Intelligence Community Technical Specification

XML Data Encoding Specification for Information Transport Service Messaging Service

Version 2015-FEB

February 23, 2015

Table of Contents

List of Figures

List of Tables

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 Trusted Data Format (TDF) Object or Collection. This DES defines how to properly structure a valid instance of an ITS-MS assertion that would conform with this specification. Use of TDF is required for compliance with this DES. A TDF 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 provides the base XML elements used to define an ITS Assertion within a Trusted Data Format Object or Collection within the ITS Enterprise Audit System.

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

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

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

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* [11] the

extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby achieving the IC's data discovery, data sharing, and interoperability goals.

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

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

1.4 - Enterprise Need

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.

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

- IC Information Technology Enterprise (IC ITE):
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[3]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[6]
  - Intelligence Community Directive (ICD) 502, Integrated Defense of the Intelligence Community Information Environment[7]
  - Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation[8]
  - Intelligence Community Standard (ICS) 500-27, Collection and Sharing of Audit Data[12]

1.5 - Audience and Applicability

DESs are primarily intended to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described.

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,[10] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

1.6 - Conventions

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

1.6.1 - Language

The keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this technical specification are to be interpreted as described in the IETF RFC 2119.[13] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.7 - Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in Table 1. The dependencies listed below are directly referenced in this specification (e.g. Schema, Schematron), and are normative or informative as indicated.

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

Table 1 - Dependencies

Name	Dependency Description
XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V1+)[5]	ITS-MS elements are used in conjunction with the Trusted Data Format and consist of structured assertions that contain information required for generating Trusted Data Objects (TDO)or a Trusted Data Collection (TDC). The dependence of ITS-MS on TDF is normative. Starting with TDF v1, the version of TDF and related specifications imported is no longer normative, so any TDF version 1 or above may be used with ITS-MS v1.
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V9+)[14]	Depends on Information Security Markings (ISM). Starting with ISM v9, the version of ISM imported is no longer normative, so any ISM version 9 or above may be used.
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V7+)[16]	Depends on Need To Know (NTK) markings. Starting with NTK v7, the version of NTK imported is no longer normative, so any NTK version 7 or above may be used.
XML Data Encoding Specification for Enterprise Data Header (IC-EDH XML.V1+)[4]	Depends on Enterprise Data Header (EDH)specification. Starting with EDH v1, the version of EDH imported is no longer normative, so any EDH version 1 or above may be used.
XML Data Encoding Specification for Access Rights and Handling (ARH.XML.V1+)[1]	Depends on Access Rights and Handling (ARH) markings. Starting with ARH v1, the version of ARH imported is no longer normative, so any ARH version 1 or above may be used.
Schematron[18]	Schematron — ISO/IEC 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative. The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. Note: The Schematron rules in this specification use XSLT 2.0[22] query binding.

Name	Dependency Description
XSLT 2.0[22] implementation of Schematron[18] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the *behavior* 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 *if and only if* 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 2 - Relationships

Related Specification	Relationship Description
XML Data Encoding Specification for Audit (AUDIT.XML.V*)[2]	Relationship on AUDIT.XML. Any version of AUDIT.XML may be used as the payload(s) of the TDF Object or Collection.

