



Intelligence Community Technical Specification

XML Data Encoding Specification for Information Transport Service Messaging Service

Version 2015-FEBr2018-JUL

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 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	2
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.6.3 - Terminology	3
1.6.4 - XML Namespaces	3
1.7 - Dependencies	4
1.7.1 - Types of Dependencies	4
1.7.2 - Specification Dependencies	4
1.7.3 - Inverse Dependencies	7
1.7.4 - 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	11
2.1 - Relationship to Abstract Data Definition and other encodings	11
2.2 - Additional Guidance	11
2.2.1 - Information Transport Service Messaging Service Usage	11
2.2.2 - Information Transport Service Messaging Service Elements	11
2.2.2.1 - Its Element	11
2.2.3 - Information Transport Service Messaging Service Assertion and Trusted Data Format	12
2.2.3.1 - ITS Assertion Scope	13
2.3 - CSV Notes	13
2.4 - JSON Notes	14
2.5 - RELAX NG Notes	14
Chapter 3 - Definitions, Interfaces, and Constraints	15
3.1 - Constraint Rule Types	15
3.2 - “Living” Constraint Rules	15
3.3 - Classified or Controlled Constraint Rules	15
3.4 - Constraint Terminology	15
3.5 - Errors and Warnings	16
3.6 - Rule Identifiers	16
3.7 - Data Validation Constraint Rules	16
3.7.1 - Purpose	16
3.7.2 - Schematron	17
3.7.3 - Non-null Constraints	17
3.7.4 - Inherited Constraints	17
3.7.5 - Value Enumeration Constraints	18
3.7.6 - Additional Constraints	18

3.7.6.1 - DES Constraints	18
3.7.6.2 - Revision Constraints	18
3.7.7 - Constraint Rules	20
3.8 - Data Rendering Constraint Rules	20
3.8.1 - Purpose	20
3.8.2 - Rendering Constraint Rules	20
Chapter 4 - Conformance Validation	21
4.1 - Schema Validation	21
4.2 - Business Rule Validation	21
Chapter 5 - Generated Guides	22
5.1 - Schema Guide	22
5.2 - Schematron Guide	23
Appendix A - Feature Summary	24
A.1 - ITS-MS Feature Summary	24
Appendix B - Change History	26
B.1 - V2015-FEBr2018-JUL Change Summary	26
B.2 - V2015-FEBr2018-APR Change Summary	26
B.3 - V2015-FEB Change Summary	28
Appendix C - List of Abbreviations	30
Appendix D - Bibliography	32
Appendix E - Points of Contact	37
Appendix F - IC CIO Approval Memo	38

List of Figures

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

List of Tables

Table 1 - XML Namepaces	3
Table 2 - Direct Dependencies	5
Table 3 - Relationships	6
Table 4 - Numerical Rule Identifier Ranges	16
Table 5 - Revision Constraints table	19
Table 6 - ITS-MS.XML Dependency over time	24
Table 7 - Feature Summary Legend	24
Table 8 - ITS-MS Feature Comparison	24
Table 9 - DES Version Identifier History	26
Table 10 - Data Encoding Specification 2015-FEBR2018-JUL Change Summary	26
Table 11 - Data Encoding Specification 2015-FEBR2018-APR Change Summary	27
Table 12 - Data Encoding Specification 2015-FEB Change Summary	29

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Information Transport Service Messaging Service* (ITS-MS.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode ITS-MS 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 ITS-MS data assertion concepts using XML within the use of a *XML Data Encoding Specification for Trusted Data Format* (IC-TDF.XML)^[10] Trusted Data Object (TDO) or Trusted Data Collection (TDC). This DES defines how to properly structure a valid instance of an ITS-MS.XML assertion that would conform with this specification. Use of IC-TDF.XML^[10] is required for compliance with this DES. A (IC-TDF.XML)^[10] instance may conform with multiple DES simultaneously assuming none of the criterion are in conflict.

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.

The ITS-MS.XML specification provides the base XML elements used to define an ITS-MS.XML Assertion within a IC-TDF.XML^[10] TDO or TDC within the Information Transport Service (ITS).

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*^[11] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common Information Technology (IT) standards, protocols, and interfaces, to establish uniform information security standards, and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community

Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[15] the extensive and consistent use of XML within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

An encoding specification defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* ADD^[2]. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID^[9] defines a plain-text format for IC Identifiers as well as an associated XML structure.

