



# **Intelligence Community Technical Specification**

---

## **XML Data Encoding Specification for Access Rights and Handling**

### **Version 3**

09 May 2014

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 .....   | 4  |
| 1.7 - Dependencies .....   | 4  |
| 1.8 - Conformance .....  | 6  |
| Chapter 2 - Development Guidance .....                                   | 7  |
| 2.1 - Understanding Access Control .....                                 | 7  |
| 2.2 - Relationship to Abstract Data Definition and other encodings ..... | 8  |
| 2.3 - Additional Guidance .....  | 8  |
| 2.3.1 - Security and ExternalSecurity .....                              | 8  |
| 2.3.2 - Usage of ISM and NTK .....                                       | 8  |
| 2.3.3 - MIME type .....  | 8  |
| Chapter 3 - Definitions, Interfaces, and Constraints .....               | 9  |
| 3.1 - Constraint Rule Types .....  | 9  |
| 3.2 - "Living" Constraint Rules .....                                    | 9  |
| 3.3 - Classified or Controlled Constraint Rules .....                    | 9  |
| 3.4 - Terminology .....  | 9  |
| 3.5 - Errors and Warnings .....  | 10 |
| 3.6 - Rule Identifiers .....   | 10 |
| 3.7 - Data Validation Constraint Rules .....                             | 10 |
| 3.7.1 - Purpose .....  | 10 |
| 3.7.2 - Schematron .....   | 10 |
| 3.7.3 - Non-null Constraints .....                                       | 11 |
| 3.7.4 - Inherited Constraints .....                                      | 11 |
| 3.7.5 - Value Enumeration Constraints .....                              | 11 |
| 3.7.6 - Additional Constraints .....                                     | 12 |
| 3.7.6.1 - DES Constraints .....  | 12 |
| 3.7.7 - Constraint Rules .....   | 12 |
| 3.8 - Data Rendering Constraint Rules .....                              | 12 |
| 3.8.1 - Purpose .....  | 12 |
| 3.8.2 - Rendering Constraint Rules .....                                 | 12 |
| Chapter 4 - Conformance Validation .....                                 | 13 |
| 4.1 - Schema Validation .....  | 13 |
| 4.2 - Business Rule Validation .....                                     | 13 |
| Chapter 5 - Generated Guides .....                                       | 14 |
| 5.1 - Schema Guide .....   | 14 |
| 5.2 - Schematron Guide .....   | 15 |
| Appendix A - Feature Summary .....                                       | 16 |
| A.1 - ARH Feature Summary .....  | 16 |
| Appendix B - Change History .....  | 17 |

|   |    |
|---|----|
| B.1 - V3 Change Summary .....           | 17 |
| B.2 - V2 Change Summary .....           | 17 |
| Appendix C - Glossary .....             | 19 |
| Appendix D - Bibliography .....         | 21 |
| Appendix E - Points of Contact .....    | 24 |
| Appendix F - IC CIO Approval Memo ..... | 25 |

## List of Tables

|   |    |
|---|----|
| Table 1 - Dependencies .....                                  | 4  |
| Table 2 - Constraint Rules .....                              | 12 |
| Table 3 - ARH Dependency over time .....                      | 16 |
| Table 4 - Feature Summary Legend .....                        | 16 |
| Table 5 - ARH Feature Comparison .....                        | 16 |
| Table 6 - DES Version Identifier History .....                | 17 |
| Table 7 - Data Encoding Specification V3 Change Summary ..... | 17 |
| Table 8 - Data Encoding Specification V2 Change Summary ..... | 17 |

## Chapter 1 - Introduction

### 1.1 - Purpose

This *XML Data Encoding Specification for Access Rights and Handling* (ARH.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode ARH 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 ARH 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.

### 1.3 - Background

The IC 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* <sup>[4]</sup> grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture.
- 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* <sup>[10]</sup> 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, for e.g., Microsoft Word, define document properties, styles, fields, cardinalities, processing requirements, and use.

## 1.4 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata (including enterprise data headers) to allow interagency access control, automated exchanges, and appropriate protection of shared intelligence. A structured, verifiable representation of security metadata bound to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions today being performed by human beings.

The Intelligence Community ( IC ) has standardized the various classification and control markings established for information sharing within the Information Security Markings ( ISM ) and Need-To-Know ( NTK ) XML specifications of the Intelligence Community Enterprise Architecture ( ICEA ) Data Standards. The IC Access Requirements and Handling XML specification combines elements of the ISM and NTK specifications and extends them to access rights management and handling needs.

