



Intelligence Community Technical Specification

XML Data Encoding Specification for Virtual Coverage

Version 2020-OCTr2022-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	7
2.1 - Relationship to Abstract Data Definition and other encodings	7
2.2 - Additional Guidance	7
2.2.1 - Usage of ISM	7
Chapter 3 - Constraints	8
3.1 - Data Validation Constraint Rules	8
3.1.1 - Purpose	8
3.1.2 - Inherited Constraints	8
3.1.3 - Value Enumeration Constraints	8
3.1.4 - Additional Constraints	8
3.1.4.1 - DES Constraints	8
3.1.5 - Constraint Rules	8
3.2 - Data Rendering Constraint Rules	9
3.2.1 - Purpose	9
3.2.2 - Rendering Constraint Rules	9
Appendix A - Feature Summary	10
A.1 - VIRT Feature Comparison	10
A.1.1 - Features from V2015-AUG to V2020-OCTr2022-MAY	10
A.1.1.1 - Features Partial and N/A from V2015-AUG to V2020-OCTr2022-MAY	10
A.1.2 - Features from V1 to V2015-AUG	11
A.1.2.1 - Features Partial and N/A from V1 to V2015-AUG	11
Appendix B - Change History	12
B.1 - V2020-OCTr2022-MAY Change Summary	12
B.2 - V2020-OCT Change Summary	12
B.3 - 2015-AUGr2017-JUL Change Summary	13
B.4 - V2015-AUG 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	6

List of Tables

Table 1 - XML Namepaces	2
Table 2 - Dependencies	3
Table 3 - Constraint Rules	9
Table 4 - Feature Summary Legend	10
Table 5 - VIRT.XML Feature comparison V2015-AUG to V2020-OCTr2022-MAY	10
Table 6 - VIRT.XML Feature comparison V2015-AUG to V2020-OCTr2022-MAY	10
Table 7 - VIRT.XML Feature comparison V1 to V2015-AUG	11
Table 8 - VIRT.XML Feature comparison V1 to V2015-AUG	11
Table 9 - DES Version Identifier History	12
Table 10 - V2020-OCTr2022-MAY Change History	12
Table 11 - V2020-OCT Change History	13
Table 12 - V2015-AUGr2017-JUL Change History	14
Table 13 - V2015-AUG Change History	15

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Virtual Coverage* (VIRT.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode virtual coverage 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 VIRT data concepts using XML.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[2]) 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.

1.3 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on describing virtual locations in shared intelligence. A structured, verifiable representation of virtual coverage 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.

The IC has standardized the various classification and control markings established for information sharing of portions within the *XML Data Encoding Specification for Information Security Markings* (ISM.XML^[9]) specification of the Intelligence Community Enterprise Architecture (ICEA) Data Standards. The VIRT.XML specification uses the ISM.XML^[9] specification to facilitate portion marking of virtual coverage needs.

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

- 200 Series:
 - Intelligence Community Directive (ICD) 208, *Write for Maximum Utility*^[3]
 - ICD 209, *Tearline Production and Dissemination*^[4]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer*^[5]
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance*^[7]
 - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information*^[8]

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^[2].

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 Namespaces

Prefix	URI
ism	urn:us:gov:ic:ism

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^[2].

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.

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ ^[9])	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[9] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[6] . 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</i> (IC-SF.XML.V2021-NOV+ ^[2])	This specification does not depend on a specific version of IC-SF.XML ^[2] ; 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.
Schematron ^[10]	<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^[11] query binding.</p>

Name	Dependency Description
<p>XSLT 2.0^[11] implementation of Schematron^[10] 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>
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.	Specification uses Controlled Vocabulary Enumeration (CVE)s to encode controlled vocabularies. The use of the VIRT CVEs is normative.

