



Intelligence Community Technical Specification

XML Data Encoding Specification for Access Rights and Handling

Version 2

14 January 2013

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
1.7 - Dependencies	4
1.8 - Conformance	4
Chapter 2 - Development Guidance	6
2.1 - Relationship to Abstract Data Definition and other encodings	6
2.2 - Additional Guidance	6
2.2.1 - Security and ExternalSecurity	6
2.2.2 - Usage of ISM and NTK	6
2.2.3 - MIME type	6
Chapter 3 - Data Constraint Rules	7
3.1 - Constraint Rule Types	7
3.2 - "Living" Constraint Rules	7
3.3 - Classified or Controlled Constraint Rules	7
3.4 - Terminology	7
3.5 - Errors and Warnings	8
3.6 - Rule Identifiers	8
3.7 - Data Validation Constraint Rules	8
3.7.1 - Purpose	8
3.7.2 - Schematron	8
3.7.3 - Non-null Constraints	9
3.7.4 - Inherited Constraints	9
3.7.5 - Value Enumeration Constraints	9
3.7.6 - Additional Constraints	9
3.7.6.1 - DES Constraints	9
3.7.7 - Constraint Rules	10
3.8 - Data Rendering Constraint Rules	10
3.8.1 - Purpose	10
3.8.2 - Rendering Constraint Rules	10
Chapter 4 - Conformance Validation	11
4.1 - Schema Validation	11
4.2 - Business Rule Validation	11
Chapter 5 - Generated Guides	12
5.1 - Schema Guide	12
5.2 - Schematron Guide	13
Appendix A - Feature Summary	14
A.1 - ARH Feature Summary	14
A.2 - ISM Feature Summary	14
A.3 - NTK Feature Summary	18
Appendix B - Change History	20
B.1 - V2 Change Summary	20

Appendix C - Acronyms	21
Appendix D - Bibliography	24
Appendix E - Points of Contact	28
Appendix F - IC CIO Approval Memo	29

List of Tables

Table 1 - Dependencies	4
Table 2 - Constraint Rules	10
Table 3 - ARH Dependency over time	14
Table 4 - Feature Summary Legend	14
Table 5 - ARH Feature comparison	14
Table 6 - ISM Feature comparison	14
Table 7 - NTK Feature comparison	18
Table 8 - DES Version Identifier History	20
Table 9 - Data Encoding Specification V2 Change Summary	20
Table 10 - Acronyms	21

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* ^[8] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA).
- Lead the IC's identification, development, and management of IC enterprise standards.
- Incorporate technically sound, deconflicted, 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 ICS 500-21, ^[14] 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.

A DES specifies how to implement the abstract data elements in the IC.ADD in a particular physical encoding (e.g., data or file format). For example:

- DESs for textual markup formats, such as Extensible Markup Language (XML) and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.
- DESs for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.
- DESs 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 ODNI policies and implementation guidance.

- IC Information Technology Enterprise (IC ITE)
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[5]
- 500 Series:
 - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC^[9]
 - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information^[14]
- 200 Series:
 - Intelligence Community Directive (ICD) 208, Write for Maximum Utility^[6]
 - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination^[7]

- Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide^[12]
- 700 Series:
 - Intelligence Community Directive (ICD) 710, Classification and Control Markings System^[10]
 - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control^[11]

1.5 - Audience and Applicability

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

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,^[13] 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.

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.^[15] 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.

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 additional technical specifications or additional documentation listed in the following table. The documents listed below are referenced in this Data 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</i> (ISM.XML.V9+) ^[16]	Depends on Information Security Markings (ISM). Starting with ISM v9, the version of ISM imported is no longer normative, so any ISM version 9 or above may be used.
<i>XML Data Encoding Specification for Need-To-Know Metadata</i> (NTK.XML.V7+) ^[21]	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.
ISO Schematron ^[24] implementation by Rick Jelliffe (2010-04-14)	Specification uses Schematron to encode IC business rules for this specification. Conformance to the logic of the business rules is normative, whereas use of the schematron language to encode them is informative.
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the ARH CVEs 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 or enlighten or inform.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron^[24] code version of the constraint rules are normative for this DES. 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^[15] 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 [\[26\]](#). 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, which are 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 DES to the abstract terms defined in the IC.ADD are described using a mapping table in the IC.ADD. The mapping tables generally show the mapping to the DES where a structure is defined, not where it is used. These mappings are provided for reference only. The complete set of DES artifacts, both normative and informative, should be consulted in order to gain a complete understanding of this DES.

