



Intelligence Community Technical Specification

XML Data Encoding Specification for Information Transport Service Organizational Messaging

Version 2015-AUG

August 13, 2015

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	3
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.6.3 - Terminology	3
1.7 - Dependencies	4
1.7.1 - Standalone and Convenience Packages	7
1.8 - Conformance	7
Chapter 2 - Development Guidance	8
2.1 - Relationship to Abstract Data Definition and other encodings	8
2.2 - Additional Guidance	8
2.2.1 - Specification for the use of the Special Handling Element	8
2.2.1.1 - HandlingPhrase Element	9
2.2.1.2 - MessageInstruction Element	9
2.2.1.3 - OrgMessageType Element	9
2.2.1.4 - OrgMsgNotice Element	10
2.2.2 - Specification for the use of the Body Element	10
2.2.2.1 - OrgMessageType Element	10
Chapter 3 - Definitions, Interfaces, and Constraints	12
3.1 - Constraint Rule Types	12
3.2 - “Living” Constraint Rules	12
3.3 - Classified or Controlled Constraint Rules	12
3.4 - Constraint Terminology	12
3.5 - Errors and Warnings	13
3.6 - Rule Identifiers	13
3.7 - Data Validation Constraint Rules	13
3.7.1 - Purpose	13
3.7.2 - Schematron	13
3.7.3 - Non-null Constraints	14
3.7.4 - Inherited Constraints	14
3.7.5 - Value Enumeration Constraints	14
3.7.6 - Additional Constraints	15
3.7.6.1 - Additional Constraint 1 (e.g., Date/Time)	15
3.7.6.2 - Additional Constraint 2 (e.g., ISM)	15
3.8 - Data Rendering Constraint Rules	15
3.8.1 - Purpose	15
3.8.2 - Rendering Constraint Rules	15
Chapter 4 - Conformance Validation	16
4.1 - Schema Validation	16
4.2 - Business Rule Validation	16
Chapter 5 - Generated Guides	17

5.1 - Schema Guide	17
5.2 - Schematron Guide	18
Appendix A - Feature Summary	19
A.1 - ITS-OM Feature Summary	19
Appendix B - Change History	20
B.1 - V2015-AUG Change Summary	20
B.2 - V2 Change Summary	20
Appendix C - IC Messaging Service XML	22
C.1 - Forward Element	22
C.1.1 - ICMS Forward Element - DateTime	23
C.1.2 - Forward Element - Icmsgid	23
C.1.3 - Forward Element - Reason	23
C.1.4 - Forward Element - PrecedenceList	23
C.1.5 - Forward Element - Originator	24
C.1.6 - Forward Element - RecipientList	24
C.1.7 - Forward Element - PreviousForward	24
C.2 - Message Element	24
C.2.1 - Message Element Attribute Group ResourceNodeAttributeGroup	26
C.2.2 - Message Element - Icmsgid	26
C.2.3 - Message Element - Icmsgid	26
C.2.4 - Message Element - OrigMsgid	26
C.2.5 - Message Element - OriginatorDateAssigned	26
C.2.6 - Message Element - AddressSpace	26
C.2.7 - Message Element - Topic	26
C.2.8 - Message Element - PrecedenceList	27
C.2.9 - Message Element - Originator	27
C.2.10 - Message Element - RecipientList	28
C.2.11 - Message Element - SpecialHandling	30
C.2.12 - Message Element - Subject	31
C.2.13 - Message Element - BodyList	31
C.2.14 - Message Element - AttachmentList	32
Appendix D - List of Abbreviations	34
Appendix E - Bibliography	36
Appendix F - Points of Contact	40
Appendix G - IC CIO Approval Memo	41

List of Figures

Figure 1 - Related Specifications	6
Figure 2 - ICMS Schema	22
Figure 3 - ICMS Forward Element	23
Figure 4 - ICMS Message Element	25
Figure 5 - ICMS PrecedenceList Element	27
Figure 6 - ICMS Originator Element	28
Figure 7 - ICMS RecipientList Element	30
Figure 8 - ICMS SpecialHandling Element	31
Figure 9 - ICMS Body Element	32
Figure 10 - ICMS AttachmentList Element	33

List of Tables

Table 1 - Dependencies	4
Table 2 - Constraint Rules	15
Table 3 - ITS-OM Dependency over Time	19
Table 4 - Feature Summary Legend	19
Table 5 - ITS-OM Feature Comparison	19
Table 6 - DES Version Identifier History	20
Table 7 - Data Encoding Specification V2015-AUG Change Summary	20
Table 8 - Data Encoding Specification V2 Change Summary	20

Chapter 1 - Introduction

1.1 - Purpose

This XML Data Encoding Specification for Information Transport Service Organizational Messaging ITS/OM defines detailed implementation guidance for using Extensible Markup Language (XML) to encode ITS/OM 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/OM data concepts using XML.

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 IC Messaging Service (ICMS) XML provides the base XML elements used to define an information object allowed to be transported via ITS/OM. This XML uses the IC standard for Information Security Marking (ISM) V5 XML attributes to provide security markings for the information.

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* ^[4] 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* ^[10] the extensive and consistent use of Extensible Markup Language (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 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

The ITS-OM provides the IC with a common set of services, architectural infrastructure, operating environment, and maintenance support to seamlessly transport information across IC-unique domains and via cross-domain systems, to other domains such as the DoD and other U.S. government agencies.

The creation of this XML standard provides a common programming schema for the IC messaging community. The extensive and consistent use of XML will improve data discovery, data sharing, and system interoperability.

Benefits for ITS:

- By creating one XML standard we are promoting interoperability among IC members (ITS customers) and assuring them of supporting best practices, superior quality and performance.
- Widespread acceptance will ensure the rapid dissemination of updates and innovation.

Benefits for Customers (IC Members):

- By adopting these standards customers reduce risks of failure, costs for development and implementation.
- Because they are tested and verified, they stand for quality and performance.

Implementing a standard XML makes all future organizational messaging products compatible across and within the IC organizations.

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^[1]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[4]
- 200 Series:

- Intelligence Community Directive (ICD) 208, Write for Maximum Utility^[2]
- Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination^[3]
- Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide^[8]

1.5 - Audience and Applicability

DESS are intended primarily 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*,^[9] 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.^[14] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.6.3 - Terminology

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

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

1.7 - 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
<i>Intelligence Community Information Transport Service Organizational Messaging Interface Control Document Appendix A, IC Messaging Service XML Schema Version 1.9</i> ^[5]	Related Specification
<i>Intelligence Community Information Transport Service Organizational Messaging Interface Control Document Appendix B, IC Organizational Messaging XML Version 1.4</i> ^[6]	Related Specification
<i>XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V2014-DEC)</i> ^[22]	Depends on Information Security Markings (ISM). Starting with ISM v2015-AUG, the version of ISM imported is no longer normative.