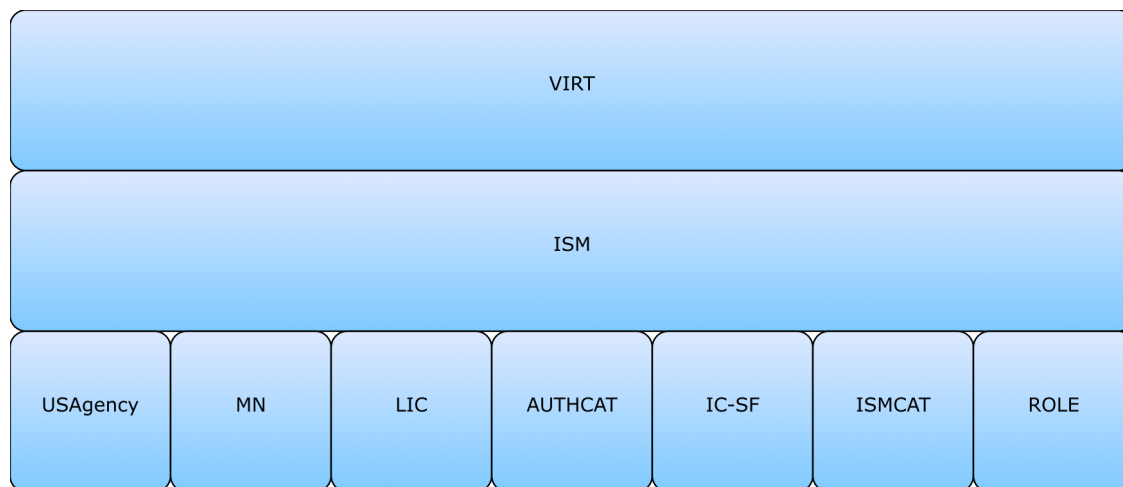


Figure 1 : Related Specifications

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](#).

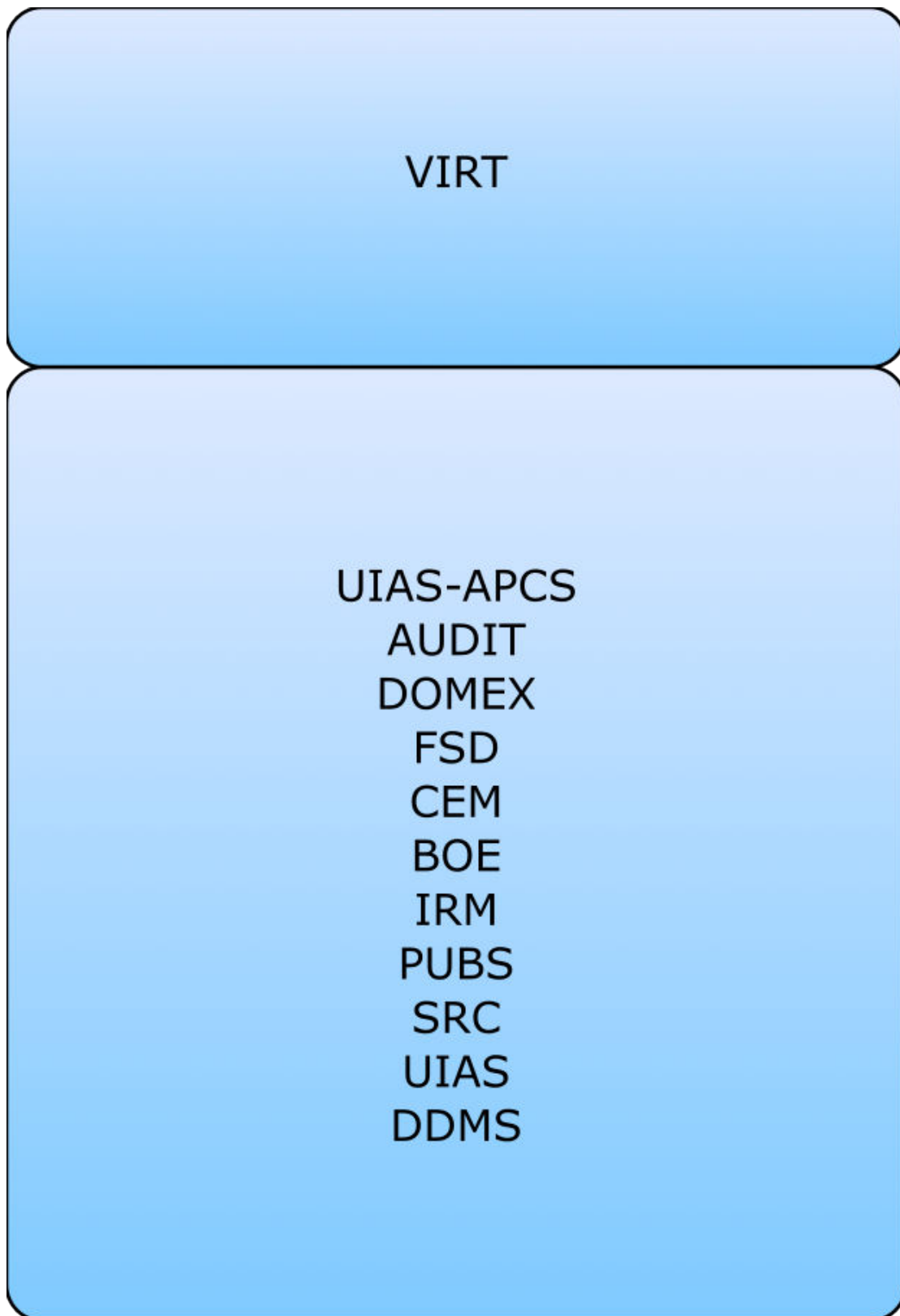


Figure 2 : Inverse Dependency Specifications

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^[2] 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