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

2.2 - Additional Guidance

2.2.1 - 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**

2.2.2 - 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.

2.2.3 - 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 - Data Constraint Rules

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 to be resolved. 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 DES 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^[24] was selected as the language in which to encode these additional rules. The provided Schematron^[24] is used to define the constraint rules; it is NOT a required implementation. Implementers can use any tools at their disposal as long as the data complies with the rules expressed. To facilitate testing and understanding of the rules they are executable in either oXygen^[23] or the XSLT 2.0^[28] implementation of ISO Schematron^[24] provided by Rick Jelliffe at <http://schematron.com/> [http://schematron.com/]. Constraint rules are dependent on XPath 2.0^[27] and XSLT 2.0^[28] features. According to Mr. Jelliffe, the editor of Schematron^[24] for ISO:

"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."

Included in the package are the ISO Schematron^[24] implementation and XSLT 2.0^[28] files provided as a convenience 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 — which allows for empty (or null) content. 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 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 (CVEs) to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE. Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

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

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

3.7.6 - Additional Constraints

3.7.6.1 - DES Constraints

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

¹"white space" is defined in XML 1.0^[25] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

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 is considered conformant with this specification if it passes all of the following normative validation steps. The following steps do not dictate how this validation strategy is implemented.

4.1 - Schema Validation

This first step in validation is to ensure that an instance document is compliant against the normative schema of this specification as well as those of this specification's dependencies.

If an instance is determined to be non-compliant with schema in this step then results from the future steps may be indeterminate. As such, schema compliance should always be ensured prior to taking action on results from other validation steps.

4.2 - Business Rule Validation

The second step in validation is to ensure that an instance document complies with the business rules expressed in this specification as well as those of this specification's dependencies. It should be noted that while the business rules for this specification are expressed in Schematron, the Schematron is informative but the constraints they express are normative. As such, any languages or tools may be used to perform the validation as long as the results are consistent with results of the Schematron included in this specification and its dependencies.

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
ISM	V9	V9+
NTK	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
	Supports multiple versions of ISM.XML (V9 - Current) and NTK.XML (V7 - Current)	N	F

A.2. ISM Feature Summary

Table 6 - ISM Feature comparison

ISM Feature Comparison											
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
Required date											
CAPCO Register and Manual 2.1	Declass Removed from Banner	N	F	F	F	F	F	F	F	F	F
January 22, 2009 (1 year after 2008 memo)											

ISM Feature Comparison											
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
Required date											
E.O. 13526 ^[4] December 29, 2009	Compilation Reason	N	F	F	F	F	F	F	F	F	F
CAPCO Register and Manual 3.1 May 7, 2010	LES	P	N	F	F	F	F	F	F	F	F
CAPCO Register and Manual 3.1 May 7, 2010	LES-NF	P	N	F	F	F	F	F	F	F	F
CAPCO Register and Manual All versions Pre 2008	Require Notices	N	N	F	F	F	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	KDK	N	N	F	F	F	F	F	F	F	F
ICD 710 ^[10] September 11, 2009	710 Foreign Disclosure or Release	P	P	F	F	F	F	F	F	F	F
E.O. 13526 ^[4] December 29, 2009	DeclassReasons/Dates	P	P	F	F	F	F	F	F	F	F
IC-CIO enhance data quality See IC ESB	schema validation of CVE values	N	N	N	F	F	F	F	F	F	F
DoD Instruction 5230.24 ^[2] March 18, 1987	DoD Distro Statements	N	N	N	F	F	F	F	F	F	F
DoD Directive 5240.01 ^[3] August 27, 2007	US Person Notice	P	P	P	P	F	F	F	F	F	F
CAPCO Register and Manual 2.2 September 25, 2010 (1 Year after 2.2)	Remove SAMI	P	P	P	P	F	F	F	F	F	F
ISOO Marking Booklet 2010 ^[18] / ISOO Notice 2009-13 ^[19] December 2010	Remove exempted source	P	P	P	P	F	F	F	F	F	F

