@action** attribute, the existing copies of the revision of the product **MUST** be retained and also indicated that they are not the latest revision. All recipients of the product **MUST** be notified that a newer version of the product is available.

2.3.3 - RETAIN_HIDE

When the RETAIN_HIDE value is used for the **@action** attribute, the existing copies of the revision of the product **MUST** be retained and access and distribution **MUST** be prevented. All recipients of the product **MUST** be notified not to disseminate the product.

2.3.4 - MANUAL_INSTRUCTION

When the MANUAL_INSTRUCTION value is used for the **@action** attribute, the action to be taken requires manual intervention by a human to read and follow the included instructions. The **ActionInstruction** element **MUST** be populated with the specific instructions for a human to perform. All recipients of the product **MUST** be notified, immediately after the product is revised or recalled, of the action that was performed.

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 business rules addressed by authoritative guidance. These rules will be expanded and modified as the model matures, and as applicable security marking 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 - 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 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. RevRecall.XML data validation constraint rule IDs are prefixed with “RevRecall-ID-”.

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

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

The RevRecall.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^[15] 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^[15] rules for this specification may be executed in *Oxygen*^[14] or with an XSLT 2.0^[21]-compliant processor using the XSLT 2.0^[21] 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^[20] and XSLT 2.0^[21] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:^[12]

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^[21] implementation of Schematron^[15] 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 - Value Enumeration Constraints

Several elements and attributes of the RevRecall.XML model use Controlled Vocabulary Enumerations (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.

3.7.5 - Additional Constraints

3.7.5.1 - 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

¹“White space” is defined in XML 1.0^[18] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

document to be certain which set of constraint rules, schema, CVEs and business rules are intended by the author to be used.

3.7.6 - Constraint Rules

The detailed constraint rules for the RevRecall.XML schema can be found in a separate document inside the SchematronGuide directory, in the RevRecall_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 RevRecall.XML documents. The intent is to inform the development of systems capable of rendering or displaying RevRecall.XML data for use by individuals not familiar with the details of the RevRecall.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 RevRecall.XML data rendering constraint rules.

Table 3 - 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 - 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.

4.2 - 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 detailed description and reference documentation for the RevRecall.XML schema can be found as a collection of HTML files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the RevRecall.XML schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen@*, [\[14\]](#) 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 RevRecall.XML Schematron rules can be found in a separate document named *RevRecall_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 RevRecall on other DESs.

Table 4 - RevRecall Dependency over time

Dependent DES	V1	V2014-DEC
IC-TDF	V1+	V2014-DEC+
ISM	V9+	V9+
ARH	N/A	V1+

The following table summarizes major features by version for RevRecall and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. For those changes driven by the IC Markings System Register and Manual, the date is often one year after the date of publication. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

Table 5 - 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. RevRecall Feature Summary

Table 6 - RevRecall Feature Comparison

RevRecall Feature Comparison			
Required date	Feature	V1	2014-DEC
	Specify type of a revision/recall	F	F
	Specify the title or subject of the intelligence product being revised/recalled	F	F
	Specify the date and time of a revision/recall	F	F
	Specify the reason for a revision/recall	F	F
	Specify an action to be taken as a result of a revision/recall	F	F
	Specify a POC for a revision/recall	F	F

Appendix B Change History

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

Table 7 - DES Version Identifier History

Version	Date	Purpose
1	14 March 2014	Initial Release
2014-DEC	4 December 2014	Routine revision to technical specification. For details of changes, see Section B.1 - V2014-DEC Change Summary .

B.1 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Promoting Revision Recall to a HandlingAssertion to enforce understanding.

The following table summarizes the changes made to V1 in developing 2014-DEC.

Table 8 - Data Encoding Specification 2014-DEC Change Summary

Change	Artifacts changed	Compatibility Notes
Deleted rule RevRecall-ID-00002.	RevRecall-ID-00002 removed	Deletion of this rule does not change compatibility since this rule was duplicative of schema validation. Deleting the rule from data generation and ingestion systems will eliminate a Saxon warning.
Context of rule RevRecall-ID-00003 updated to use element instead of attribute (CR-2014-006).	RevRecall-ID-00003 updated.	Data generation and Ingestion systems need to be updated to incorporate this rule.
Regular expression restriction removed from @DESVersion since the restriction is not applicable with the new versioning scheme. Changed @DESVersion to represent the year and month of release. Also allowed for extension of specification by adding a '-' followed by a string to denote a custom implementation.	DES Schema	Data generation and Ingestion systems need to be updated to incorporate the new schema.

Change	Artifacts changed	Compatibility Notes
Added rule RevRecall-ID-00006 to enforce restriction that a Revision Recall assertion may not have Revision Recall assertion siblings (CR-2014-020).	RevRecall-ID-00006 added.	Data generation and Ingestion systems need to be updated to incorporate this rule.
Revision Recall assertion changed from tdf:Assertion to tdf:HandlingAssertion. Requires an arh:Security element.	Schema	Data generation and Ingestion systems need to be updated to incorporate the new schema.
Schematron rules added to enforce rules for tdf:HandlingAssertion.	Schematron RevRecall-ID-00007 RevRecall-ID-00008 RevRecall-ID-00009	Data generation and Ingestion systems need to be updated to incorporate the new rules.

Appendix C List of Abbreviations

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

ADD	Abstract Data Definition
ARH	Access Rights and Handling
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EDH	Enterprise Data Header
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
ISOO	Information Security Oversight Office
IT	Information Technology
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PDF	Portable Document Format
PUBS	Intelligence Publications

RFC	Request for Comments
TDF	Trusted Data Format
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] ARH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*. Available online Intelink-TS at: <http://go.ic.gov/Fub6Gnw>
Available online Intelink-U at: <http://purl.org/IC/Standards/ARH>
Available online at: <http://purl.org/IC/Standards/public>

[3] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012. Available online Intelink-TS at: <http://go.ic.gov/HvBHBmY>

[4] IC-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: <http://purl.org/IC/Standards/TDF>
Available online at: <http://purl.org/IC/Standards/public>

[5] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008. Available online Intelink-TS at: <http://go.ic.gov/enm8L9x>
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[6] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009. Available online Intelink-TS at: <http://go.ic.gov/GG61roi>
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[7] 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/yAqVQ0H>

[8] 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: <http://www.purl.org/ic/standards/policy/ICS500-20>

[9] 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: <http://www.purl.org/ic/standards/policy/ICS500-21>

[10] 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>

[11] 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: <http://purl.org/IC/Standards/ISM>

Available online at: <http://purl.org/IC/Standards/public>

[12] Jelliffe

Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*. <http://www.schematron.com>

[13] Negroponte Memo

Memorandum For Distribution - Subject: Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products. 2005-08-05. John Negroponte.

Available online Intelink-U at: <http://purl.org/ic/standards/policy/revrecall>

[14] Oxygen

SyncRO Soft. *<oXygen/> XML Editor*. Version 14.1.

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

[15] 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/>

[16] 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>

[17] 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>

[18] 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>

[19] 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>

[20] 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/>

[21] 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: ic-standards-support@ugov.gov [mailto: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.^[8]