Intelligence Community Technical Specification

XML Data Encoding Specification for Need-To-Know Metadata

Version 7

17 July 2012

Table of Contents

Chapter 1 - Introduction 1
1.1 - Purpose 1
1.2 - Scope 1
1.3 - Background 1
1.4 - Enterprise Need 2
1.5 - Audience and Applicability 2
1.6 - Conventions 3
1.7 - Conformance 3
1.8 - Dependencies 4
Chapter 2 - Development Guidance 5
2.1 - Relationship to Abstract Data Definition and other encodings 5
2.2 - Additional Guidance 5
2.2.1 - Integration into a schema 5
2.2.2 - Basic usage model 6
2.2.3 - Guidance for the specification of constraints for a particular access system ... 6
2.2.4 - Guidance for systems processing data containing NTK metadata 7
Chapter 3 - Data Validation Constraint Rules 8
3.1 - Basics 8
3.1.1 - Schematron 8
3.1.2 - “Living” Constraint Rules 8
3.1.3 - Classified or Controlled Constraint Rules 9
3.1.4 - Terminology 9
3.1.5 - Rule Identifiers 9
3.1.6 - Errors and Warnings 9
3.2 - Non-null Constraints 9
3.3 - Inherited Constraints 10
3.4 - Value Enumeration Constraints 10
3.5 - Additional Constraints 10
3.5.1 - DES Constraints 10
3.6 - Constraint Rules 10
Chapter 4 - Data Rendering Constraint Rules 11
4.1 - Basics 11
4.1.1 - "Living" Constraint Rules 11
4.1.2 - Classified or Controlled Constraint Rules 11
4.1.3 - Rule Identifiers 11
4.1.4 - Errors and Warnings 11
4.2 - Constraint Rules 12
Chapter 5 - Generated Guides 13
5.1 - Schema Guide 13
5.2 - Schematron Guide 14
Appendix A - Feature Summary 15
A.1 - NTK Feature Summary 15
A.2 - ISM Feature Summary 15
Appendix B - Change History 20
B.1 - V7 Change Summary 20
B.2 - V6 Change Summary 21

B.3 - V5 Change Summary 21
B.4 - V4 Change Summary 22
B.5 - V3 Change Summary 22
B.6 - V2 Change Summary 23
Appendix C - Acronyms 24
Appendix D - Bibliography 26
Appendix E - Points of Contact 29
Appendix F - IC CIO Approval Memo 30

List of Tables

Table 1 - Dependencies 4
Table 2 - Constraint Rules 12
Table 3 - NTK Dependency over time 15
Table 4 - Feature Summary Legend 15
Table 5 - NTK Feature comparison 15
Table 6 - ISM Feature comparison 15
Table 7 - DES Version Identifier History 20
Table 8 - Data Encoding Specification V7 Change Summary 20
Table 9 - Data Encoding Specification V6 Change Summary 21
Table 10 - Data Encoding Specification V5 Change Summary 22
Table 11 - Data Encoding Specification V4 Change Summary 22
Table 12 - Data Encoding Specification V3 Change Summary 23
Table 13 - Data Encoding Specification V2 Change Summary 23
Table 14 - Acronyms 24

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Need-To-Know Metadata* (NTK.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode NTK metadata necessary to facilitate automated systems making a "need-to-know" (NTK) determination. This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing NTK data concepts using XML.

These metadata are used to represent the system-specific properties assigned to an information resource that will be used, in conjunction with information about the user, and possibly other information, to determine the user's access to the data. A single information resource may include multiple occurrences of these metadata in order to specify (NTK) information according to multiple, different access systems. Each of the access systems will provide the specifics about the metadata to be captured.

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* [5] 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,[8] 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 frequently relies on being able to determine an individual’s need-to-know as one component in determining whether to allow access to data. The enterprise will increasingly rely on need-to-know metadata to allow users and systems to find and access a wide-range of data throughout the enterprise. A successful information sharing enterprise depends on the ability of the data creator and or providers to specify the means by which need-to-know can be established in a manner to facilitate discovery and access via automated means.

This DES provides a common specification for the means by which a data producer can encode, in their data, the information an access system needs to determine how to grant access. This DES enables a comprehensive capability that can appropriately protect data across the enterprise while also allowing access by individuals having appropriate need-to-know. The nature of the information to be encoded will vary system by system and could include lists of individuals or groups permitted access, descriptions of subject matter in terms defined by the access system, or other traits to be used in evaluating the access an individual has to the data.

This DES provides that common specification. Currently the particulars of any access system’s data needs are not defined. Details for specifying access information and documenting access parameters for particular access systems are to be added in the near future. The systems for which access information will be recorded and constrained will be expanded as their applicabilities are identified to the enterprise.

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,[7] 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.[9] 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 - 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, CVE values from the XML CVE files, and the Schematron[16] 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[9] is considered normative within the scope of the sentence. All other parts of this document are informative.