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<sup>[1]</sup>
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer<sup>[4]</sup>
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC<sup>[5]</sup>

- Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information<sup>[10]</sup>
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility<sup>[2]</sup>
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination<sup>[3]</sup>
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide<sup>[8]</sup>
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System<sup>[6]</sup>
  - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control<sup>[7]</sup>

## 1.5 - Audience and Applicability

DES s 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*,<sup>[9]</sup> 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.<sup>[11]</sup> 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 depends on the technical specifications, documentation, and implementations listed in the following table. The dependencies listed below are referenced in this encoding specification, and are normative or informative as indicated in the dependencies table.

**Table 1 - Dependencies**

| Name  | Dependency Description   |
|---|--|
| <i>XML Data Encoding Specification for Information Security Marking (ISM . XML .V12+)</i> <sup>[12]</sup> | Depends on Information Security Markings (ISM ). The version of ISM imported is not normative, but the minimum allowed version is ISM version 12.              |
| <i>XML Data Encoding Specification for Need-To-Know Metadata ( NTK . XML .V7+)</i> <sup>[14]</sup>        | 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. |

| Name   | Dependency Description  |
|--|---|
| Schematron <sup>[16]</sup>   | <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 <b>MUST</b> 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 <b>MAY</b> 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<sup>[20]</sup> query binding.</p> |
| <p>XSLT 2.0<sup>[20]</sup> implementation of Schematron<sup>[16]</sup> 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: <a href="http://code.google.com/p/schematron/">http://code.google.com/p/schematron/</a>.</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 <b>MAY</b> use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator <b>MUST</b> find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>  |
| Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES .  | Specification uses CVE s to encode controlled vocabularies. The use of the ARH CVE s is normative.  |

## 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<sup>[16]</sup> 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<sup>[11]</sup> is considered normative within the scope of the sentence. All other parts of this document are informative.

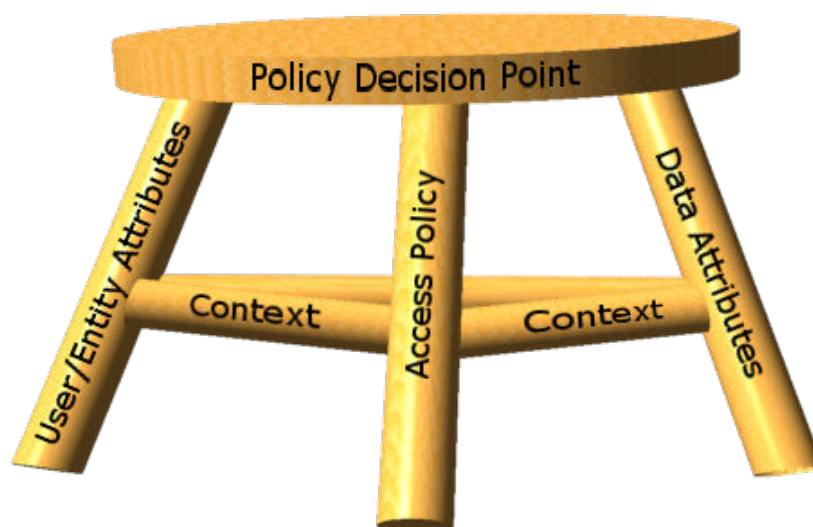
The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.<sup>[18]</sup> 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 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions comprise three components (data attributes, user attributes, and access control policies) and are held together by the context in which the access control decision is made. The context itself includes various elements, such as the environment, temporal state, and method of access, that together provide the Where, When, and How details of the access request. The context, together with the user making the request and the data being requested (the Who and What respectively), make up the framework that supports an access control decision. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. The following is a depiction of the concept of access control decision framework.



All of these parts come together to create a tri-legged stool of access control. When a stool is missing one of the components of its frame, it is unable to function properly. The same is true of access control. Without each component of the framework, access control falls apart. Each component is crucial to make accurate, reliable, and automated access control decisions. Each Enterprise Integration and Architecture (EI&A) document will address a piece of the framework of access control decisions.

This specification addresses matters dealing with data and it falls into the data attributes leg of the access control framework. Data attribute specifications include: Access Rights and Handling (ARH), Information Security Marking (ISM), CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT), Need-To-Know Metadata (NTK), Intelligence Only NTK Profile (ICO-NTK), Originator Control NTK Profile (OC-NTK), and PROPIN Need-To-Know (PROPIN-NTK).