1.4 - Enterprise Need

Broad information sharing within the national intelligence enterprise is facilitated by the creation and identification of variants of information resources. This enterprise requires a seamless transport for data and information resources between IC elements, able to scale and fit the various needs of the IC and the IC elements. A common specification for the description of transport information allows for a comprehensive and scalable capability that can transport any and all resources across the enterprise regardless of format, type, location, or classification.

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

- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[11]
 - ICD 502, *Integrated Defense of the Intelligence Community Information Environment* ^[12]
 - ICD 503, *Intelligence Community Information Technology Systems Security Risk Management* ^[13]
 - ICS 500-20, *IC Enterprise Standards Compliance* ^[14]
 - ICS 500-27, *Collection and Sharing of Audit Data* ^[16]

1.5 - Audience and Applicability

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

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance* ^[14] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD* ^[7], requires DoD elements to use the DoD IT Standards Registry (DISR) ^[6].

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their

cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

1.6 - Conventions

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

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2119, “Key words for use in RFCs to Indicate Requirement Levels” [\[17\]](#). When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.6.3 - Terminology

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

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

1.6.4 - XML Namespaces

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

Table 1 - XML Namespaces

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

1.7 - Dependencies

1.7.1 - Types of Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. Dependencies play an important role in functionality or provide informational relationships between the various artifacts. The following terms are defined to help assist with understanding how the various artifacts work together:

Dependency	Directly or transitively influenced by. Examples: 1. A is influenced by B therefore B is a dependency of A. 2. A is influenced by B and B is influenced by C; therefore C is a dependency of A.
Direct Dependency	Explicit influence. Example: A influences B.
Inverse Dependency	Directly or transitively influences. Example: B influences A.

1.7.2 - 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 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 - Direct Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Trusted Data Format</i> (IC-TDF.XML.V2014-DEC+) ^[10]	ITS-MS.XML elements as well as its dependent specifications are used in conjunction with IC-TDF.XML ^[10] objects as structured assertions or content that compose the necessary material represented by ITS-MS.XML. The dependence of ITS-MS.XML on IC-TDF ^[10] is normative. This specification does not depend on a specific version of IC-TDF.XML ^[10] ; IC-TDF.XML ^[10] versions later than version 2014-DEC MAY be used. The minimum version was based on program choice; the Audit Developers Forum requested the minimum versions be those that were most current in 2015-FEB when this version of ITS-MS.XML was created.
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2014-DEC+) ^[18]	This specification does not depend on a specific version of ISM.XML ^[18] ; versions later than version 2014-DEC MAY be used. The minimum version was based on program choice; the Audit Developers Forum requested the minimum versions be those that were most current in 2015-FEB when this version of ITS-MS.XML was created.
Schematron ^[26]	<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^[34] query binding.</p>

Name	Dependency Description
XSLT 2.0 ^[34] implementation of Schematron ^[26] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/ .	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

This technical specification can be used in conjunction with the additional technical specifications or additional documentation listed in the following table. The documents listed below may or may not be referenced in this Data Encoding Specification, and may or may not be considered normative or informative.

Table 3 - Relationships

Related Specification	Relationship Description
XML Data Encoding Specification for Audit (AUDIT.XML.V*) ^[4]	Relationship on AUDIT.XML. Any version of AUDIT.XML may be used as the payload(s) of the IC-TDF.XML ^[10] TDO or TDC.