Name	Dependency Description
Schematron ^[25]	<p>Schematron — ISO/IEC 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use XSLT 2.0^[29] query binding.</p>
<p>XSLT 2.0^[29] implementation of Schematron^[25] by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>

ITS-OM

ISM

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 enumerations (CVEs) 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

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron^[25] 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^[14] 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.^[27] 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 - Specification for the use of the Special Handling Element

The ICMS XML element **SpecialHandling** provides the capability to include additional XML elements using another schema. For the exchange of organizational messages, an additional schema containing these elements is available to ITS/OM Clients. The IC Organizational Messaging schema includes elements such as the following:

- **HandlingPhrase**
- **MessageInstruction**
- **OrgMessageType**
- **OrgMsgNotic.**
- **OrgMsgType**

The ICMS **SpecialHandling** element is unbounded, thus an ICMS XML may include multiple IC Organizational Messaging elements. It is obligatory for the originating client's sponsoring agency to coordinate with the recipient clients' sponsoring agencies on the specifics of the XML schema and the function of the information placed into a **SpecialHandling** element.

2.2.1.1 - HandlingPhrase Element

The **HandlingPhrase** element is a text element which can be used by the originating ITS/OM Client to provide additional security handling text used in organizational messaging that is not provided in the ISM attributes. This element may indicate any security handling conditions which have been agreed to between the message originator and its receiver(s). Multiple handling phrase values can be placed into a single **HandlingPhrase** element or multiple **SpecialHandling** elements with each individual **HandlingPhrase** can be used.

2.2.1.2 - MessageInstruction Element

The **MessageInstruction** element is an enumeration element which can be used by an originating ITS/OM Client to provide additional message delivery handling instructions for the associated message. Multiple **SpecialHandling** elements each containing a single **MessageInstruction** element may be used when multiple message delivery handling information selections are required. The **MessageInstruction** element contains:

- **MsgInst**: An enumeration for the various message instruction choices:
 - NIGHT_ACTION – This selection should only be used with Immediate precedence messages. It is used to indicate the message is of such importance that action offices should be informed of its arrival no matter the time of day.
 - ALARM_REQUIRED – This selection is used to indicate an alarm should be raised within the communications center upon receipt of this message.
 - REPLY_REQUESTED – This selection is used to indicate each Action recipient of the message should respond with a reply message.
 - PASS_TO – This selection is used to indicate delivery passing instructions. When used, the originator should provide the specific passing instructions in the PassToText element.
- **PassToText**: A string containing the text associated with the PASS_TO choice.

2.2.1.3 - OrgMessageType Element

The **OrgMessageType** element can be used by an originating ITS/OM Client to provide metadata about the type of organizational message included in the ICMS XML. Only one (1) **OrgMessageType** element should be used. The **OrgMessageType** element contains an enumeration of the various organizational message types:

- ORGANIZATIONAL – This selection is used to indicate the standard organizational message. This is the presumed type of message when the OrgMessageType element is not included in ICMS XML.
- EXERCISE – This selection is used to indicate an “Exercise” message.
- PROJECT – This selection is used to indicate a “Project” message.
- DRILL – This selection is used to indicate a “Drill” message.

- **SERVICE** – This selection is used to indicate a “Service” message. Service messages are typically disseminated within the messaging operations staff but not the general population of the agency’s organizational messaging community.

2.2.1.4 - OrgMsgNotice Element

The **OrgMsgNotice** element can be used by the originating ITS/OM Client to provide notice text appropriate for the message’s contents. This element includes the ISM attribute, **NoticeAttributesOptionGroup**, which allows the originator to provide the security marking attributes appropriate for the associated notice text.

Multiple **SpecialHandling** elements each containing a single **OrgMsgNotice** element may be used when multiple notices are needed.

2.2.2 - Specification for the use of the Body Element

The ICMS XML element **Body** provides the capability to include additional XML elements using another schema. For the exchange of organizational messages, an additional schema containing these elements is available to ITS/OM Clients. The IC Organizational Messaging schema includes elements such as the **ItsOrgMsg** element.

2.2.2.1 - OrgMessageType Element

The **ItsOrgMsg** element can be used within the **Body** element to transport messages primarily consisting of text. The **ItsOrgMsg** schema contains three elements:

1. **Text**: This element is required. It contains the ASCII representation of the textual information.
1. **Mime**: This element is optional. It may contain the textual information as rich text by representing it as a “text/html” media type with embedded objects.
1. **Structured**: This element is optional and is of type xs:any. It can contain a XML formatted representation of the data. It is incumbent upon the originating client’s sponsoring agency to coordinate with the receiving clients’ sponsoring agencies the specifics of the XML schema if use of this structured data is to be expected.

Every ITS/OM Client should at a minimum be able to originate and receive textual-based organizational messages using the **ItsOrgMsg** element. In addition, any ITS/OM Client intending to support rich text content, should be able to create and display the **Mime** element.

If included, the **ItsOrgMsg/Mime** element should contain MIME encoded content (per RFC 2045^[11]) represented as a “text/html” media type (per RFC 2854^[16]) using the HTML 4.01 specification. Any embedded objects within the HTML should be locally referenced within the MIME content (see RFC 2557^[15]). The resulting MIME entity should then be base64 encoded after optionally being compressed using ZIP. The attribute, **composition**, identifies which method was used to encode the data. The **composition** attribute should contain “base64” or “zip:base64”.

An ITS client may originate any HTML defined within the specification, except for any active content, such as script or object tags. A minimum set of HTML should be recognized by a

consuming ITS client. This minimum set is also the only HTML allowed to cross a security domain. Within a single security domain other HTML content is allowed as long as the originating client and receiving client are in agreement on the handling of the information. The minimum HTML includes support for text in various fonts, colors, styles and effects and embedded static images. The static image types allowed are:

- **image/gif**: GIF extension (see RFC 2045,^[11] RFC 2046^[12])
- **image/jpeg**: JPG, JPEG, JPE extension (see RFC 2045,^[11] RFC 2046^[12])
- **image/png**: PNG extension (see RFC 2083^[13])

The HTML should include at a minimum the <html></html> and <body></body> tags and the default character set is expected to be UTF-8.

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 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-OM.XML data validation constraint rule IDs are prefixed with “ITS-OM-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-OM.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^[25] 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^[25] rules for this specification may be executed in *Oxygen*[®]^[24] or with an XSLT 2.0^[29]-compliant processor using the XSLT 2.0^[29] 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^[28] and XSLT 2.0^[29] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:^[23]

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^[29] implementation of Schematron^[25] 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-OM.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-OM.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.

¹“White space” is defined in XML 1.0^[26] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

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

3.7.6 - Additional Constraints

This section provides additional constraints.

3.7.6.1 - Additional Constraint 1 (e.g., Date/Time)

All Date and Time elements within ITS/OM must specify a time zone of ZULU or Greenwich Mean Time (GMT).

3.7.6.2 - Additional Constraint 2 (e.g., ISM)

This XML uses the IC standard for Information Security Marking (ISM.XML)^[22] attributes to provide security markings for the information.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of ITS-OM.XML documents. The intent is to inform the development of systems capable of rendering or displaying ITS-OM.XML data for use by individuals not familiar with the details of the ITS-OM.XML markup. While expressed in a similar manner to the data validation constraint rules above, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

3.8.2 - Rendering Constraint Rules

The following table contains the information for the ITS-OM.XML data rendering constraint rules.

Table 2 - Constraint Rules

Rule Number	Severity	Description	Human Readable Description
There are no Data Rendering Constraint rules at this time.			