## 2.2 - 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.

## 2.3 - Additional Guidance

### 2.3.1 - Security and ExternalSecurity

The ARH specification defines two root elements, **Security** and **ExternalSecurity**, for expressing the access rights and handling information for a data object.

- The **Security** element reflects ARH for a data object that is either present in the same instance document as **Security** or is the instance document containing the **Security** element.
- The **ExternalSecurity** element reflects ARH for a data object external to the instance document containing the **ExternalSecurity** element. Compared to **Security**, **ExternalSecurity** includes two additional ISM elements to describe its external status, **ism:externalNotice** and **ism:excludeFromRollup**

### 2.3.2 - Usage of ISM and NTK

ISM elements and attributes used in ARH reflect the security markings and notices required for access rights management and handling. The NTK specification is leveraged by ARH to provide a formalized Need To Know of internal and external documents through the utilization of the **ntk:Access** and **ntk:ExternalAccess** elements, respectively.

### 2.3.3 - MIME type

The Multipurpose Internet Mail Extensions ( MIME ) type for a ARH.XML document is application/dni-arh+xml. This is a convention for our community. This type has NOT been registered with the Internet Assigned Numbers Authority ( IANA ). Should there be a conflict in the future it will be addressed at that time. Systems can use this MIME type to facilitate communications and address business needs within the community.

## 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. ARH.XML data validation constraint rule IDs are prefixed with “ARH-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 ARH.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<sup>[16]</sup> 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<sup>[16]</sup> rules for this specification may be executed in *Oxygen*®<sup>[15]</sup> or with an XSLT 2.0<sup>[20]</sup>-compliant processor using the XSLT 2.0<sup>[20]</sup> 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<sup>[19]</sup> and XSLT 2.0<sup>[20]</sup> features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:<sup>[13]</sup>

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<sup>[20]</sup> implementation of Schematron<sup>[16]</sup> 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.<sup>1</sup> Elements, which are allowed to only have text content, must have text content specified.

## 3.7.4 - Inherited Constraints

In an instance of ARH.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 ARH.XML model use Controlled Vocabulary Enumerations ( CVE s) to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE . Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVE s 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 CVE s 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

<sup>1</sup>“White space” is defined in XML 1.0<sup>[17]</sup> as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”



entire CVE is not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

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

## 3.7.6 - Additional Constraints

### 3.7.6.1 - DES Constraints

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

### 3.7.7 - Constraint Rules

The detailed constraint rules for the ARH.XML schema can be found in a separate document inside the SchematronGuide directory, in the ARH\_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 ARH.XML documents. The intent is to inform the development of systems capable of rendering or displaying ARH.XML data for use by individuals not familiar with the details of the ARH.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 ARH.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 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.

## Chapter 5 - Generated Guides

### 5.1 - Schema Guide

The detailed description and reference documentation for the ARH.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 ARH.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 (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 ARH.XML Schematron rules can be found in a separate document named *ARH\_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 ARH on other DES .

Table 3 - ARH Dependency over time

| Dependent DES | V1 | V2     | V3   |
|---------------|----|--------|------|
| ISM           | V9 | V9-V11 | V12+ |
| NTK           | V7 | V7+    | V7+  |

The following table summarizes major features by version for this ARH 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)                             |
| N/A   | Not Applicable. Feature is no longer required.            |
| Cell Colors represent the same information as the Key value |   |

A.1. ARH Feature Summary

Table 5 - ARH Feature Comparison

| ARH Feature Comparison |  |    |    |    |
|------------------------|--|----|----|----|
| Required date          | Feature  | V1 | V2 | V3 |
|                        | Supports multiple versions of ISM . XML (V12 - Current) and NTK . XML (V7 - Current) | N  | F  | 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 <a href="#">Section B.2 - V2 Change Summary</a> |
| 3       | 16 August 2013  | Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V3 Change Summary</a> |

### B.1 - V3 Change Summary

Significant drivers for Version 3 include:

- See ISM V12 drivers

The following table summarizes the changes made to V2 in developing V3.