ISM Feature Comparison											
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
Required date											
E.O. 13526 ^[4]	derivativelyClassifiedBy	P	P	P	P	F	F	F	F	F	F
December 29, 2009											
CAPCO Register and Manual 4.1	Atomic Energy New banner location	N	N	N	N	F	F	F	F	F	F
December 10, 2011 (1 Year after 4.1)											
CAPCO Register and Manual 4.1	Display Only	N	N	N	N	F	F	F	F	F	F
December 10, 2011 (1 Year after 4.1)											
IC-CIO enhance data quality	Schematron ^[24] Implementation of rules	N	N	N	N	F	F	F	F	F	F
See IC ESB											
E.O. 13526 ^[4]	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F	F
December 29, 2009											
DoD Manual 5200.1 ^[1]	DoD ACCM Markings	N	N	N	N	N	F	F	F	F	F
January 1997											
CAPCO Register and Manual 4.2	SSI	N	N	N	N	N	F	F	F	F	F
May 31, 2011											
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) ^[17]	TFNI	N	N	N	N	N	F	F	F	F	F
June 28, 2010											
CAPCO Register and Manual 4.1	HCS SubCompartments	N	N	N	N	N	F	F	F	N	N
December 10, 2010											
CAPCO Register and Manual 4.1	MCFI Remove	P	P	P	P	P	F	F	F	F	F
November 16, 2010 (date disestablished)											
CAPCO Register and Manual 4.2	MIFH, EUDA and EFOR removed	P	P	P	P	P	P	F	F	F	F
May 31, 2011											

ISM Feature Comparison											
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
Required date											
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) ^[17] June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F	F	N/A
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F	F	F
ICD 710 ^[10] September 11, 2009	710 POC	N	N	N	N	N	N	F	F	F	F
DNI ORCON Memo ^[22] March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F	N/A
ISOO Marking Booklet ^[18] December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	F	F	F	F
IC-CIO enhance data quality See IC ESB	RD, FRD, and Sigma rolldown enforced	N	N	N	N	N	N	N	F	F	F
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	F	F	F
IC-CIO enhance data quality See IC ESB	@ism:excludeFromRollup=true() allowed to not have an ICD-710 foreign release indicator	N	N	N	N	N	N	N	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SINFO Remove	P	P	P	P	P	P	P	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SC Remove	P	P	P	P	P	P	P	F	F	F
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	F	F	F
CAPCO Register and Manual 5.1 December 30, 2011	Require using 50X1-HUM instead of 25X1-human	N	N	N	N	P	P	P	F	F	F

ISM Feature Comparison											
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
Required date											
CAPCO Register and Manual 5.1	Allow use of KDK compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F
December 30, 2011											
CAPCO Register and Manual 5.1	Allow use of SI compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F
December 30, 2011											
CAPCO Register and Manual 5.1 Annex A	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F	F
IC-CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F	F
DoD Manual 5200.1-R ^[1]	COMSEC Notice	N	N	N	N	N	N	N	N	F	F
February 2012											
DoD Manual 5200.1-R ^[1]	Support for NNPI	N	N	N	N	N	N	N	N	F	F
February 2012											
Decouple ISM from the Schema	Schema is Informative, Schematron and CVEs are Normative.	N	N	N	N	N	N	N	N	N	F
January 2013											
CAPCO Register and Manual 5.1	Add ENDSEAL system with compartments ECRU and NONBOOK	N	N	N	N	N	N	N	N	N	F
December 2012											
CAPCO Register and Manual 5.1	Limit KDK system compartments to BLUEFISH, IDITAROD and KANDIK.	N	N	N	N	N	N	N	N	P	F
December 2013											
ISOO Notice 2013-01 ^[20] .	Support NATO exemptions to declass date.	N	N	N	N	N	N	N	N	N	F
November 2012											

A.3. NTK Feature Summary

Table 7 - NTK Feature comparison

NTK Feature Comparison										
Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	
	Schematron ^[24] Implementation of rules	N	N	F	F	F	F	F	F	F
	Portion Level NTK	N	N	N	N	N	N	F	F	

NTK Feature Comparison									
Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8
	Support multiple verions of ISM.XML (V9 - Current)	N	N	N	N	N	N	N	F

Appendix B Change History

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

Table 8 - 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.1 - V2 Change Summary

B.1 - 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 9 - 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 ARH-ID-00004 Added ARH-ID-00005 Added	Data generation and ingestion systems need to be updated enforce the new rules.
Update ISM to V10	Schema 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 NTKv7	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.