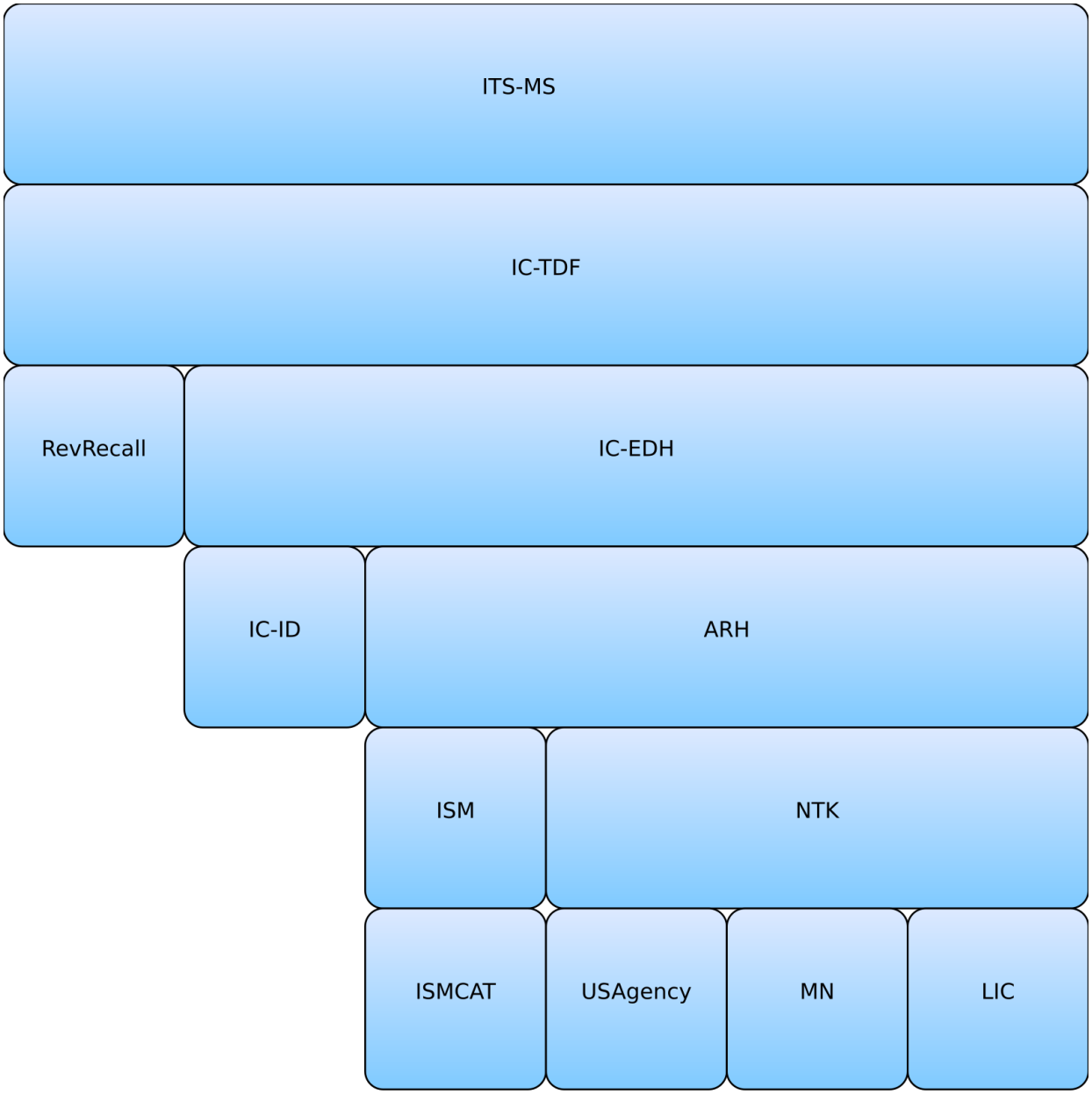

Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions of all transitive dependent specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained.

These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumeration (CVE) to validate and operate as intended.

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

1.8 - Conformance

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

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

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron[18] rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[13] 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.[20] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion**='9' to **@ism:DESVersion**='10' in the xsd:schema statement. The ability to import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications such as ISM CVE updates. The decoupling of dependency versions is not retroactive; see the dependency table for allowed dependency versions.

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

Chapter 2 - Development Guidance

2.1 - Relationship to Abstract Data Definition and other encodings

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

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

2.2 - Additional Guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations for which there is not clearly a single method of encoding the data are documented here. The content of this section will evolve over time as additional situations are identified. Implementers of this DES are encouraged to contact the maintainers of this DES for further guidance when necessary.

2.2.1 - Information Transport Service Messaging Service Usage

ITS-MS.XML is used in conjunction with the Trusted Data Format and consists of structured assertions that contain information required for generating an ITS-OM compliant instance. A Trusted Data Object or Trusted Data Collection conforms to the ITS-MS specification when it contains:

- A structured assertion of scope TDO or TDC with an **Its** element.
- A payload that is the message contents.
- 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** element.