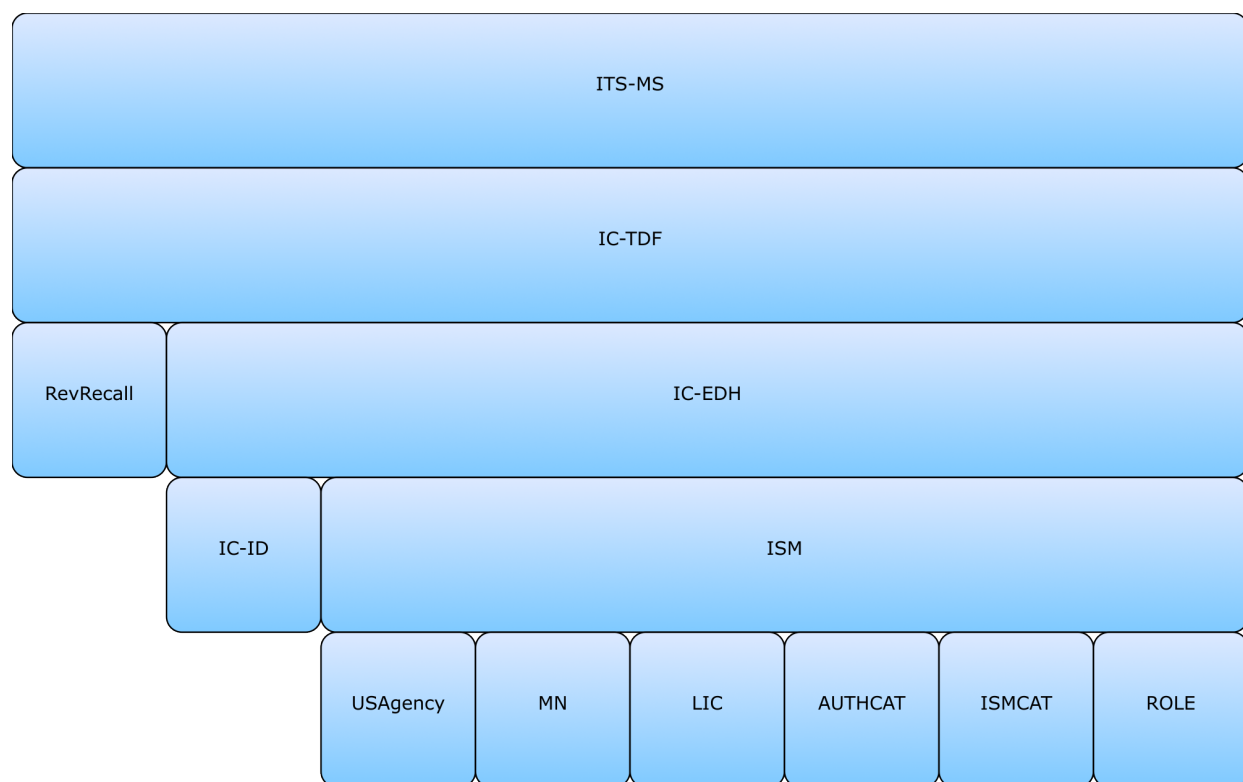


Figure 1 : Related Specifications

1.7.3 - 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).

This specification is not used by other specifications released by the IC CIO, and therefore does not contain an Inverse Dependency Diagram.

1.7.4 - 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 dependent (see [Dependency](#)) specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and Controlled Vocabulary Enumeration (CVE)s 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 any Schematron^[26] 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 Extensible Stylesheet Language (XSL) transformations, the SchematronGuide, and PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[17] 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^[32]. For example, a schema could be changed to incorporate a different version of a dependency like ISM.XML^[18] by changing the attribute declaration of `@ism:DESVersion="201508"` to `@ism:DESVersion="201609"` in the `xsd:schema` statement. The ability to specify which version of a dependent specification to import enables the configuration change control of parent specifications (such as AUTHCAT.CES^[5]) to be “decoupled” from the configuration change control of dependent specifications (such as UIAS.XML^[28] CVE updates). This “decoupling” method has not been in place for all versions of these parent specifications; therefore, please verify with the dependency table to ensure use of allowed dependency versions.

Additional guidance that is either classified or has handling controls can be found in separate annexes distributed to the appropriate networks and environments as necessary. Systems and services operating in those environments **MUST** consult the appropriate annexes.

1.9 - Version Policies

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from “The Disposition of Names in an XML Namespace.”^[27] This decision allows for systems that process information encoded with these specifications to use the same Path Language (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.”^[30]

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

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

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

1.9.2 - Version Numbering

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-
MMM). This provides a temporal representation of when the specification was released. Revisions to a version of the specification also use a year-month structure (e.g., YYYY-
MMM). 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](#)["." [Revision](#)] ["-" [CustomizationSuffix](#)]
- [2] VersionYear ::= 4(DIGIT)
- [3] VersionMonth ::= 2(DIGIT)
- [4] Customization ::= 1*23(ALPHA / DIGIT / "_")
Suffix
- [5] RevisionYear ::= 4(DIGIT)
- [6] RevisionMont ::= 2(DIGIT)
h
- [7] Revision ::= [Year Month](#)

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/revision being referenced.
VersionYear	The four digit year from the version of the specification being referenced.
VersionMonth	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.

RevisionYear	The four digit year from the revision of the specification being referenced.
RevisionMonth	The 2 digit month from the revision of the specification being referenced.
Revision	The Year and Month from the revision of the specification being referenced. Revisions are modifications to Versions.