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.

1.8 - Dependencies

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

Table 1 - Dependencies

Name
XML Data Encoding Specification for Information Security Marking (ISM.XML.V9)[10]
ISO Schematron[16] implementation by Rick Jelliffe (2010-04-14)
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.

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

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

2.2.1 - Integration into a schema

The NTK schema is not designed nor intended to be used as a stand-alone schema. In order to use the capabilities of this DES, the XML schema that is part of this DES must be incorporated into another XML schema. For purposes of this documentation, we will refer to this other schema as the “resource” schema. Additionally, the “resource” schema must include the XML schema of the XML Data Encoding Specification for Information Security Marking (ISM.XML). The basic process for incorporation is as follows:

- Import this schema in to “resource” schema
- Define a namespace prefix
- Allow for the **DESVersion** attribute to be used in the “resource” schema
- Ensure (Information Security Marking Metadata) ISM is incorporated into the “resource” schema
- Add the Access element to the “resource” schema model at an appropriate location
- Add the ntk:access attribute to applicable portions in the "resource" schema model.

The specification is designed to record NTK information for an entire resource to include the NTK information itself. This means that those that have access to the resource will have access to all of the NTK information.

2.2.2 - Basic usage model

In order for this DES to be effectively implemented in the enterprise, the following usage model description should be used.

First, an access system that wishes to provide access control services to the enterprise must define the parameters they need to make decisions and/or the specific syntax by which individuals and/or groups are referenced. This information should also be published and made accessible to those who created resources and who wish to control access to those resources via that system. These specifications can be documented as per **Section 2.2.3**.

Next, the creators of resources who wish to control access to their resources via one of these access systems must specify the access to the resource using the specifics defined by the desired access system. The resource creator can decide to specify access in terms of more than one access system.

This DES is initially published without specifying Controlled Vocabulary Enumerations (CVEs) or many constraint rules. It is expected that as enterprise systems are recognized and adopt this model the CVEs and constraints will be fleshed out. The expectation is to have a small number of enterprise access systems.

2.2.3 - Guidance for the specification of constraints for a particular access system

When an access system desires to use the capabilities of this DES to document how information concerning access should be specified by resource producers, they shall abide by the following guidelines.

- The access system owner shall provide a name for the system to be used in the CVE for the element **AccessSystemName**.
- The access system owner shall provide a syntax, pattern, or CVE for the elements **AccessIndividualValue**, **AccessGroupValue**, and **AccessProfileValue**.
- The access system owner shall provide guidance on encoding, in the syntax of this DES, for all parameters necessary to be specified on the resource and in portions when applicable, other than those encoded via ISM.

When it is desired or required to denote access control information at the portion level, the implementing system must define how the portions roll-up to the resource level access control requirements. Without a roll-up scheme there is a great risk that the resource level access controls may not sufficiently restrict access to the data. NTK does not currently enforce or implement any roll-up from portion level NTK attributes.

Depending on the data format for the resource, data used for access control, may be duplicated; one instance in the resource’s usual encoding, the other in the access model. The benefit of this possible duplication is that the explicit specification of the access information in a consistent manner allows for resources to implement this DES in multiple different schemas’ that may locate the duplicate information in many different elements or attributes.

More information about systems and their vocabularies can be found in their documentation external to this DES.

- GIMMEE: https://gimmee.cia.ic.gov/help/service_specification.doc
- EDH: To be determined

2.2.4 - Guidance for systems processing data containing NTK metadata

It is important to note that data may have multiple access system requirements expressed (e.g., system A profile, system B profile, etc.). Each system is to be considered separately. This means that the set of people or systems having access to the data is the union of the people or systems described by the NTK metadata supplied for all access systems.

Systems handling data containing NTK metadata must assess and understand the NTK metadata in order to protect the data appropriately. A best practice for addressing this issue is to first examine any NTK metadata that may exist within the data being received. If NTK metadata is present, the receiving system should look for NTK metadata expressed in terms of an access system it understands. If no understandable NTK metadata is located, the files should be segregated and protected via the most restrictive manner available, and the submitter should be contacted to understand any possible ramifications.

Chapter 3 - Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for NTK.XML. They provide additional restrictions (i.e., constraints) on how the data should be structured and encoded, especially for criteria that exceed the constraints implemented in the XML Schema. These rules are written in plain English phrases; however, knowledge of the NTK.XML schemas is required to understand the rules. Complex constraint rules may be followed by text labeled *Human Readable*. This text is intended to inform the intent of the more formal language above it. Implementers are intended to implement the formal language, and should there be a perception of conflict, bring it to the attention of the appropriate configuration control body to be resolved.

3.1 - Basics

The NTK.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.

3.1.1 - Schematron

Schematron[16] was selected as the language in which to encode these additional rules. The provided Schematron[16] 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*® [15] or the XSLT 2.0[19] implementation of ISO Schematron[16] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[18] and XSLT 2.0[19] features. According to Mr. Jelliffe, the editor of Schematron[16] 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[16] implementation and XSLT 2.0[19] files provided as a convenience along with a compiled version of the rules.