**Table 7 - Data Encoding Specification V3 Change Summary**

| Change  | Artifacts changed                   | Compatibility Notes  |
|---|-------------------------------------|--|
| Added an optional attribute to declare the CES Version for ISMCAT on the ARH root elements. | Schema                              | Data generation and ingestion systems need to be updated enforce the updated schema. |
| Updated the schematron rules for the minimum allowed version of ISM .                       | Schematron<br>ARH-ID-00004 Modified | Data generation and ingestion systems need to be updated enforce the modified rule.  |

### 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 schematron rules to ensure that the versions of the imported specs meet the minimum allowed versions. | Schematron<br>ARH-ID-00004 Added<br>ARH-ID-00005 Added | Data generation and ingestion systems need to be updated enforce the new rules. |

| Change   | Artifacts changed          | Compatibility Notes  |
|--|----------------------------|--|
| Update ISM to V10  | Schema<br>Constraint Rules | Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification.          |
| Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM V9 and NTK V7 | DES                        | Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation. |

## Appendix C Glossary

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

|         |  |
|---------|--|
| ADD     | Abstract Data Definition                                   |
| ARH     | Access Rights and Handling                                 |
| CES     | CVE Encoding Specification                                 |
| CIO     | Chief Information Officer                                  |
| CVE     | Controlled Vocabulary Enumeration                          |
| DES     | Data Encoding Specification                                |
| DNI     | Director of National Intelligence                          |
| EI&A    | Enterprise Integration and Architecture                    |
| FOUO    | For Official Use Only                                      |
| HTML    | HyperText Markup Language                                  |
| IANA    | Internet Assigned Numbers Authority                        |
| 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  | IC Information Technology Enterprise                       |
| ICD     | Intelligence Community Directive                           |
| ICO-NTK | Intelligence Community Only Need-to-Know                   |
| ICPG    | Intelligence Community Program Guidance                    |
| ICPM    | Intelligence Community Policy Memorandum                   |
| ICS     | Intelligence Community Standard                            |
| IEC     | International Electrotechnical Commission                  |
| IETF    | Internet Engineering Task Force                            |
| ISM     | Information Security Markings                              |
| ISMCAT  | Information Security Marking Country Codes and Tetragraphs |



---

|            |  |
|------------|--|
| ISO        | International Organization for Standardization                       |
| IT         | Information Technology   |
| MIME       | Multipurpose Internet Mail Extensions                                |
| NTK        | Need-To-Know Metadata  |
| OCIO       | Office of the Intelligence Community Chief Information Officer       |
| OC-NTK     | Originator Controlled Need-to-Know                                   |
| ODNI       | Office of the Director of National Intelligence                      |
| PDF        | Portable Document Format   |
| PDP        | Policy Decision Point  |
| PROPIN     | Proprietary Information  |
| PROPIN-NTK | Data Encoding Specification for Proprietary Information Need-To-Know |
| PUBS       | Intelligence Publications  |
| RFC        | Request for Comments   |
| TDF        | Trusted Data Format  |
| XML        | Extensible Markup Language   |
| XPath      | XML Path Language  |
| XSL        | Extensible Stylesheet Language                                       |
| XSLT       | XSL Transformations  |

## Appendix D 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/HvBHBmY>
- [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](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\\_209 Tearline Production and Dissemination.pdf](http://www.dni.gov/files/documents/ICD/ICD_209_Tearline_Production_and_Dissemination.pdf) [http://www.dni.gov/files/documents/ICD/ICD\_209 Tearline Production and Dissemination.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/enm8L9x>  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_500.pdf](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)
- [5] ICD 501  
Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.  
Available online Intelink-TS at: <http://go.ic.gov/GG61roi>  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_501.pdf](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)
- [6] ICD 710  
Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_710.pdf](http://www.dni.gov/files/documents/ICD/ICD_710.pdf)
- [7] ICPG 710.1  
Assistant Director of National Intelligence for . *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>
- [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/QUDIJKZ>

Available online Intelink-U at: [https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500\\_20\\_signed\\_16DEC2010.pdf](https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf)

[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-U at: [https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS\\_500-21\\_SIGNED\\_20110128.pdf](https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf)

[11] 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>

[12] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML)*.

Available online Intelink-U at: <http://purl.org/IC/Standards/ISM>

Available online at: <http://purl.org/IC/Standards/public>

[13] Jelliffe

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

<http://www.schematron.com>

[14] NTK.XML

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

Available online Intelink-U at: <http://purl.org/IC/Standards/NTK>

Available online at: <http://purl.org/IC/Standards/public>

[15] Oxygen

SyncRO Soft. *<oXygen/> XML Editor*. Version 14.1.

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

[16] 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/>  
[<http://code.google.com/p/schematron/>]

[17] 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>

[18] 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>

[19] 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/>

[20] 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@intelink.gov](mailto:ic-standards-support@intelink.gov) [mailto:ic-standards-support@intelink.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.<sup>[9]</sup>