Chapter 4 - Conformance Validation

An instance document conforms with this specification if it 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.

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-OM.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-OM.XML schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen@*, [\[24\]](#) produced by SyncRO Soft.

The guide provides an interactive index to:

- Global Elements and Attributes
- Local Elements and Attributes
- Simple and Complex Types
- Groups and Attribute Groups
- Referenced Schemas

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of the master HTML file *SchemaGuide.html* with supporting graphics.

5.2 - Schematron Guide

The detailed description and reference documentation for the ITS-OM.XML Schematron rules can be found in a separate document named *ITS-OM_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-OM on other specifications.

Table 3 - ITS-OM Dependency over Time

Dependent DES	V1	V2	V2015-AUG
ISM	V10	V10+	V2014-DEC+

The following table summarizes major features by version for this ITS-OM and all dependent specs.

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-OM Feature Summary

Table 5 - ITS-OM Feature Comparison

ITS-OM Feature Comparison				
Required date	Feature	V1	V2	V2015-AUG
	Supports multiple versions of ISM.XML	N	F	F
	Require UUID for Identifier	N	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	17 July 2012	Initial Release
2	21 January 2013	Routine revision to technical specification. For details of changes, see Section B.2 - V2 Change Summary
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.1 - V2015-AUG Change Summary

B.1 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Updates associated with IC Messaging Service v1.12

The following table summarizes the changes made to V2 in developing V2015-AUG.

Table 7 - Data Encoding Specification V2015-AUG Change Summary

Change	Artifacts changed	Compatibility Notes
Harmonized specification with IC Messaging Service v1.12	DES	Data generation and ingestion systems need to be updated to handle the updates.

B.2 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V10 drivers

The following table summarizes the changes made to V1 in developing V2.

Table 8 - Data Encoding Specification V2 Change Summary

Change	Artifacts changed	Compatibility Notes
Added a schematron rule to ensure that the version of the imported ISM spec meets the minimum allowed version.	Schematron ITS-OM-ID-00001 Added	Data generation and ingestion systems need to be updated enforce the new rule.

Change	Artifacts changed	Compatibility Notes
Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM v9.	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.

Appendix C IC Messaging Service XML

The IC Messaging Service (ICMS) XML provides the base XML elements used to define an information object allowed to be transported via ITS/OM. This XML uses the IC standard for Information Security Marking (ISM) V5 XML attributes to provide security markings for the information.

ICMS XML root element, **lcms**, contains two major elements:

- The **Forward** element supports the transmission of a message to destination clients not included in the original recipient list.
- The **Message** element provides the message content (including rich text and attachment or other xml objects) and message metadata including a security attribute.

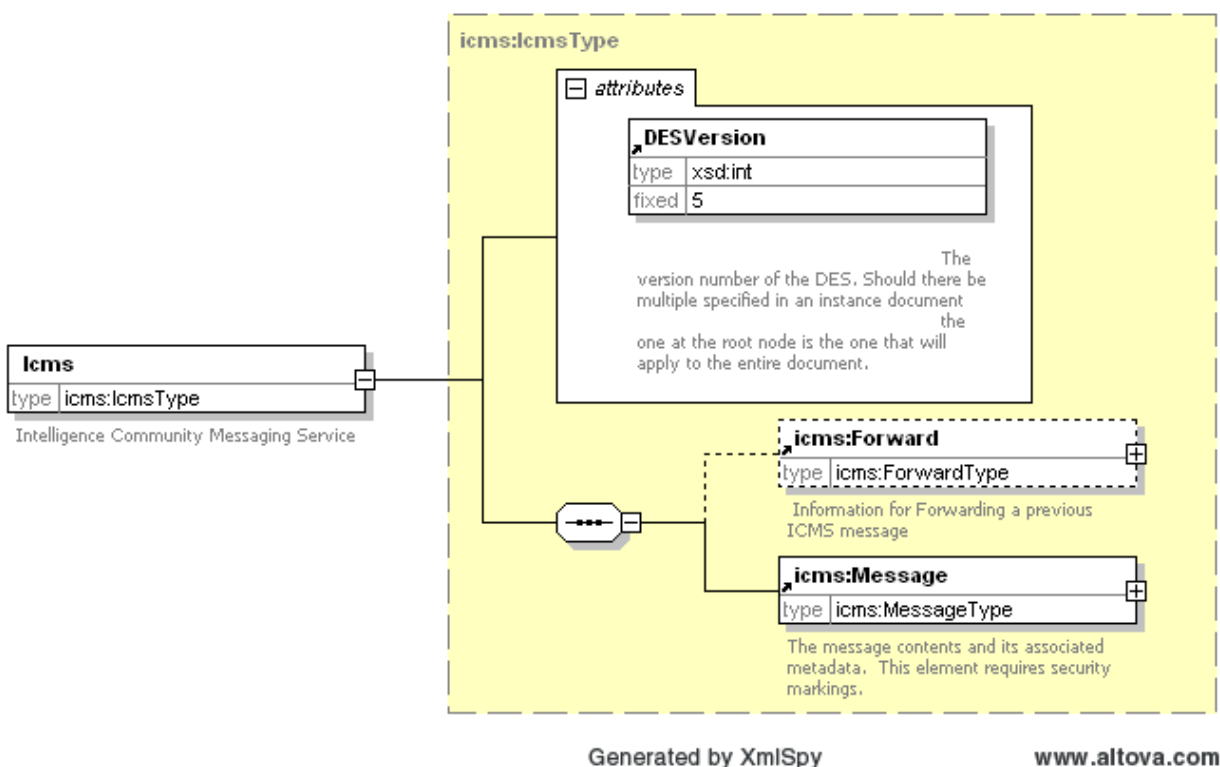


Figure 2 : ICMS Schema

The **lcms** element includes a required attribute from the IC ISM schema, **ISMRootNodeAttributeGroup**.

C.1 - Forward Element

The **Forward** element provides information for a received **lcms/Message** to be forwarded to additional recipients.