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 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 - Information Transport Service Messaging Service Usage

ITS-MS.XML is used in conjunction with the IC-TDF.XML^[10] format and consists of structured assertions that contain information required for generating an ITS-MS.XML compliant instance. A TDO or TDC conforms to the ITS-MS.XML specification when it contains:

- A structured assertion of scope TDO or TDC with an **its:Its** element.
- A payload that is the data object to be transported by ITS .
- No other Assertions.

2.2.2 - Information Transport Service Messaging Service Elements

The ITS-MS.XML schema has only one root element and that is the **its:Its** element.

2.2.2.1 - Its Element

The **its:Its** element is contained in the structured statement of an assertion within a TDO with scope [TDO] or a TDC with scope [TDC]. In this context, the instance should be representative of

the entire TDO or TDC, including all variants. The DESVersion attribute indicates the ITS-MS.XML version, and the other elements and attributes represent the messaging information for the object.

Example:

```
<Assertion tdf:scope="TDO">
  <StatementMetadata>
    <Security xmlns="urn:us:gov:ic:arh"
      ism:classification="U"
      ism:ownerProducer="USA"/>
  </StatementMetadata>
  <StructuredStatement>
    <its:Its its:DESVersion="201502.201807">
      ...
    </its:Its>
  </StructuredStatement>
</Assertion>
```

2.2.3 - Information Transport Service Messaging Service Assertion and Trusted Data Format

The TDO and TDCs adhere to the IC-TDF.XML^[10] specification. The metadata required by the ITS Client is contained in the structured statement of an ITS-MS.XML assertion within the TDO or TDC, and this metadata adheres to the ITS-MS.XML schema.

The following **its:Its** elements are required to be included in the ITS-MS.XML assertion structured statement, and must be populated prior to submission to the ITS Client.

- **its:ObjectType** – is required to identify the type of data object in the message payload. All ITS assertions must be listed as “AUDIT” or “ACINT” as enumerated in the schema.
- **its:Originator** – contains child elements that identify the originating ITS client (**its:Client**) and also includes the CreateDateTime (**its:CreateDateTime**).
- **its:RecipientList** - contains one or more ClientIDs (**its:Client/its:ClientID**) of the receiving ITS clients.
- **its:encryptTDO** – Boolean value indicating whether TDO should be encrypted in transit is generally set to False. This indicates no encryption during transit. If the value is set to True then encryption during transit applies.
- **its:Fabric** – expressly identifies the network domain from which the message is originating restricted to values from a CVE “CVEnumITSMSFabric” in ITS-MS.XML.

These elements will be populated by the ITS Client when it transmits the message. They will be available to the receiving client.

- **its:MessageId** – A version 4 Universal Unique Identifier (UUID) which can be used to track the transport of this IC-TDF.XML^[10] from originating ITS client to all recipient ITS clients. This element is optional when creating ITS-MS.XML for transport by ITS, but will be populated by the originating ITS client at the point of transport.

- **its:Priority** – sets the importance of a message relative to others in the queue.



Note

For Audit objects this should be set to **ROUTINE**.

- **its:PublishDateTime** – set to the date/time the object is published to the queue by the ITS Client [YYYY-MM-DDTHH:MM:SS.0Z].

In addition to those mentioned above, instances must be fully schema and Schematron valid for all specifications. For more information please review the appropriate SchemaGuides.

2.2.3.1 - ITS Assertion Scope

If the file being sent is a TDC, then the TDC, must contain one and only one ITS-MS.XML assertion and its scope attribute must be [TDC]. A TDC is a collection of TDOs and when the file being sent is a TDC there must be no ITS-MS.XML assertions within the TDOs.

If the file being sent is a TDO then the TDO must contain one and only one ITS assertion and its scope attribute must be [TDO].

2.3 - CSV Notes

There are Comma Separated Value (CSV) files provided for all of the CVEs. They are in the CVE folder with the XML and JavaScript Object Notation (JSON) versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence.



Important

The CSV files on many systems will open “automatically” in Microsoft Excel; the default opening however, may not correctly read UTF-8 special characters. These are found in some country names such as “Republic of Côte d’Ivoire”. We added the Byte Order Mark (BOM) as this appears to make newer versions of Excel work properly without the following workaround. If you need to use a CVE that contains such special characters, or you think may contain such characters in Excel, you should:



Note

The following steps tested successfully for macOS Excel version 15.3.9 and Microsoft Windows Excel version 14.0.7; it was unsuccessful for macOS Excel version 14.7.1

1. Open Excel to a blank sheet
2. Under the Data menu choose to get external data from a text file
3. Choose UTF-8 as the file origin
4. Choose delimited as the format

5. Choose next
6. Change from tab to Comma as the delimiter
7. Finish import to get the data in with the UTF-8 Characters properly encoded in Excel.

