



Intelligence Community Technical Specification

XML Data Encoding Specification for Revision Recall

Version 2021-NOVr2022-MAY

December 1, 2022

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 - Enterprise Need	1
1.4 - Conventions	2
1.4.1 - XML Namespaces	2
1.5 - Dependencies	2
1.5.1 - Specification Dependencies	2
1.5.2 - Inverse Dependencies	5
Chapter 2 - Development Guidance	6
2.1 - Relationship to Abstract Data Definition and other encodings	6
2.2 - Additional Guidance	6
2.2.1 - Trusted Data Format Handling Assertion	6
2.2.2 - Assertion Resource Level Markings	7
2.3 - Revision/Recall Actions	7
2.3.1 - PURGE	7
2.3.2 - RETAIN_WARN	7
2.3.3 - RETAIN_HIDE	7
2.3.4 - MANUAL_INSTRUCTION	7
Chapter 3 - Constraints	9
3.1 - Data Validation Constraint Rules	9
3.1.1 - Value Enumeration Constraints	9
3.1.2 - Additional Constraints	9
3.1.2.1 - DES Constraints	9
3.1.3 - Constraint Rules	9
3.2 - Data Rendering Constraint Rules	10
3.2.1 - Purpose	10
3.2.2 - Rendering Constraint Rules	10
Appendix A - Feature Summary	11
A.1 - RevRecall Feature Summary	11
A.1.1 - Features from V2014-DEC to V2021-NOVr2022-MAY	11
A.1.2 - Features from V1 to V2014-DEC	11
Appendix B - Change History	12
B.1 - V2021-NOVr2022-MAY Change Summary	12
B.2 - V2021-NOV Change Summary	12
B.3 - V2014-DECr2018-APR Change Summary	13
B.4 - V2014-DEC Change Summary	15
Appendix C - List of Abbreviations	17
Appendix D - Bibliography	18
Appendix E - Points of Contact	20
Appendix F - IC CIO Approval Memo	21

List of Figures

Figure 1 - Related Specifications 4
Figure 2 - Inverse Dependency Specifications 5

List of Tables

Table 1 - XML Namepaces	2
Table 2 - Dependencies	3
Table 3 - Constraint Rules	10
Table 4 - Feature Summary Legend	11
Table 5 - RevRecall Feature comparison V2014-DEC to V2021-NOVr2022-MAY	11
Table 6 - RevRecall Feature comparison V1 to V2014-DEC	11
Table 7 - DES Version Identifier History	12
Table 8 - Data Encoding Specification 2021-NOVr2022-MAY Change Summary	12
Table 9 - Data Encoding Specification 2021-NOV Change Summary	13
Table 10 - Data Encoding Specification 2014-DECr2018-APR Change Summary	14
Table 11 - Data Encoding Specification 2014-DEC Change Summary	16

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.XML 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.XML 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

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[3]) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (IC) technical specifications. For convenience, a copy of this framework is included in every package.

This specification is applicable to the 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 Intelligence Community Policy Memorandum (ICPM) 200-1, *Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products* ^[8] which supersedes the Memorandum for Distribution signed by Negroponete on August 5, 2005 of the same name (Negroponete Memo^[11]). 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 - 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.

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 200 Series:
 - ICPM 200-01, *Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products* ^[8]

- 500 Series:
 - Intelligence Community Directive (ICD) 500, *Director Of National Intelligence Chief Information Officer* [\[5\]](#)
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* [\[6\]](#)
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [\[9\]](#)

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the “Specification Conventions” chapter in the IC-SF.XML[\[3\]](#).

1.4.1 - 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 Namepaces

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

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML[\[3\]](#).

1.5.1 - Specification 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 Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts 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 IC CIO specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

In the related specifications figure, [Figure 1](#), SOME-TDF is not an actual specification but a placeholder in the diagram that represents the fact that this specification depends on some

Trusted Data Format (TDF) specification in its usage as an assertion in a Trusted Data Object (TDO).

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V2019-MAR+)</i> ^[4]	REVRECALL.XML elements, as well as its dependent specifications, are used in conjunction with IC-TDF.XML ^[4] objects as structured assertions or content that compose the necessary material represented by REVRECALL.XML. The dependence of REVRECALL.XML on IC-TDF.XML ^[4] is normative. This specification does not depend on a specific version of IC-TDF.XML ^[4] ; versions later than version 2019-MAR MAY be used. The minimum version was based on the earliest non-retired version; Enterprise Standards Baseline (ESB) 22-1 was used for determining the version.
<i>XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V2021-NOVr2022-NOV+)</i> ^[10]	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[10] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[7] . Per ICD-710, all security markings MUST be updated within 365 days of a release of the Register and Manual. As of this release, the latest version of ISM.XML is 2021-NOVr2022-NOV which is based on the Register and Manual released in August, 2019.
<i>Intelligence Community Specification Framework (IC-SF.XML.V2021-NOV+)</i> ^[3]	This specification does not depend on a specific version of IC-SF.XML ^[3] ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.