2.2.1 - Usage of ISM

ISM.XML^[9] attributes used in VIRT.XML reflect the security markings required for access rights management and handling. However, VIRT.XML is NOT a standalone specification; it does not include the necessary dependencies and structures to produce an instance document that is valid to the ISM.XML^[9] specification. VIRT.XML is a reusable component meant to be integrated into another specification that does fully implement ISM.XML^[9].

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

3.1.1 - Purpose

The VIRT.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^[2] framework document.

3.1.2 - Inherited Constraints

In an instance of VIRT.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 1.5 - Dependencies](#).

3.1.3 - Value Enumeration Constraints

Several elements and attributes of the VIRT.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.

3.1.4 - Additional Constraints

3.1.4.1 - 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.

3.1.5 - Constraint Rules

The detailed constraint rules for the VIRT.XML schema can be found in a separate document inside the Documents/VIRT directory, in the “VIRT_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 “VIRT_Rules.pdf” file as well.

3.2 - Data Rendering Constraint Rules

3.2.1 - Purpose

Rendering rules define constraints on the rendering and display of VIRT.XML documents. The intent is to inform the development of systems capable of rendering or displaying VIRT.XML data for use by individuals not familiar with the details of the VIRT.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 VIRT.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 VIRT.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 Marking System Register and Manual^[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. VIRT Feature Comparison

A.1.1. Features from V2015-AUG to V2020-OCTr2022-MAY

Table 5 - VIRT.XML Feature comparison V2015-AUG to V2020-OCTr2022-MAY

Required date	Feature	V2015-AUG	V2015-AUGr2017-JUL	V2020-OCT	V2020-OCTr2022-MAY
	Correct bug in VIRT-ID-00004	N/A	N/A	N	F

A.1.1.1. Features Partial and N/A from V2015-AUG to V2020-OCTr2022-MAY

Table 6 - VIRT.XML Feature comparison V2015-AUG to V2020-OCTr2022-MAY

Required date	Feature	V2015-AUG	V2015-AUGr2017-JUL	V2020-OCT	V2020-OCTr2022-MAY
	Support for NTK attribute based controls.	N/A	N/A	N/A	N/A

A.1.2. Features from V1 to V2015-AUG

Table 7 - VIRT.XML Feature comparison V1 to V2015-AUG

Required date	Feature	V1	V2015-AUG
	Support for NTK attribute based controls.	F	N/A
	Addition of new networks.	N	F

A.1.2.1. Features Partial and N/A from V1 to V2015-AUG

Table 8 - VIRT.XML Feature comparison V1 to V2015-AUG

Required date	Feature	V1	V2015-AUG
	Support for NTK attribute based controls.	F	N/A
	Correct bug in VIRT-ID-00004	N/A	N/A

Appendix B Change History

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

Table 9 - DES Version Identifier History

Version	Date	Purpose
1	January 21, 2013	Initial Release
2015-AUG	August 13, 2015	Added missing networks values to CVE
2015-AUGr2017-JUL	July 21, 2017	Routine revision to technical specification. For details of changes, see Section B.3 - 2015-AUGr2017-JUL Change Summary
2020-OCT	October 1, 2020	Routine revision to technical specification. For details of changes, see Section B.2 - V2020-OCT Change Summary
2020-OCTr2022-MAY	May 13, 2022	Routine revision to technical specification. For details of changes, see Section B.1 - V2020-OCTr2022-MAY Change Summary

B.1 - V2020-OCTr2022-MAY Change Summary

Significant drivers for Revision 2020-OCTr2022-MAY include:

- Community Change Requests

[Table 10](#) summarizes the changes made to this technical specification from Version 2020-OCT to Revision 2020-OCTr2022-MAY.

Table 10 - V2020-OCTr2022-MAY Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Fix bug in VIRT schematron. (CR-2022-016)	Documentation Schematron VIRT-ID-00004 modified	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Add specVersion attribute to all CVEs. (CR-2022-017)	CVE	Data generation and ingestion systems need to be updated to accommodate the changes.