2.2.2.1 - Its Element

The **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">
              ...
        </its:Its>
     </StructuredStatement>
  </Assertion>
```

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

The Trusted Data Objects and Trusted Data Collections adhere to the IC Trusted Data Format XML specification. The metadata required by the ITS Audit Client is contained in the structured statement of an ITS assertion within the TDO or TDC, and this metadata adheres to the ITS-MS.XML schema.

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

- its:**ObjectType** – is required to identify the type of message object. All ITS Audit files must be listed as “AUDIT” or “ACINT”.
- its:**Originator** – identifies the originating ITS Audit client and also includes the CreateDateTime.
- its:**RecipientList** - contains the ClientID for the receiving ITS Audit client.
- 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** – uses a CVE (CVEnumITSMSFabric) to set value to “EA-SCI” or “ACINT”.

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

- its:**MessageId** – the ITS Audit Client will replace this element with a valid universal unique identifier (UUID).
- its:**Priority** – set to **ROUTINE** for Audit objects.

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

2.2.3.1 - Required ISM.XML Attributes

The following are required ISM XML attributes for Message Elements. This XML uses the IC XML Data Encoding Specification for Information Security Marking (ISM.XML) attributes to provide security markings for the information. ITS Client developers should refer to the XML Data Encoding Specification for Information Security Marking Technical Specification for an explanation of the relationships of the ISM.XML attributes and the associated controlled vocabularies. The IC Markings System Register and Manual provides additional business rules (that may be classified) not provided in this schema or the associated documentation.

- **ownerProducer** – must be set to “USA”
- **resourceElement** – must be set to “true”
- **createDate** – must be set to creation date with the following format: [YYYY-MM-DD] (e.g., “2012-06-15”)
- **classification** – must be set to a value which follows the ISM.XML schema **Note - the ITS Audit Client will fail the processing of any message that does not contain a classification value based upon the IC_ISM schema. The receiving organization must also be authorized to receive data at the level identified by the classification value. The ITS Audit Client does not check for "dirty words" and assumes that the sender has classified the message correctly.

2.2.3.2 - ITS Assertion Scope

If the file being sent is a TDC, then the TDC must contain one and only one ITS 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 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].

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

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

3.2 - "Living" Constraint Rules

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

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

3.3 - Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the encoding specification artifacts wherever they are located.

3.4 - Terminology

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

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

3.5 - Errors and Warnings

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

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

3.6 - Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are “for official use only.”(FOUO) IDs from 20001 to 30000 are reserved for “Secret” rules and 30001 and above for more classified rules. ITS-MS.XML data validation constraint rule IDs are prefixed with “ITS-MS-ID-”.

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

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

The 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[18] 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[18] rules for this specification may be executed in *Oxygen®* [17] or with an XSLT 2.0[22]-compliant processor using the XSLT 2.0[22] 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[21] and XSLT 2.0[22] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:[15]

> 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[22] implementation of Schematron[18] 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.

3.7.5 - Value Enumeration Constraints

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

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

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

[1] “White space” is defined in XML 1.0[19] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

3.7.6 - Additional Constraints

3.7.6.1 - DES Constraints

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

3.7.7 - Constraint Rules

The detailed constraint rules for the 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 SchematronGuide.

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 passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

4.1 - Schema Validation

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

4.2 - Business Rule Validation

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

Chapter 5 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the ITS-MS.XML schema can be found as a collection of HTML files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the 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 DES.

Table 3 - ITS-MS.XML Dependency over time

Dependent DES	V1
IC-TDF	V1+
ISM	V9+
NTK	V7+
ARH	V1+
IC-EDH	V1+

The following table summarizes major features by version for ITS-MS.XML.

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)
Cell Colors represent the same information as the Key value	