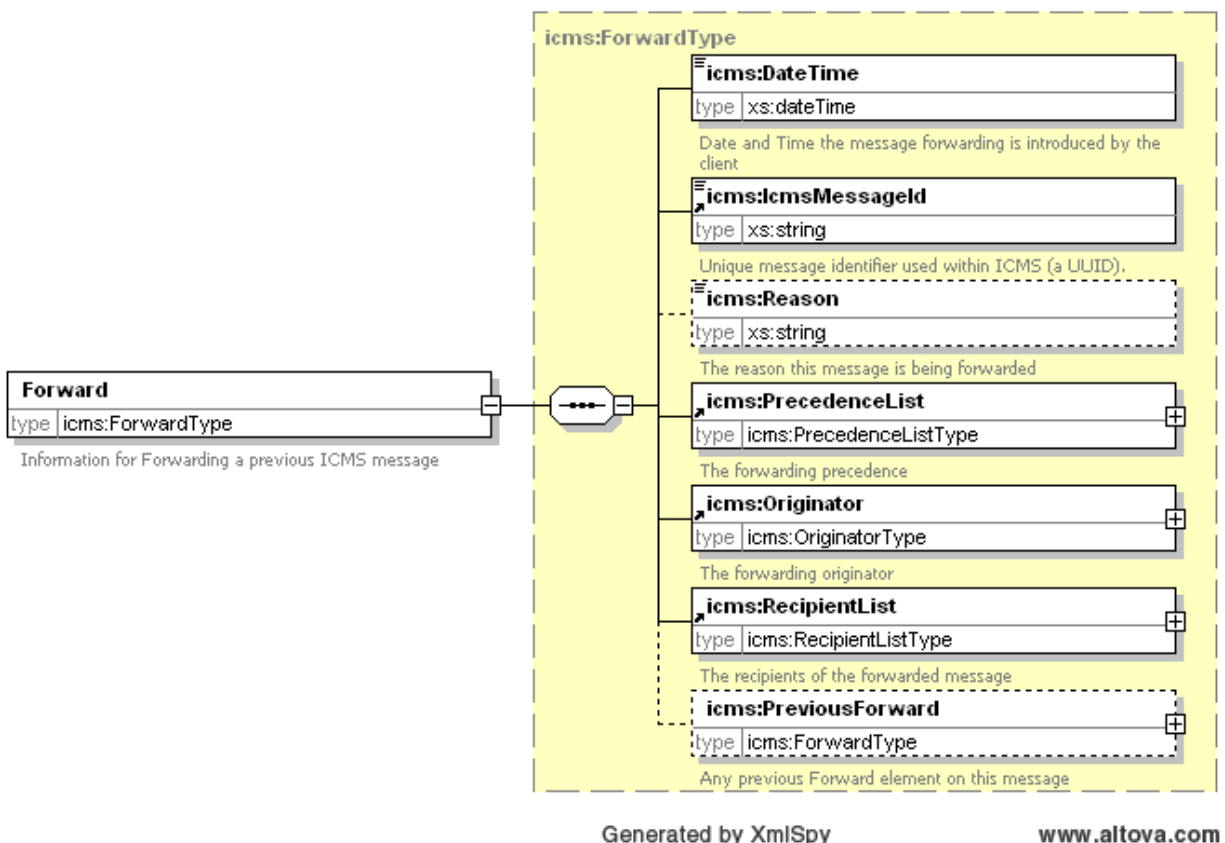


Figure 3 : ICMS Forward Element

C.1.1 - ICMS Forward Element - DateTime

The **DateTime** element should be set to the date and time the ITS Client releases the forwarded message to ITS.

C.1.2 - Forward Element – icmsMessageId

The **icmsMessageId** element is the required UUID assigned when the forwarded message is released. This is the message identifier used throughout the IC ITS to track the message. The UUID should be built as specified in RFC 4122.^[20]

C.1.3 - Forward Element - Reason

The **Reason** element is optional and can be set to a text string explaining the reason this message is being forwarded.

C.1.4 - Forward Element – PrecedenceList

The **PrecedenceList** element provides the precedence values at which the forwarded delivery(s) should be made. This element has the same structure and rules as the **Message.PrecedenceList** element; see [Section C.2.8 - Message Element – PrecedenceList](#) for details.

C.1.5 - Forward Element - Originator

The **Originator** element provides the necessary information about the originator which is performing the forwarding of the message. This element has the same structure and rules as the Message.Originator element; see [Section C.2.9 - Message Element – Originator](#) for details.

C.1.6 - Forward Element - RecipientList

The **RecipientList** element provides the recipients to which the forwarded delivery(s) should be made. When a Forward element is provided on an ICMS message, the IcmsRouting property should include only the client IDs for the recipients of the Forward.RecipientList. This element has the same structure and rules as the Message.RecipientList element; see [Section C.2.10 - Message Element – RecipientList](#) for details.

C.1.7 - Forward Element – PreviousForward

The **PreviousForward** element contains the current forward element when a new forward element is created to forward an **ICMS** message which already has a **Forward** element.

C.2 - Message Element

The Message element provides information about the message including:

- security labels and address space
- identification number, subject, client and originator dates
- originator and recipients
- precedence(s)
- special handling instructions
- content including body and attachments.

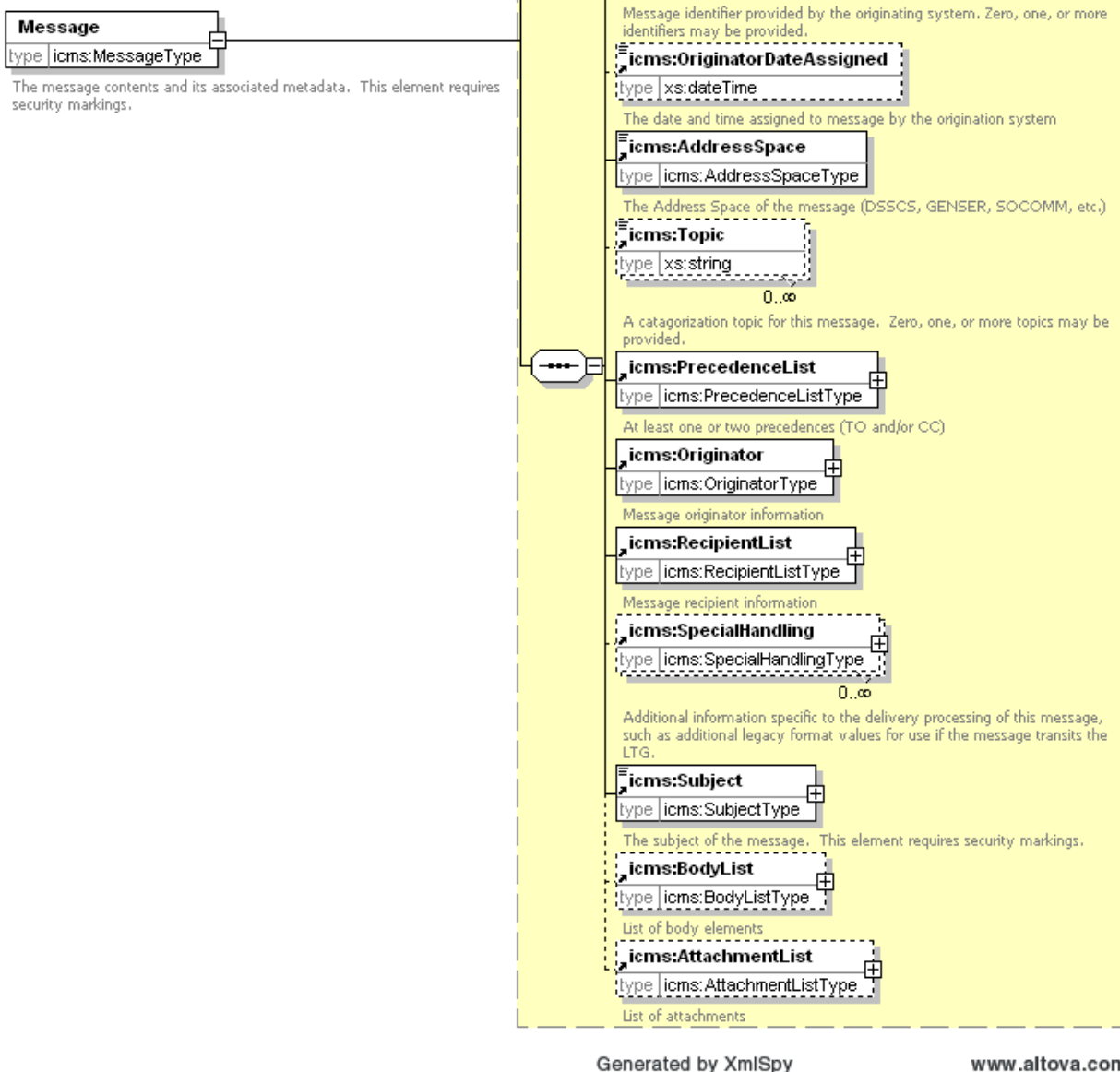


Figure 4 : ICMS Message Element

C.2.1 - Message Element Attribute Group ResourceNodeAttributeGroup

The **Message** element has the IC ISM security attribute group, **ResourceNodeAttributeGroup**, which identifies **Message** as the primary resource element of ICMS XML.