B.2 - V2020-OCT Change Summary

Significant drivers for Version 2020-OCT include:

- Community Change Requests

[Table 11](#) summarizes the changes made to this technical specification from Revision 2015-AUGr2017-JUL to Version 2020-OCT.

Table 11 - V2020-OCT Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Create RelaxNG CVE Fragments. (CR-2017-189)	CVEs	No impact to systems.
2	Added schema PDF. (CR-2018-031)	Documentation	No impact to systems.
3	Update Schematron rules to have ISM ^[9] attributes on their sch:p elements to mark up the documentation. (CR-2017-319)	Schematron VIRT_XML.sch modified VIRT-ID-00001 modified VIRT-ID-00003 modified	No impact to existing systems. enhanced documentation.
4	Update Schematron rules to check for VIRT DESVersion if any VIRT elements or attributes exist. (CR-2019-017)	Schematron VIRT_XML.sch modified VIRT-ID-00004 added	Data generation and ingestion systems need to be updated to accommodate the new rule.
5	Update schema guide implementation notes with root node. (CR-2019-111)	Schema	No impact to systems.
6	Updated documentation to use the specification framework. (CR-2019-044)	Documentation	No impact to systems.
7	CSV CVEs are missing the deprecation field. (CR-2018-090)	CVEs	No impact to systems.
8	Updated rows in the Dependency Table to point to the appropriate Authoritative Source. (CR-2019-138)	Documentation	No impact to systems.
9	Corrected listed name of 5EE network in CVE (CR-2019-134)	CVEs CVEnum-VIRTNetworkName.xml modified	No impact to systems.
10	Enforce content in VirtualCoverage (CR-2020-006)	Schematron VIRT-ID-00005 added	Data generation and ingestion systems need to be updated to accommodate the new rule.

B.3 - 2015-AUGr2017-JUL Change Summary

Significant drivers for Version 2015-AUGr2017-JUL include:

- Community Change Requests

[Table 12](#) summarizes the changes made to this technical specification from Version 2015-AUG to revision 2015-AUGr2017-JUL.

Table 12 - V2015-AUGr2017-JUL Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Added the following networks: BICES, CFBLNet, DDTE in support of DI2E to VIRT Network (CR-2016-045)	CVEs CVEnum-VIRTNetworkName.xml modified	Data generation and ingestion systems need to be updated to accommodate the new values.
2	Create JSON version of CVEs in VIRT (CR-2017-070)	CVEs	No impact to systems.
3	Create CSV version of CVEs in VIRT (CR-2017-049)	CVEs	No impact to systems.
4	Added DESVersion enforcement rule as warning (CR-2017-098)	Schema Schematron VIRT-ID-00003 added VIRT_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.
5	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-127)	Documentation	No impact to systems.
6	The schema change logs will no longer be maintained as of the 2015-AUGr2017-JUL release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2015-AUGr2017-JUL, reference the change history in the DES.	Schema	No impact to systems.
7	Added the revision constraint section since this is the first revision of VIRT.	Documentation	Data generation and ingestion systems will may need to be updated to properly validate against the right revisions of specifications.
8	Added DES section describing versioning strategy. (CR-2017-201)	Documentation	No impact to systems.

#	Change	Artifacts Changed	Compatibility Notes
9	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-2017-216)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
10	Update prose to align with current specifications. Specifically, change e-mail address to ic-standards-support@iarpa.gov, update dependency table to standardize wording. (CR-2017-235)	Documentation	No impact to systems.
11	Modified cardinality rendering. (CR-2017-023)	CVEs	No impact to existing systems, documentation rendering change only.
12	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-237, CR-2017-260)	Documentation	No impact to systems.

B.4 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Community Change Requests

[Table 13](#) summarizes the changes made to this technical specification from Version 1 to Version 2015-AUG.

Table 13 - V2015-AUG Change History

	Change	Artifacts Changed
1	Added network values to CVE	CVE
2	Updated code descriptions to improve readability.	Schematron
3	Removed NTK attribute based access	DES
4	Removed Dependency on NTK	DES Schema

	Change	Artifacts Changed
5	Deleted Schematron rule 00002	VIRT_ID_00002.sch

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
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
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-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>

[3] ICD 208

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

[4] ICD 209

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012. Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf>

[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 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

[7] ICS 500-20

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

[8] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-TS at: <https://go.ic.gov/0Agmenr> (case sensitive – 0 Alpha golf mike echo november romeo)

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

[9] 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>

[10] 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/>

[11] 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^[7].