2.4 - JSON Notes

There are JSON format files provided for all of the CVEs. They are in the CVE folder with the XML and CSV versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence. The JSON files are formatted using JavaScript Object Notation for Linked Data (JSON-LD) based on a proposed method for JSON in National Information Exchange Model (NIEM).

2.5 - RELAX NG Notes

There are REgular LAnguage for XML Next Generation (RELAX NG) format files provided for all of the CVEs. They are in the Schema folder with the XML Schema Definition (XSD) versions of the information. They are provided as a convenience to developers who wish to import IC Specification CVEs into other XML specifications that utilize RELAX NG. They will not affect specifications that do not utilize RELAX NG and there are no new requirements because of their existence. RELAX NG is an alternative schema language for XML and it provides both an XML syntax and a compact non-XML syntax. The XML syntax format fragments are provided with the .rng file name extension and the Compact syntax fragments are provided with the .rnc file name extensions.

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 - Constraint Terminology

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

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

- The term “must not be specified” indicates that an attribute **MUST NOT** be applied to an element.

3.5 - Errors and Warnings

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

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

3.6 - Rule Identifiers

Each constraint rule has an assigned rule identifier, indicated in brackets preceding the constraint rule description. ITS-MS.XML data validation constraint rule identifiers are prefixed with “ITS-MS-ID-” and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in [Section 3.6 - Rule Identifiers \[16\]](#). As the constraint rules are managed over time, IDs from deleted rules will not be reused.

Table 4 - Numerical Rule Identifier Ranges

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

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

The ITS-MS.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^[26] 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^[26] rules for this specification may be executed in *Oxygen*^[24] or with an XSLT 2.0-compliant processor using the XSLT 2.0^[34] 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^[33] and XSLT 2.0^[34] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard^[20] stated the following:

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^[34] implementation of Schematron^[26] along with a compiled version of the rules.

3.7.3 - Non-null Constraints

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

3.7.4 - Inherited Constraints

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

¹“White space” is defined in XML 1.0^[31] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

3.7.5 - Value Enumeration Constraints

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

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

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

3.7.6 - Additional Constraints

3.7.6.1 - DES Constraints

The DES version is specified through attributes on the root element. The schema constrains the values of these attributes. The **DESVersion** attribute enables systems processing an instance document to be certain which set of constraint rules, schema, CVEs and business rules are intended by the author to be used.

3.7.6.2 - Revision Constraints

When validating an instance document against the validation rule sets and schema provided by the specification there is a certain philosophy that **SHOULD** be applied to both protect the data and the systems processing that data. This validation philosophy consists of the following seven basic rules that describe how the DESVersion matters to validation:

1. One **MUST NOT** validate with rules older than the integer version declared in an instance; this is an error.
2. One **MAY** validate with rules that are of a greater integer version than an instance.
3. When validating an instance with a lower integer version number than that of the validation rules, there **MAY** be a minimum integer version cutoff for a set of rules. If such a limit exists, this is an error.
4. Within an integer, validation **MUST** only occur with the newest decimal value implemented by the validator; that is a validator **MUST** only implement one signed validation rule set within an integer and it **SHOULD** be the latest.
5. When a validator detects an instance document claiming a version newer than what is implemented in the validator, a notice/log **SHOULD** be generated so a human can evaluate if the validator needs to be updated to the latest rule set, as passing the old rules **MAY** not comply with current law or policy.

6. A validator SHOULD document and communicate all versions and revisions it accepts, including the constraints (business/policy rules, allowed values, schema formats, etc.) in each of those versions.

The matrix of fictional generic examples in [Table 5](#) are provided to illustrate these validation concepts with the following assumptions:

- Version 11: Technically incompatible with newer versions
- Version 12: Technically compatible with newer versions, but retired from the Enterprise Standards Baseline
- Version 13: Oldest in the Enterprise Standards Baseline
- Version 13.201701: Revision to version 13
- Version 13.201804: Revision to version 13
- Version 201508: Standard release
- Version 201609: Latest version release