Appendix C Acronyms

This appendix lists all the acronyms referenced in this DES and lists other acronyms that may have been used in other DES. This appendix is a shared resource across multiple documents so in any given DES there are likely acronyms that are not referenced in that particular DES.

Table 10 - Acronyms

Name	Definition
A&A	Access Rights and Handling
ABAC	Attribute Based Access Control
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CMS	Cryptographic Message Syntax
CVE	Controlled Vocabulary Enumeration
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DDMS	Department of Defense Discovery Metadata Specification
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
EDH	Enterprise Data Header
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
GIS	Geospatial Information System
GNS	Geographic Names Server
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I2	Information Integration
IC	Intelligence Community
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
IC EA	IC Enterprise Architecture

Name	Definition
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
IRM	Information Resource Metadata
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWT	JSON Web Token
KA	Knowledge Assertion
KOS	Knowledge Organization System
MAC	Multi Audience Collection
MIME	Multipurpose Internet Mail Extensions
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NGT	Next Generation Trident
NPE	Non-Person Entity
NSI	National Security Information
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PK	Private Key
PKI	Public Key Infrastructure
RDBMS	Relational Database Management System
REST	REpresentational State Transfer

Name	Definition
RFC	Request for Comments
RR-ID	REST Security Encoding Specification for End-to-End Identity Propagation
SAML	Security Assertion Markup Language
SSD	Special Security Directorate
SSL	Secure Sockets Layer
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TGN	Thesaurus of Geographic Names
TLS	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VIRT	Virtual Coverage
W3CDTF	World Wide Web Consortium Date Time Format
WSDL	Web Service Definition Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

Appendix D Bibliography

Bibliography

- [1] DoD Manual 5200.1
Under Secretary of Defence for Intelligence. *DoD Information Security Program (Vol 1-4)*. 5200.1. February 24, 2012.
Vol 1 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
Vol 2 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf
Vol 3 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf
Vol 4 Available online at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf
- [2] DoD Instruction 5230.24
Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. 23 August 2012.

23 August 2012 edition replaced the March 18, 1987.
Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf>
- [3] DoD Directive 5240.01
Secretary of Defense. *DoD Intelligence Activities*. 5240.01. August 2007.
Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/524001p.pdf>
- [4] E.O. 13526
The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.
Available online at: <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>
- [5] 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 at: <http://go.ic.gov/HvBHBmY>
- [6] 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
- [7] 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
- [8] ICD 500
Director of National Intelligence Chief Information Officer. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

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

[9] ICD 501

Director of National Intelligence Chief Information Officer. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[10] ICD 710

Director of National Intelligence Chief Information Officer. *Classification and Control Markings System*. Intelligence Community Directive 710. 11 September 2009.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[11] 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 at: <http://go.ic.gov/fU3HML>

[12] ICPM 2007-200-2

Assistant Director of National Intelligence for . *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>

[13] 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 at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[14] 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 at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[15] 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>

[16] ISM.XML

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

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

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

[17] ISOO 32 CFR Parts 2001 and 2003

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information; Final Rule*. 32 CFR Parts 2001 and 2003. Federal Register, Vol. 75, No. 123. 28 June 2010.
Available online at: <http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf>

[18] ISOO Marking Booklet
Information Security Oversight Office. *Marking Classified National Security Information*. December 2010.
Available online at: <http://www.archives.gov/isoo/training/marketing-booklet.pdf>

[19] ISOO Notice 2009-13
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2009-13: Prohibited Use of X1-X8 Markings*.
Available online at: <http://www.archives.gov/isoo/notices/notice-2009-13.pdf>

[20] ISOO Notice 2013-01
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2013-01: Further Marking Guidance on Commingling North Atlantic Treaty Organization (NATO) and Classified National Security Information (NSI)*.
Available online at: www.archives.gov/isoo/notices/notice-2013-01.pdf

[21] NTK.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.
Available online IntelLinkU at: <http://purl.org/IC/Standards/NTK>
Available online at: <http://purl.org/IC/Standards/public>

[22] ORCON Memo
Director of National Intelligence. *Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities*. 29 March 2011.

ICPG 710.1 signed July 2012^[11], rescinded the ORCON Memo.
Available online at: https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf
Attachment A: <https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20A.doc.pdf>
Attachment B: <https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20B.pdf>
Attachment C: <https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20C.pdf>

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

[24] Schematron

International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.

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

[25] 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>

[26] 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>

[27] 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/>

[28] 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.

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.^[13]