The **Message** element's security attributes are used to provide the organizational message's security markings. This security marking should represent the highest overall classification of the message taking into account any security attributes which exist on the elements for **Subject**, **Body**, and/or **Attachment** elements.

C.2.2 - Message Element – IcmsDateReleased

IcmsDateReleased is a mandatory element of type xs:dateTime. This is the Greenwich Mean Time of the date and time the message was released by the ITS/OM Client.

C.2.3 - Message Element – IcmsMessageld

The **IcmsMessageld** element is the required UUID assigned when the message is released. This is the message identifier used throughout the IC ITS to track the message. The UUID should be built as specified RFC 4122.^[20] Most application development languages have libraries which support the creation of a UUID based on the specific server information and the current date and time.

C.2.4 - Message Element – OrigMessageID

The optional element, **OrigMessageID**, provides a field for an originating client to include a local identifier assigned to the message. It is of type xs:string and multiple elements may be included.

Although optional, ITS/OM Clients are encouraged to provide this information as it is extremely useful for interagency coordination on specific messages.

C.2.5 - Message Element – OriginatorDateAssigned

OriginatorDateAssigned is an optional element of type xs:dateTime. This is the date and time assigned to the message by the originator.

C.2.6 - Message Element – AddressSpace

AddressSpace is a mandatory element of type xs:string. It provides a field for indicating the message's address space. The address space of the originator and all message recipients must match the address space of the message.

C.2.7 - Message Element – Topic

The optional element, **Topic**, provides a field for indicating the general topic of the message. It is of type xs:string and multiple elements may be included. This element is planned for future use.

C.2.8 - Message Element – PrecedenceList

The **PrecedenceList** element is a choice element from which at least one precedence element, either **ToPrecedence** or **CcPrecedence**, must be defined for a message. A **ToPrecedence** is required if any recipient's **OrgType** is **TO**. A **CcPrecedence** is required if any recipient's **OrgType** is **CC**. The **ToPrecedence** and **CcPrecedence** are of the type **PrecedenceType** that have enumerated values of ROUTINE, PRIORITY, IMMEDIATE, FLASH, ECP or CRITIC.

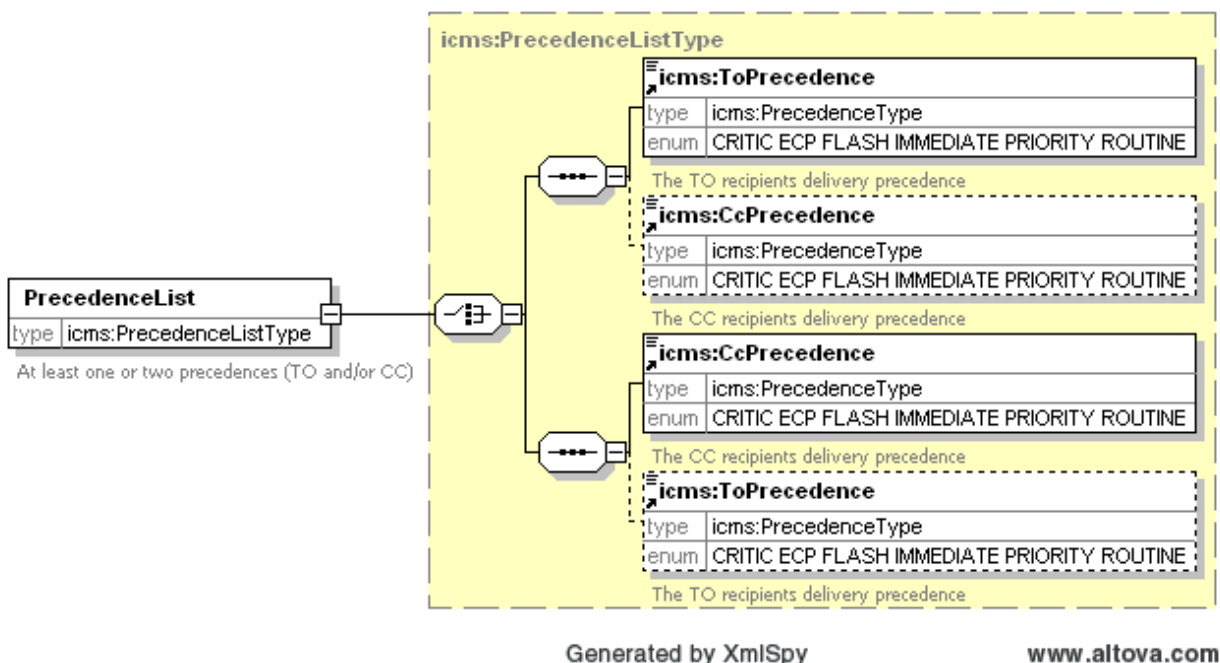


Figure 5 : ICMS PrecedenceList Element

C.2.9 - Message Element – Originator

The required element, **Originator**, is composed of an **OrgName** element and two optional elements: **OfficeCodes** and **ReleaserName**. **OrgName** contains the message originator's organizational address as associated to the message's address space. **OfficeCodes** can be used to identify the office within the associated organization which is originating this message. Typically only one office code would be associated with an originator. **ReleaserName** can be used to include the authorized releaser's name as validated by the client's user interface.