Table 5 - Revision Constraints table

Validation Rules Version	11	12	13	13.201701	13.201804	201508	201609
Instance Version							
11	Version Match	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)
12	Instance Too New	Version Match	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)
13	Instance Too New	Instance Too New	Version Match	Same Integer	Same Integer	Allowed	Allowed
13.201701	Instance Too New	Instance Too New	Same Integer	Version Match	Same Integer	Allowed	Allowed
13.201804	Instance Too New	Instance Too New	Same Integer	Same Integer	Version Match	Allowed	Allowed
201508	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Version Match	Allowed
201609	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Version Match

3.7.7 - Constraint Rules

The detailed constraint rules for the ITS-MS.XML schema can be found in a separate document inside the SchematronGuide directory, in the ITS-MS_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 ITS-MS_Rules.pdf file.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of ITS-MS.XML documents. The intent is to inform the development of systems capable of rendering or displaying ITS-MS.XML data for use by individuals not familiar with the details of the ITS-MS.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

There are no Data Rendering Constraint rules for ITS-MS.XML at this time.

Chapter 4 - Conformance Validation

An instance document conforms with this specification if it conforms to all normative guidance of this specification and this specification's dependencies and 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.



Warning

If IC-TDF.XML^[10] is being used it is critical to follow the validation strategy outlined in IC-TDF.XML^[10] to achieve proper schema validation. Failure to do so will have a high probability of schema invalid data appearing to be valid.

4.2 - Business Rule Validation

An instance document **MUST** comply with the business rules expressed in this specification and those expressed in this specification's dependencies. 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 ITS-MS.XML schema can be found as a collection of HyperText Markup Language (HTML) files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the ITS-MS.XML schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen®*, 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
- 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 ITS-MS.XML Schematron rules can be found in a separate document named *ITS-MS_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 ITS-MS.XML on other specifications. Direct dependencies are marked with an asterisk.

Table 6 - ITS-MS.XML Dependency over time

Dependent DES	V1	V2015-FEB	V2015-FEBr2018-APR	V2015-FEBr2018-JUL
IC-TDF.XML ^[10] *	V1+	V1+	V2014-DEC+	V2014-DEC+
ISM.XML ^[18] *	V9+	V9+	V2014-DEC+	V2014-DEC+
NTK.XML ^[23]	V7+	V7+	V10+	V10+
ARH.XML ^[3]	V1+	V1+	V3+	V3+
IC-EDH.XML ^[8]	V1+	V1+	V4+	V4+
ISMCAT.CES ^[19]			V2017-SEP+	V2017-SEP+
USAgency.CES ^[29]			V2015-FEB+	V2015-FEB+
MN.CES ^[22]			V2015-AUG+	V2015-AUG+
LIC.CES ^[21]			V2015-AUG+	V2015-AUG+
AUTHCAT.CES ^[5]			V2018-APR+	V2018-APR+
IC-ID.XML ^[9]			V1+	V1+
RevRecall.XML ^[25]			V2014-DEC+	V2014-DEC+

The following tables summarize major features by version for ITS-MS.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 has an implementation date of one year after issuance).

Table 7 - 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. ITS-MS Feature Summary

Table 8 - ITS-MS Feature Comparison

Required date	Feature	V1	V2015-FEB	V2015-FEBr2018-APR	V2015-FEBr2018-JUL
	Express Recipient information	F	F	F	F
	Express Sender information	F	F	F	F
	IC Identifier (IC-ID)	F	N	N	N

Required date	Feature	V1	V2015-FEB	V2015-FEBr2018-APR	V2015-FEBr2018-JUL
	UUID Version 4	N	F	F	F
	Enable Non-SCI fabric deployment	N	N	F	F
	Use EA-COL for non-SCI fabric deployment	N	N	N	F

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	21 January 2013	Initial Release
2015-FEB	23 February 2015	Routine revision to technical specification. For details of changes, see Section B.3 - V2015-FEB Change Summary .
2015-FEBr2018-APR	April 20, 2018	Routine revision to technical specification. For details of changes, see Section B.2 - V2015-FEBr2018-APR Change Summary .
2015-FEBr2018-JUL	July 31, 2018	Routine revision to technical specification. For details of changes, see Section B.1 - V2015-FEBr2018-JUL Change Summary .

B.1 - V2015-FEBr2018-JUL Change Summary

Significant drivers for Version 2015-FEBr2018-JUL include:

- Enable Non-SCI fabric deployment of ITS-MS.XML.

The following table summarizes the changes made to 2015-FEBr2018-APR in developing 2015-FEBr2018-JUL.