Name	Dependency Description
<p>Schematron^[12]</p>	<p>Schematron — International Organization for Standardization (ISO)/International Electrotechnical Commission (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 Transformations (XSLT) 2.0^[13] query binding.</p>
<p>XSLT 2.0^[13] implementation of Schematron^[12] 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 Uniform Resource Locator (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>

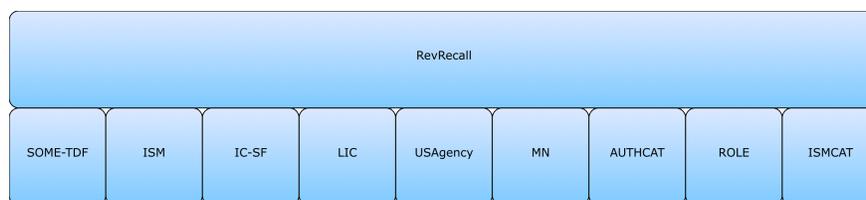


Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

Generally, it is only necessary to think of the *dependencies* in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies*, for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies (specifications that uses the given specification).

Since this specification is one such specification that is used by other specifications released by the IC CIO, the [Figure 2](#) has been included to assist readers in understanding all of the inverse dependency relationships and how changes in this given specification may impact others specifications. This diagram is representative of direct and transitive inverse dependencies at the time of the release of this specification, but are subject to change over time and is presented in a list format that is different than [Figure 1](#).

For specifications that are used as assertions by some TDF specification, the inverse dependency specification diagram, [Figure 2](#), will only show the TDF specifications that are typically used with this specification and will not show all TDF specifications that can use it.



Figure 2 : Inverse Dependency Specifications

Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML^[3] framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

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 Abstract Data Definition (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 *XML Data Encoding Specification for Trusted Data Format* (IC-TDF.XML)^[4] which prevents the assertion from being encrypted. An instance of REVRECALL.XML is intended only to be transmitted within an instance of the IC-TDF.XML^[4]. The IC-TDF.XML^[4] 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, IC-TDF.XML^[4] has a special type of required assertion, called HandlingAssertion, that indicates the access and protection mechanisms that systems must implement to process the IC-TDF.XML^[4] contents. REVRECALL.XML metadata is carried inside IC-TDF.XML^[4] as a HandlingAssertion; therefore, systems processing IC-TDF.XML^[4] instances 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 IC-TDF.XML^[4] document that contains the REVRECALL.XML instance. For a revision the payload will be the modified body, whether narrative, media, or reference to an external payload. For a recall the payload should contain what the author desires the end-customer to see if end-customer has bookmarked or becomes aware of the existence of the information object through some other means. The recall payload could be a short description of what or why the information object was

recalled, a boilerplate notice, or a reference to an external object that the object was recalled, all using organizationally agreed upon presentations.

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 an IC-TDF.XML^[4]. The resource level markings of the Revision/Recall assertion contribute to and will be reflected in the IC-EDH.XML^[2] enterprise data header within the `tdf:HandlingAssertion` with scope of TDO or Trusted Data Collection (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 ICPM 200-01^[8].

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.

MAY meet FISA-Compliance Recall guidance depending on your agencies legal council.

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.

MAY meet FISA-Compliance Recall guidance depending on your agencies legal council.

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.

MAY meet FISA-Compliance Recall guidance depending on your agencies legal council.

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

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. For more information, please see the “Data Validation Constraint Rules” chapter in the IC-SF.XML^[3] framework document.

3.1.1 - Value Enumeration Constraints

Several elements and attributes of the REVRECALL.XML model use Controlled Vocabulary Enumeration (CVE)s 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.

3.1.2 - Additional Constraints

3.1.2.1 - 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.

3.1.3 - Constraint Rules

The detailed constraint rules for the REVRECALL.XML schema can be found in a separate document inside the Documents/REVRECALL 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 “REVRECALL_Rules.pdf” file.

3.2 - Data Rendering Constraint Rules

3.2.1 - 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.

3.2.2 - 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.			

Appendix A Feature Summary

The following tables summarize major features by version for REVRECALL.XML. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g., The IC Markings^[1] has an implementation date of one year after issuance).