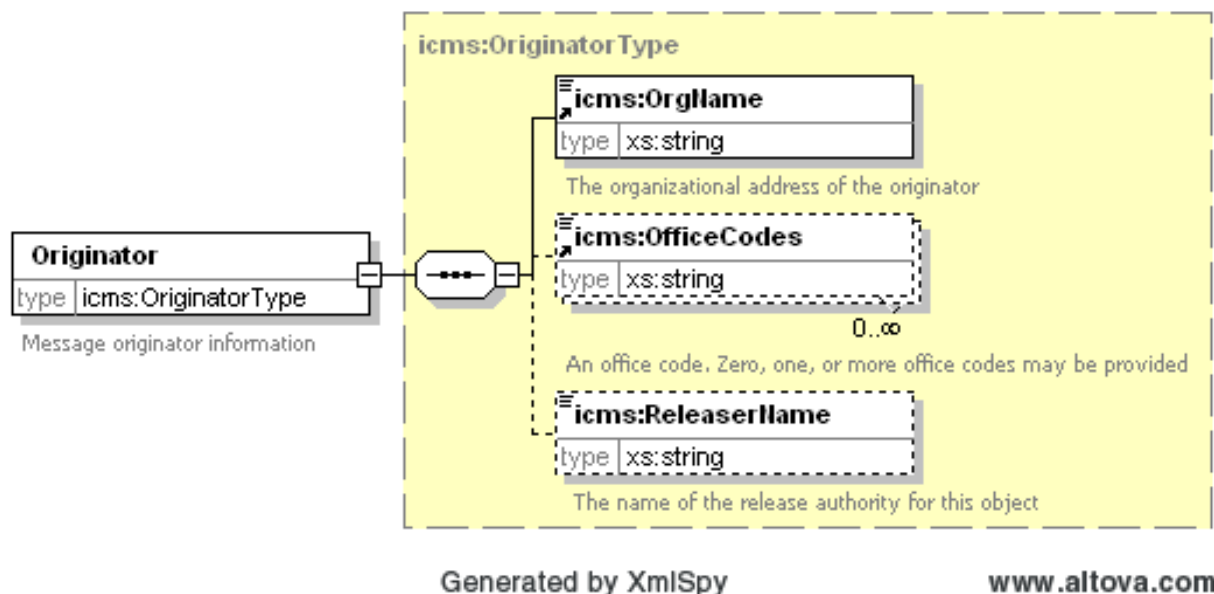


Figure 6 : ICMS Originator Element

C.2.10 - Message Element – RecipientList

The element, **RecipientList**, contains one or more **Recipient** elements. Each **Recipient** element contains the following elements:

- **RecpType**: This element is required and identifies the type of recipient. It is one of TO, CC, EXCLUDE, TO_ZEN, or CC_ZEN. The TO value indicates the recipient should receive a copy at the message's associated action precedence (**Message.PrecedenceList.ToPrecedence**) while the CC value indicates the recipient should receive a copy at the message's associated info precedence (**Message.PrecedenceList.CcPrecedence**). The EXCLUDE value indicates the recipient is a member of a group which should not receive a copy of the message and should only be used when the **OrgType** is GroupMember. The TO_ZEN and CC_ZEN values indicate the recipient should not receive a copy of the message because that copy was delivered to that recipient outside the organizational messaging systems.
- **OrgName**: This element is required and contains the organizational address of the recipient or the address list name for a group of organizational addresses which should receive the message.
- **OfficeCodes**: This element can be used to identify the office within the associated organization which is to receive this message. The element is optional, but may also exist multiple times if multiple offices within the same organization should receive the message.
- **OrgType**: This element is required and indicates the type of organization provided in the **OrgName** element. It is one of PLA, Group, or GroupMember. PLA indicates the value is an individual recipient identified by its plain language address. Group indicates the value is a group name identifying multiple recipients by their membership in the group. GroupMember indicates the value is the plain language address of an address group member.

GroupMember should only be used when the recipient list also includes an **OrgType** of Group.

- **OrgClient**: This element is used to identify the ITS client which provides the delivery path to the recipient. If the **RecpType** is EXCLUDE, TO_ZEN, or CC_ZEN, this element is not necessary since no delivery will be made to this type of recipient. If the **OrgType** is Group, this element is not necessary since deliveries are made to group members and not the group itself. If the **RecpType** is TO or CC and the **OrgType** is PLA or GroupMember, this element if it exists contains the ITS client ID of the client which provides the organization's messaging support. More than one **OrgClient** element may exist if more than one ITS client receives messages for the associated organization.
- **ReceiptRequested**: This element is optional and can be used to indicate to a recipient that the originator requests acknowledge that the message has been read. It is a Boolean element and should be set to true or false.

In addition, the **Recipient** element contains the optional **Dual-Rcv** attribute. This attribute is used to indicate the **Recipient** element is a duplicate entry for use in the dual receive testing process.