Table 10 - Data Encoding Specification 2015-FEBr2018-JUL Change Summary

	Change	Artifacts changed	Compatibility Notes
1	Replace the "AUDIT" token with "EA-COL" in CVEnum-ITSMSFabric.xml (CR-2018-108)	CVEnum-ITSMSFabric.xml updated	Systems must be able to account for a new value that they may receive.

B.2 - V2015-FEBr2018-APR Change Summary

Significant drivers for Version 2015-FEBr2018-APR include:

- Enable Non-SCI fabric deployment of ITS-MS.XML.

The following table summarizes the changes made to 2015-FEB in developing 2015-FEBr2018-APR.

Table 11 - Data Encoding Specification 2015-FEB2018-APR Change Summary

	Change	Artifacts changed	Compatibility Notes
1	Added "AUDIT" to CVEnum-ITSMSFabric.xml (CR-2018-041)	CVEnum-ITSMSFabric.xml updated	Systems must be able to account for a new value that they may receive.
2	Added schema PDF. (CR-2018-018)	Documentation	No impact to systems.
3	Create JSON version of CVEs in ITS-MS (CR-2017-059)	CVEs	No impact to systems.
4	Create CSV version of CVEs in ITS-MS (CR-2017-037)	CVEs	No impact to systems.
5	Create RelaxNG CVE Fragments for ITS-MS. (CR-2017-178)	CVEs	No impact to systems.
6	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-2017-224)	Schematron ITS-MS-ID-00001 modified	No impact to existing systems. Additional capabilities.
7	Modified cardinality rendering. (CR-2018-044)	CVEs	No impact to existing systems, documentation rendering change only.
8	Update Schematron rules to have ISM ^[18] attributes on their sch:p elements to mark up the documentation. (CR-2017-307)	Schematron ITS-MS-ID-00001 modified	No impact to existing systems. enhanced documentation.
9	Add Version numbering EBNF to reflect the existence of Revisions (CR-2018-043)	Documentation	Systems processing the Desversion attribute should be aware of the Revision structure and able to process it.
10	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-278)	Documentation	No impact to systems.
11	Updated DESVersion attribute to generic regex in the schema and created schematron rule to check current DESVersion. (CR-2017-340) Ensured Schematron rule is warning instead of errors for matching Version attribute (CR-2017-086)	Schema Schematron ITS-MS-ID-00002 added	Data generation and ingestion systems need to be updated to accommodate the changes.

	Change	Artifacts changed	Compatibility Notes
12	Constrained its:PublishDateTime to a date format. (CR-2016-027)	Schema	Data generation and ingestion systems need to be updated to accommodate the changes, although the current ITS client software already requires this.
13	The schema change logs will no longer be maintained as of the 2015-FEBr2018-APR release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2015-FEBr2018-APR, reference the change history in the DES.	Schema	No impact to systems.
14	Update prose to align with current specifications. Change e-mail address to ic-standards-support@iarpa.gov. (CR-2018-045)	Documentation	No impact to systems.
15	Updated rule documentation to remove use of "we". (CR-2018-046)	Schematron ITS-MS-ID-00001 modified ITS-MS_XML.sch modified	No impact to systems.
16	Update applicability section to reflect a requirement to comply with Law/Policy (CR-2018-049)	Documentation	Implementers must verify that they are complying with applicable laws and policies.
17	Enforce minimum versions for ITS-MS dependent specifications. (CR-2018-048)	Schematron ITS-MS-ID-00003 added	Data generation and ingestion systems need to be updated to accommodate the changes.
18	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.3 - V2015-FEB Change Summary

Significant drivers for Version 2015-FEB include:

- Alignment with system implementations of ITS-MS.XML

The following table summarizes the changes made to V1 in developing 2015-FEB.

Table 12 - Data Encoding Specification 2015-FEB Change Summary

Change	Artifacts changed	Compatibility Notes
Changed <code>MessageId</code> from a IC-ID to a version 4 UUID and made the element optional.	Schema	Data generation and ingestion systems need to be updated to handle this schema change.
Made <code>DESVersion</code> attribute required.	Schema	No impact to systems that already specified the <code>DESVersion</code> attribute. Data generation and ingestion systems that did not fill out the <code>DESVersion</code> attribute need to be updated to handle this schema change.
Added Acoustic Intelligence (ACINT) as another possible value for the type of message object defined by the <code>ObjectType</code> element.	Schema	Data generation and ingestion systems need to be updated to handle this Schema change.
Added ACINT as another possible value for the originating network defined by the <code>Fabric</code> element.	CVE	Data generation and ingestion systems need to be updated to handle this CVE change.