Table 4 - 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

A.1.1. Features from V2014-DEC to V2021-NOVr2022-MAY

Table 5 - RevRecall Feature comparison V2014-DEC to V2021-NOVr2022-MAY

Required date	Feature	V2014-DEC	V2014-DECr2018-APR	V2021-NOV	V2021-NOVr2022-MAY
	Scope rule to improve streaming validation	N	F	F	F
	Support rule consistency of timezone usage on dateTime	N	F	F	F
	Support for FISA-Compliance Recall	N	N	F	F

A.1.2. Features from V1 to V2014-DEC

Table 6 - RevRecall Feature comparison V1 to V2014-DEC

Required date	Feature	V1	V2014-DEC
---------------	---------	----	-----------

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	March 14, 2014	Initial Release
2014-DEC	December 4, 2014	Routine revision to technical specification. For details of changes, see Section B.4 - V2014-DEC Change Summary .
2014-DECr2018-APR	April 20, 2018	Routine revision to technical specification. For details of changes, see Section B.3 - V2014-DECr2018-APR Change Summary .
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see Section B.2 - V2021-NOV Change Summary .
2021-NOVr2022-MAY	May 13, 2022	Routine revision to technical specification. For details of changes, see Section B.1 - V2021-NOVr2022-MAY Change Summary .

B.1 - V2021-NOVr2022-MAY Change Summary

Significant drivers for Version 2021-NOVr2022-MAY include:

- Community Change Requests

[Table 8](#) summarizes the changes made to 2021-NOV in developing 2021-NOVr2022-MAY.

Table 8 - Data Encoding Specification 2021-NOVr2022-MAY Change Summary

#	Change	Artifacts Changed	Compatibility Notes
1	Fix bug in RevRecall schematron. (CR-2022-010)	Documentation Schematron RevRecall-ID-00010 modified	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Add specVersion attribute to all CVEs. (CR-2022-014)	CVEs	Data generation and ingestion systems need to be updated to accommodate the changes.

B.2 - V2021-NOV Change Summary

Significant drivers for Version 2021-NOV include:

- Community Change Requests
- Alignment with ICPM 200-01

[Table 9](#) summarizes the changes made to 2014-DECr2018-APR in developing 2021-NOV.

Table 9 - Data Encoding Specification 2021-NOV Change Summary

#	Change	Artifacts Changed	Compatibility Notes
1	Updated documentation to use the specification framework. (CR-2019-040)	Documentation	No impact to systems.
2	Update Dependency table to point to the appropriate law or policy for ISM. (CR-2019-158)	Documentation	No impact to systems.
3	To align with ICPM 200-01 ^[8] which supersedes the Memorandum for Distribution signed by Negroponte on August 5, 2005 of the same name (Negroponte Memo ^[11]), updated the definition for Administrative Recall and added FISA-Compliance Recall Type. (CR-2020-051)	Documentation CVE CVEnumRevRecallType modified Schema Schematron RevRecall-ID-00012 added RevRecall_XML modified	Data generation and ingestion systems need to be updated to accommodate the changes.
4	Identify the root node in the Schema Guide. (CR-2019-126)	Documentation	No impact to systems.
5	Added DESVersion warning enforcement rules (CR-2021-001)	Schematron RevRecall-ID-00013 added	No impact to systems.

B.3 - V2014-DECr2018-APR Change Summary

Significant drivers for Version 2014-DECr2018-APR include:

- Community Change Requests

[Table 10](#) summarizes the changes made to V2014-DEC in developing 2014-DECr2018-APR.

Table 10 - Data Encoding Specification 2014-DECr2018-APR Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated RevRecall-ID-00006 to be more friendly for streaming implementations. (CR-2015-026)	Schematron RevRecall-ID-00006 modified	Data generation and ingestion systems need to be updated to enforce the modified rule.
2	Added @ism:DESVersion value. (CR-2016-052)	Schema	Data generation and ingestion systems need to be updated to accommodate the changes.
3	The schema change logs will no longer be maintained as of the 2014-DECr2018-APR release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2014-DECr2018-APR, reference the change history in the DES.	Schema	No impact to systems.
4	Create RelaxNG CVE Fragments for RevRecall. (CR-2017-186)	CVEs	No impact to systems.
5	Timezone information required for dateTime. (CR-2017-165)	Schema Schematron RevRecall-ID-00010 added REVRECALL.XML.sch modified	Systems need to be updated to enforce the new restriction.
6	Added DESVersion warning enforcement rule and updated schema version restriction to be more generic. (CR-2017-094)	Schema Schematron RevRecall-ID-00011 added RevRecall_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes.
7	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-123, CR-2017-278)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
8	Updated @ism:DESVersion and version value. (CR-2016-051,CR-2016-052)	Schema	Data generation and ingestion systems need to be updated to accommodate the changes.
9	Updated the Dependency Over Time table with the appropriate specs. (CR-2017-282)	Documentation	No impact to systems.
10	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-257)	Documentation	No impact to systems.
11	Update prose to align with current specifications. Change e-mail address to ic-standards-support@iarpa.gov. (CR-2017-285)	Documentation	No impact to systems.
12	Create JSON version of CVEs in RevRecall (CR-2017-067)	CVEs	No impact to systems.
13	Create CSV version of CVEs in RevRecall (CR-2017-045)	CVEs	No impact to systems.
14	Added schema PDF. (CR-2018-032)	Documentation	No impact to systems.
15	Added ISM.XML ^[10] attributes to Schematron files to mark up the documentation. (CR-2017-315)	Schematron	No impact to systems.
16	Added @id and @role to all sch:rule elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-232)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
17	Updated CSV generation to include a column for deprecation date information. (CR-2018-091)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.