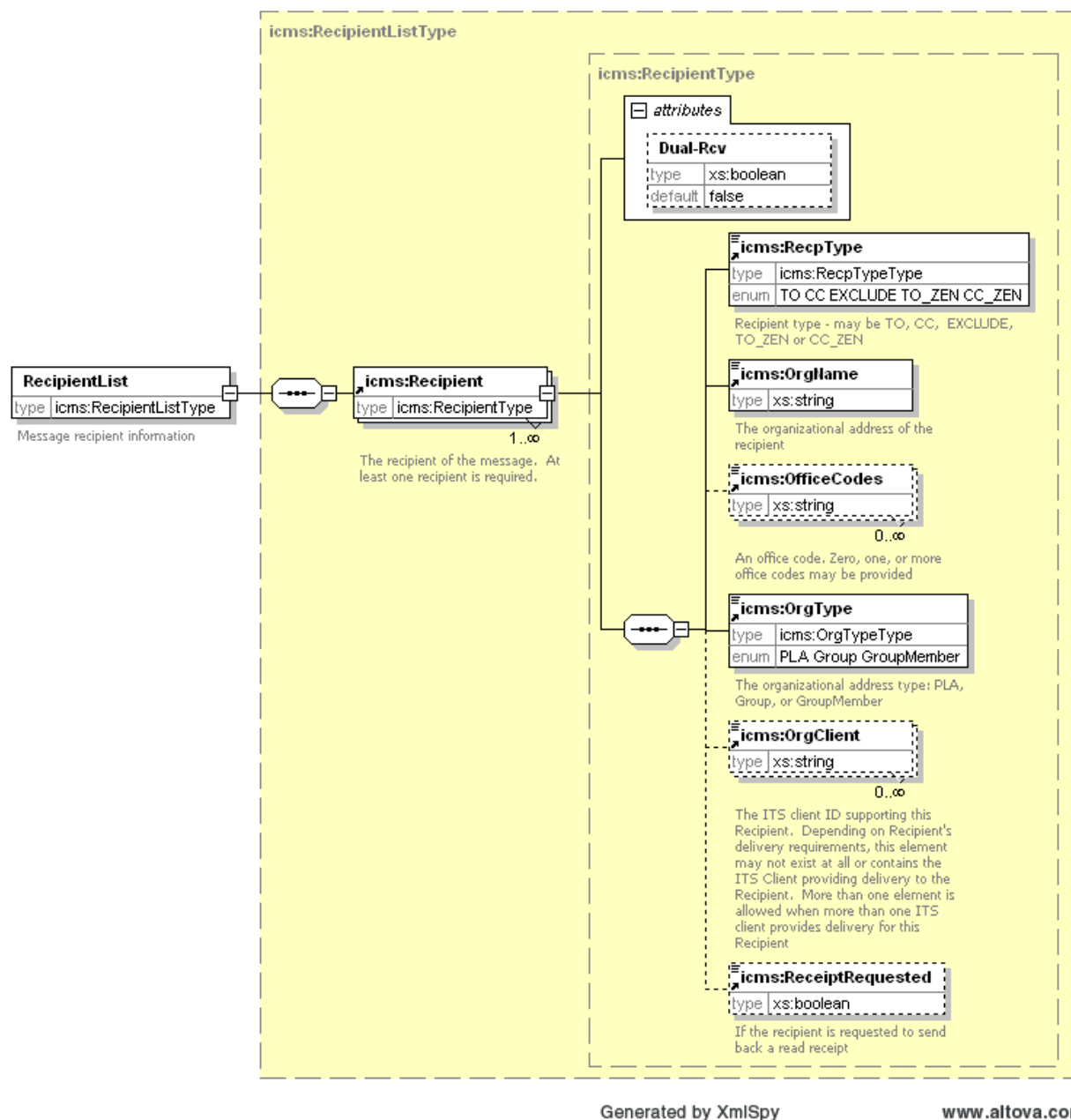


Figure 7 : ICMS RecipientList Element

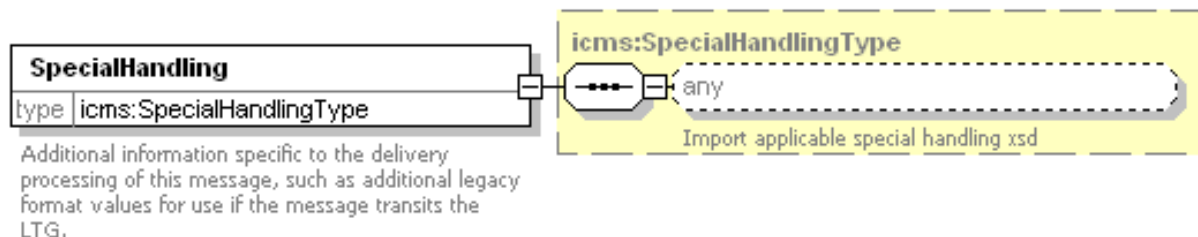
C.2.11 - Message Element – SpecialHandling

The optional element, **SpecialHandling**, provides the capability to send message handling instructions based upon another schema. The **SpecialHandling** element is of type **xs:any**. They include:

- **HandlingPhrase** – used by an originating ITS/OM client to provide addition security marking text not already provided in the ISM attributes.

- **MessageInstruction** – used by an originating ITS/OM client to provide additional message delivery handling information.

Multiple **SpecialHandling** elements can be included in a single message.



Generated by XmlSpy

www.altova.com

Figure 8 : ICMS SpecialHandling Element

C.2.12 - Message Element – Subject

The required element, **Subject**, contains the subject or description of the message content. The **Subject** element has the IC ISM security attribute, **SecurityAttributesOptionGroup**.

C.2.13 - Message Element – BodyList

The **BodyList** element is optional. It contains one or more **Body** elements which constitute the message content. Each **Body** element is of type xs:any and has two optional attributes, **SecurityAttributesOptionGroup** and **title**.

The **SecurityAttributesOptionGroup** attribute is used to provide security markings for the **Body** element.

In general, any XML could be included within the **Body** elements, but it is incumbent upon the originating client's sponsoring agency to coordinate with the receiving client sponsoring agencies the specifics of the XML schemas and use of the information placed into the **Body** elements. For example, if an originator has a document formatted in the IC MSP XML standard, that document could be included as a Body without alteration, as long as all receiving clients have expectation of receiving this structure as a message body.

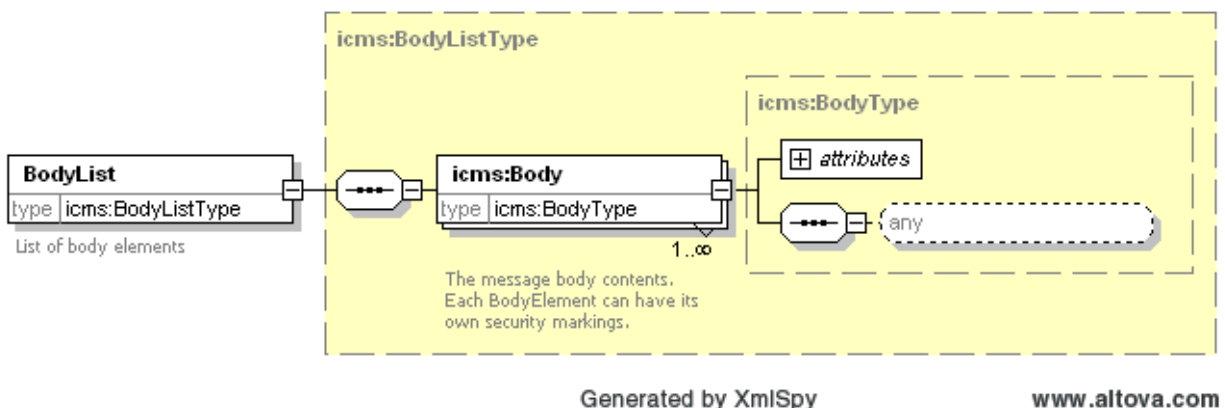


Figure 9 : ICMS Body Element

C.2.14 - Message Element – AttachmentList

The **AttachmentList** element is optional and consists of one or more **Attachment** elements. The **Attachment** element has the optional **SecurityAttributesOptionGroup** attribute group.

Each **Attachment** element consists of the following elements.

- **AttachmentName**: This element contains the name of the attachment along with the mime-type attribute which identifies the content type using the MIME media type values found in RFC 2046.^[12] An ITS client may originate any attachment type defined within the specification. A minimum set of file types should be recognized by a consuming ITS client. This minimum set is also the only file types allowed to cross a security domain. Within a single security domain other file types are allowed as long as the originating client and receiving Client are in agreement on the handling of the attachment. The following types constitute the minimum set:
 - **text/plain**: File has TXT extension (see RFC 2046,^[12] RFC 3676,^[18] and RFC 5147^[21])
 - **text/html**: File with HTML extension (see RFC 2854^[16]). Please see Appendix B for the details of allowable ITS text/html content
 - **text/xml**: File with XML extension (see RFC 3023^[17])
 - **image/gif**: File has GIF extension (see RFC 2045,^[11] RFC 2046^[12])
 - **image/jpeg**: File has JPG, JPEG, JPE extension (see RFC 2045,^[11] RFC 2046^[12])
 - **image/png**: File has PNG extension (see RFC 2083^[13])
 - **application/vnd.ms-excel**: File has XLS extension (Microsoft Excel)
 - **application/vnd.ms-powerpoint**: File has PPT extension (Microsoft PowerPoint)
 - **application/msword**: File has DOC extension (Microsoft Word)

- **application/pdf**: File has PDF extension (see RFC 3778^[19])
- **application/xml**: File has XML extension (see RFC 3023^[17])
- **AttachmentDescription**: This element is optional and may contain a textual description of the attachment contents.
- **AttachmentSize**: This element contains the size in bytes. If the attachment content is included in the element, **AttachmentData**, this represents the size of the attachment after any conversion and compression actions are applied to its contents.
- **AttachmentLocation**: This element can be used to provide the URI of where the attachment can be found. **AttachmentLocation** should not be used when the **AttachmentData** element is used.
- **AttachmentData**: This element can contain the actual data either base64 encoded or zipped and then base64 encoded. The associated attribute, composition, identifies which method was used to encode the data. The composition attribute should contain “base64” or “zip:base64”. **AttachmentData** should not be used when the **AttachmentLocation** element is used.