Appendix C List of Abbreviations

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

ACINT	Acoustic Intelligence
ADD	Abstract Data Definition
CSV	Comma Separated Value
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOD	Department of Defense
FOUO	For Official Use Only
HTML	HyperText Markup Language
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
IC-ID	IC Identifier
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology
ITS	Information Transport Service
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
NIEM	National Information Exchange Model

RELAX NG	REgular LAnguage for XML Next Generation
RFC	Request for Comments
TDC	Trusted Data Collection
TDO	Trusted Data Object
URL	Uniform Resource Locator
UUID	Universal Unique Identifier
XML	Extensible Markup Language
XPath	XML Path Language
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

[1] ABNF

Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.

Available online at: <http://tools.ietf.org/html/std68>

Also known as: <http://www.ietf.org/rfc/rfc5234.txt>

[2] ADD

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

Available online Intelink-TS at: <https://go.ic.gov/6I5LJNo> (case sensitive – 6 India 5 Lima Juliet November oscar)

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

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

[3] 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: <https://go.ic.gov/FTSj6AO> (case sensitive – Foxtrot Tango Sierra juliet 6 Alpha Oscar)

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

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

[4] AUDIT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Audit Exchange (AUDIT.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/Og5CcLk> (case sensitive – Oscar golf 5 Charlie charlie Lima kilo)

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

[5] AUTHCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Authority Category (AUTHCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/JIMIYN5> (case sensitive – Juliet India Mike lima Yankee November 5)

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

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

[6] DISR

Department of Defense. *DoD Information Technology Standards Registry*.

Available online at: <https://gtg.csd.disa.mil/distr/> continuing on to the actual registry requires a CAC and an account.

[7] DoD Instruction 8310.01

DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 31 July 2017.

31 Jul 2017 edition incorporates Change 1 to the 2 February 2015 edition.

Available online at: <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/831001p.pdf>

[8] 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>

[9] IC-ID.XML

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

Available online Intelink-TS at: <https://go.ic.gov/aKlfr9y> (case sensitive – alpha Kilo lima foxtrot romeo 9 yankee)

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

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

[10] 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>

[11] 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

[12] ICD 502

Office of the Director of National Intelligence. *Integrated Defense of the Intelligence Community Information Environment*. Intelligence Community Directive 502. 11 March 2011.

Available online at: <https://go.ic.gov/KvTQYLw> (case sensitive – Kilo victor Tango Quebec Yankee Lima whiskey)

[13] ICD 503

Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management*. Intelligence Community Directive 503. 21 July 2015.

Available online Intelink-TS at: <https://go.ic.gov/Ru5XGc9> (case sensitive – Romeo uniform 5 Xray Golf charlie 9)

Available online at: <http://www.dni.gov/files/documents/ICD/ICD503.pdf>

[14] 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>

[15] 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>

[16] ICS 500-27

Director of National Intelligence Chief Information Officer. *Intelligence Community Standard for Collection and Sharing of Audit Data*. Intelligence Community Standard 500-27. 2 June 2011.

Available online Intelink-TS at: <https://go.ic.gov/Jznuy0x> (case sensitive – Juliet zulu november uniform yankee 0 xray)

[17] 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>

[18] 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>

[19] ISMCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/mL5WA9> (case sensitive – mike Lima Foxtrot 5 Whiskey Alpha 9)

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

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

[20] Jelliffe

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

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

[21] LIC.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for License (LIC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/lsHgQxJ> (case sensitive – India sierra Hotel golf Quebec xray Juliet)

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

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

[22] MN.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Mission Need (MN.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/ndd7V1R> (case sensitive – november delta delta 7 Victor 1 Romeo)

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

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

[23] NTK.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/6wFIZpE> (case sensitive – 6 whiskey Foxtrot India Zulu papa Echo)

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

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

[24] Oxygen

SyncRO Soft. <oXygen/> XML Editor.

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

[25] REVRECALL.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Revision Recall (RevRecall.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/cC4WFa0> (case sensitive – charlie Charlie 4 Whiskey Foxtrot alpha 0)

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

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

[26] 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/>

[27] 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>

[28] UIAS.XML

Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/xQK4AX1> (case sensitive – xray Quebec Kilo 4 Alpha Xray 1)

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

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

[29] USAgency.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/wmyIRCV> (case sensitive – whiskey mike yankee India Romeo Charlie Victor)

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

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

[30] 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>

[31] 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>

[32] 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>

[33] 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/>

[34] 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^[14].