A.1. ITS-MS Feature Summary

Table 5 - ITS-MS Feature Comparison

ITS-MS Feature Comparison			
Required date	Feature	V1	V2015-FEB
	Express Recipient information	F	F
	Express Sender information	F	F
	IC-ID	F	N
	UUID Version 4	N	F

Appendix B Change History

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

Table 6 - 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.1 - V2015-FEB Change Summary.

B.1 - V2015-FEB Change Summary

Significant drivers for Version 2015-FEB include:

- Alignment with system implementations of ITS-MS.

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

Table 7 - Data Encoding Specification 2015-FEB Change Summary

Change	Artifacts changed	Compatibility Notes
Changed `MessageId` 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 `DESVersion` attribute required.	Schema	No impact to systems that already specified the `DESVersion` attribute. Data generation and ingestion systems that did not fill out the `DESVersion` attribute need to be updated to handle this schema change.
Added ACINT as another possible value for the type of message object defined by the `ObjectType` element.	CVE	Data generation and ingestion systems need to be updated to handle this CVE change.
Added ACINT as another possible value for the originating network defined by the `Fabric` 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
ARH	Access Rights and Handling
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EDH	Enterprise Data Header
FOUO	For Official Use Only
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
IC-ID	IC Identifier
ICD	Intelligence Community Directive
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Transport Service
ITS-MS	Information Transport Service Messaging Service
ITS-OM	Information Transport Service Organizational Messaging

NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PDF	Portable Document Format
PUBS	Intelligence Publications
RFC	Request for Comments
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
UUID	Universal Unique Identifier
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

Bibliography

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

[2] AUDIT.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Audit Exchange (AUDIT.XML)*.
Available online Intelink-TS at:http://go.ic.gov/mCNQV5X
Available online Intelink-U at:http://purl.org/IC/Standards/AUDIT

[3] IC ITE INC1 IMPL
Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at:http://go.ic.gov/HvBHBmY

[4] IC-EDH.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Data Header (IC-EDH.XML)*.
Available online Intelink-TS at:http://go.ic.gov/TQjVx3d
Available online Intelink-U at:http://purl.org/IC/Standards/EDH
Available online at:http://purl.org/IC/Standards/public

[5] IC-TDF.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (TDF.XML)*.
Available online Intelink-TS at:http://go.ic.gov/sonBSai
Available online Intelink-U at:http://purl.org/IC/Standards/TDF
Available online at:http://purl.org/IC/Standards/public

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

[7] 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:http://www.dni.gov/files/documents/ICD/ICD_502.pdf

[8] ICD 503

Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*. Intelligence Community Directive 503. 15 September 2008.
Available online Intelink-TS at:http://go.ic.gov/b1ZONju
Available online at:http://www.dni.gov/files/documents/ICD/ICD_503.pdf

[9] ICPG 710.1
Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at:http://go.ic.gov/yAqVQ0H

[10] ICS 500-20
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.
Available online Intelink-TS at: http://go.ic.gov/sLKNq3N
Available online Intelink-U at: http://www.purl.org/ic/standards/policy/ICS500-20

[11] ICS 500-21
Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online Intelink-TS at: http://go.ic.gov/cWyv9nw
Available online Intelink-U at: http://www.purl.org/ic/standards/policy/ICS500-21

[12] 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: http://go.ic.gov/5yamXTu

[13] 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

[14] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.
Available online Intelink-TS at:http://go.ic.gov/3oipfOY
Available online Intelink-U at:http://purl.org/IC/Standards/ISM
Available online at:http://purl.org/IC/Standards/public

[15] Jelliffe
Richard Alan Jelliffe. *FAQ*. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?.
Available online at: http://www.schematron.com

[16] 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:http://go.ic.gov/YLXsYUX
Available online Intelink-U at:http://purl.org/IC/Standards/NTK
Available online at:http://purl.org/IC/Standards/public

[17] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. Version 14.1.
Available online at:http://www.oxygenxml.com/

[18] 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/

[19] 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

[20] 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

[21] 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/

[22] XSLT2
World Wide Web Consortium (W3C). *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.
Available online at:http://www.w3.org/TR/xslt20/

Appendix E Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

Public Website: http://purl.org/ic/standards/public

E-mail: ic-standards-support@ugov.gov [mailto:ic-standards-support@ugov.gov].

Appendix F IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

Specification artifacts display a date representing the last time a version's artifacts as a whole were modified. This date most often represents the conclusion of the IC Element collaboration and coordination process. Once the IC Element coordination process is complete, the specification goes through an internal OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.[10]