B.4 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Promoting Revision Recall to a HandlingAssertion to enforce understanding.

[Table 11](#) summarizes the changes made to V1 in developing 2014-DEC.

Table 11 - Data Encoding Specification 2014-DEC Change Summary

#	Change	Artifacts changed
1	Deleted rule RevRecall-ID-00002.	RevRecall-ID-00002 removed
2	Context of rule RevRecall-ID-00003 updated to use element instead of attribute (CR-2014-006).	RevRecall-ID-00003 updated.
3	Regular expression restriction removed from @DESVersion since the restriction is not applicable with the new versioning scheme. @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
4	Added rule RevRecall-ID-00006 to enforce restriction that a Revision Recall assertion may not have Revision Recall assertion siblings per Change Request #80.	RevRecall-ID-00006 added.
5	Revision Recall assertion changed from tdf:Assertion to tdf:HandlingAssertion. Requires an arh:Security element.	Schema
6	Schematron rules added to enforce rules for tdf:HandlingAssertion.	Schematron RevRecall-ID-00007 RevRecall-ID-00008 RevRecall-ID-00009

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
ESB	Enterprise Standards Baseline
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

[1] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. Available online Intelink-TS at: <https://go.ic.gov/tGXkwGO> (case sensitive – tango Golf Xray kilo whiskey Golf Oscar) Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[2] 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: <https://go.ic.gov/5Pg1r8s> (case sensitive – 5 Papa golf 1 romeo 8 sierra) Available online Intelink-U at: <https://w3id.org/ic/standards/EDH> Available online at: <https://w3id.org/ic/standards/public>

[3] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*. Available online Intelink-TS at: <https://go.ic.gov/pNFyuVg> (case sensitive – papa November Foxtrot yankee uniform Victor golf) Available online Intelink-U at: <https://w3id.org/ic/standards/IC-SF> Available online at: <https://w3id.org/ic/standards/public>

[4] IC-TDF.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML)*. Available online Intelink-TS at: <https://go.ic.gov/hdwc8fn> (case sensitive – hotel delta whiskey charlie 8 foxtrot november) Available online Intelink-U at: <https://w3id.org/ic/standards/TDF> Available online at: <https://w3id.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: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima) 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: <https://go.ic.gov/FTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra) Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[7] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.
Available online Intelink-TS at: <https://go.ic.gov/oSj9K7O> (case sensitive – oscar Sierra juliet 9 Kilo 7 Oscar)
Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[8] ICPM 200-01

Office of the Director of National Intelligence. *Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products*. Intelligence Community Policy Memorandum 2020-200-01. 27 February 2020.
Available online at: https://www.dni.gov/files/documents/ICPM_2020_200-01_U-FOUO_SIGNED-FINAL_Redacted.pdf

[9] 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: <https://go.ic.gov/kh8NMVJ> (case sensitive – kilo hotel 8 November Mike Victor Juliet)
Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[10] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.
Available online Intelink-TS at: <https://go.ic.gov/qoNICy7> (case sensitive – quebec oscar November India Charlie yankee 7)
Available online Intelink-U at: <https://w3id.org/ic/standards/ISM>
Available online at: <https://w3id.org/ic/standards/public>

[11] NegroponTE Memo

Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products. 2005-08-05. John NegroponTE.
Available online Intelink-U at: <https://w3id.org/ic/standards/policy/revrecall>
Available online Intelink-TS at: <https://go.ic.gov/3YUdWbl> (case sensitive – 3 Yankee Uniform delta Whiskey bravo India)

[12] Schematron

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

[13] 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 Director of National Intelligence (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@odni.gov.

Appendix F IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO 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 IC CIO staffing and coordination process leading to signature of the IC CIO Approval Memo. The signature date of the IC CIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the IC CIO 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 Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20^[9].