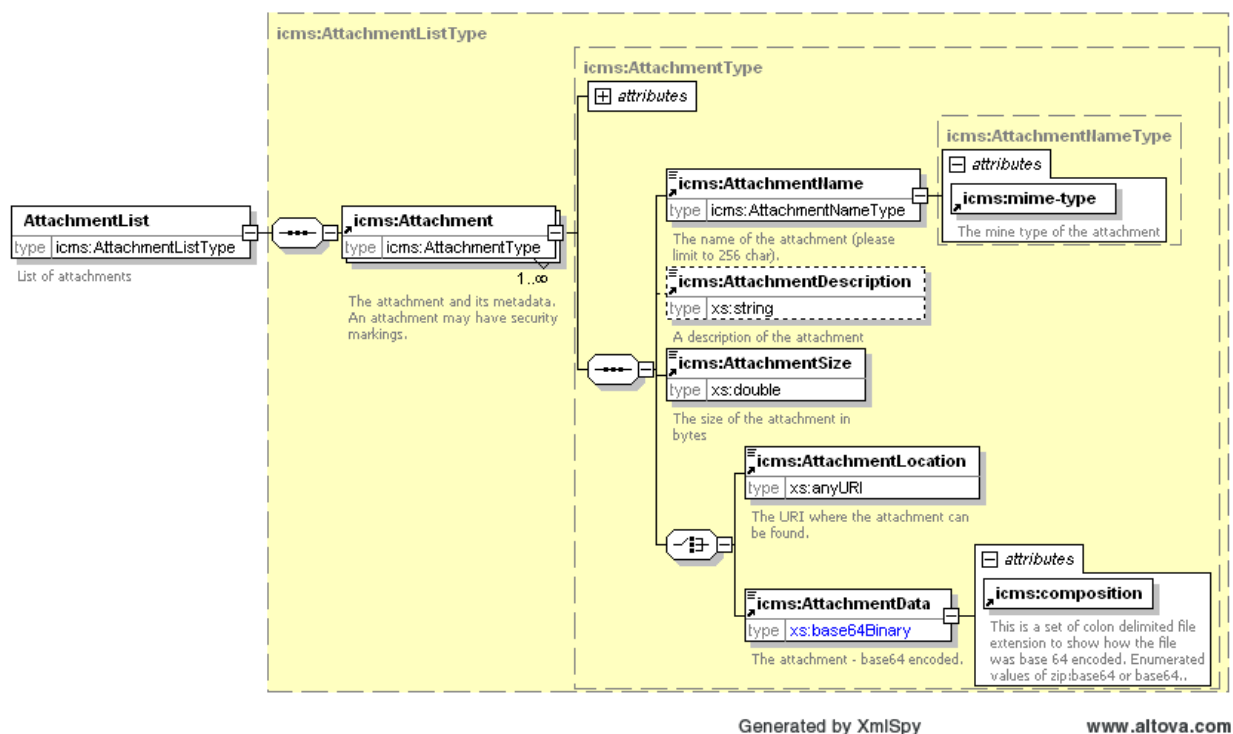


Figure 10 : ICMS AttachmentList Element

Appendix D List of Abbreviations

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

ADD	Abstract Data Definition
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOD	Department of Defense
FOUO	For Official Use Only
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICMS	Intelligence Community Messaging Service
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISM	Information Security Markings
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Transport Service
ITS-OM	Information Transport Service Organizational Messaging
MIME	Multipurpose Internet Mail Extensions
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence

PDF	Portable Document Format
PUBS	Intelligence Publications
TDF	Trusted Data Format
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universal Unique Identifier
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix E Bibliography

Bibliography

[1] 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/4X6TOc1>

[2] ICD 208

Office of the Director of National Intelligence. *Write For Maximum Utility*. Intelligence Community Directive 208. 17 December 2008.

Available online at: http://www.dni.gov/files/documents/ICD/icd_208.pdf

[3] ICD 209

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.

Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf>

[4] 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/5Ot5sbK>

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[5] ICMS

Intelligence Community Information Transport Service Organizational Messaging Interface Control Document. Appendix A IC Messaging Service (ICMS) XML Schema. Version 1.9. 18 April 2011.

[6] ICOM

Intelligence Community Information Transport Service Organizational Messaging Interface Control Document. Appendix B IC Organizational Messaging (ICOM) XML Schema. Version 1.4. 25 August 2011.

[7] ICPG 710.1

Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online Intelink-TS at: <http://go.ic.gov/JztUoEQ>

[8] ICPM 2007-200-2

Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2. 11 December 2007.

Available online at: <http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf>

[9] ICS 500-20

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

Available online Intelink-TS at: <http://go.ic.gov/sLKNq3N>

Available online Intelink-U at: <http://www.purl.org/ic/standards/policy/ICS500-20>

[10] 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>

[11] IETF-RFC 2045

Internet Engineering Task Force. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. November 1996.

Available online at: <http://tools.ietf.org/html/rfc2045>

[12] IETF-RFC 2046

Internet Engineering Task Force. *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*. November 1996.

Available online at: <http://tools.ietf.org/html/rfc2046>

[13] IETF-RFC 2083

Internet Engineering Task Force. *PNG (Portable Network Graphics) Specification Version 1.0*. March 1997.

Available online at: <http://tools.ietf.org/html/rfc2083>

[14] 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>

[15] IETF-RFC 2557

Internet Engineering Task Force. *MIME Encapsulation of Aggregate Documents, such as HTML (MHTML)*. March 1999.

Available online at: <http://tools.ietf.org/html/rfc2557>

[16] IETF-RFC 2854

Internet Engineering Task Force. *The 'text/html' Media type*. June 2000.

Available online at: <http://tools.ietf.org/html/rfc2854>

[17] IETF-RFC 3023

Internet Engineering Task Force. *XML Media Types*. January 2001.

Available online at: <http://www.ietf.org/rfc/rfc3023.txt>

[18] IETF-RFC 3676

Internet Engineering Task Force. *The Text/Plain Format and DelSpParameters*. February 2004.

Available online at: <http://www.ietf.org/rfc/rfc3676.txt>

- [19] IETF-RFC 3778
Internet Engineering Task Force. *The application/pdf Media Type*. May 2004.
Available online at: <http://www.ietf.org/rfc/rfc3778.txt>
- [20] IETF-RFC 4122
Internet Engineering Task Force. *A Universally Unique IDentifier (UUID) URN Namespace*. July 2005.
Available online at: <http://tools.ietf.org/html/rfc4122>
- [21] IETF-RFC 5147
Internet Engineering Task Force. *URI Fragment Identifiers for the text/plain Media Type*. April 2008.
Available online at: <http://www.ietf.org/rfc/rfc5147.txt>
- [22] 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>
- [23] Jelliffe
Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*.
Available online at: <http://www.schematron.com>
- [24] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*.
Available online at: <http://www.oxygenxml.com/>
- [25] 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/>
- [26] 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>
- [27] 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>
- [28] 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/>

[29] 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 F 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 DNI-sponsored web sites.

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

Intelshare: <http://purl.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@ugov.gov.

Appendix G 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.^[9]