3.1.2 - “Living” Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a starter set and do not attempt to address the full scope tradecraft and business rules addressed by multiple policy drivers. These rules will be expanded and modified as the model matures, and as applicable documentation and tradecraft 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.

3.1.3 - 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.

3.1.4 - 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.

3.1.5 - 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. NTK.XML data validation constraint rule IDs are prefixed with “NTK-ID-”.

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

3.1.6 - 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.

3.2 - 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.

3.3 - Inherited Constraints

In an instance of NTK.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 1.8 - Dependencies.

3.4 - Value Enumeration Constraints

Several elements and attributes of the NTK.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.

3.5 - Additional Constraints

3.5.1 - DES Constraints

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

3.6 - Constraint Rules

The detailed constraint rules for the NTK.XML schema can be found in a separate document inside the SchematronGuide directory, in the NTK_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.

[1] "white space" is defined in XML 1.0[17] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

Chapter 4 - Data Rendering Constraint Rules

The constraint rules in this chapter define constraints on the rendering of NTK.XML documents. The intent is to inform the development of systems capable of rendering or displaying NTK.XML data for use by individuals not familiar with the details of the NTK.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.

4.1 - Basics

4.1.1 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a starter set and do not attempt to address the full scope tradecraft and business rules addressed by multiple policy drivers. These rules will be expanded and modified as the model matures, and as applicable documentation and tradecraft 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.

4.1.2 - 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.

4.1.3 - 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 and10001 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. NTK.XML data rendering constraint rule IDs are prefixed with “NTK-RENDER-”.

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

4.1.4 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning” and is indicated in brackets preceding each constraint rule description. 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 system. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a system.

Each system responsible for rendering documents must be evaluated based on its use. Those evaluating the system must make a mission-appropriate decision about the system's suitability for use.

4.2 - Constraint Rules

The following table contains the information for the NTK.XML data rendering constraint rules.

Table 2 - Constraint Rules

Rule Number	Severity	Description	Human Readable Description

Chapter 5 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the NTK.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 NTK.XML schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen*® [15], produced by SyncRO Soft.

The guide provides an interactive index to:

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

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

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

5.2 - Schematron Guide

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

Table 3 - NTK Dependency over time

Dependent DES	V1	V2	V3	V4	V5	V6	V7
ISM	V3	V4	V5	V6	V7	V8	V9

The following table summarizes major features by version for NTK and all dependent specs.

Table 4 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can't comply)
Cell Colors represent the same information as the Key value	

A.1. NTK Feature Summary

Table 5 - NTK Feature comparison

NTK Feature Comparison								
Required date	Feature	V1	V2	V3	V4	V5	V6	V7
	Schematron[16] Implementation of rules	N	N	F	F	F	F	F
	Portion Level NTK	N	N	N	N	N	N	F

A.2. ISM Feature Summary

Table 6 - ISM Feature comparison

ISM Feature Comparison										
Driver Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9
CAPCO Register and Manual 2.1 January 22, 2009 (1 year after 2008 memo)	Declass Removed from Banner	N	F	F	F	F	F	F	F	F
E.O. 13526[4] December 29, 2009	Compilation Reason	N	F	F	F	F	F	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
CAPCO Register and Manual 3.1 May 7, 2010	LES	P	N	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
CAPCO Register and Manual All versions Pre 2008	Require Notices	N	N	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
ICD 710[6] September 11, 2009	710 Foreign Release	P	P	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
IC-CIO enhance data quality See IC ESB	schema validation of CVE values	N	N	N	F	F	F	F	F	F
DoD Directive 5230.24[2] March 18, 1987	DoD Distro Statements	N	N	N	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
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
ISOO Marking Booklet 2010[12] / ISOO Notice 2009-13[13] December 2010	Remove exempted source	P	P	P	P	F	F	F	F	F
E.O. 13526[4] December 29, 2009	derivativelyClassifiedBy	P	P	P	P	F	F	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Atomic Energy New banner location	N	N	N	N	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Display Only	N	N	N	N	F	F	F	F	F
IC-CIO enhance data quality See IC ESB	Schematron[16] Implementation of rules	N	N	N	N	F	F	F	F	F
E.O. 13526[4] December 29, 2009	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F
DoD Directive 5200.1-R[1] January 1997	DoD ACCM Markings	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	SSI	N	N	N	N	N	F	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[11] June 28, 2010	TFNI	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	HCS SubCompartments	N	N	N	N	N	F	F	F	N
CAPCO Register and Manual 4.1 November 16, 2010 (date disestablished)	MCFI Remove	P	P	P	P	P	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	MIFH, EUDA and EFOR removed	P	P	P	P	P	P	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[11] June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F	F
ICD 710[6] September 11, 2009	710 POC	N	N	N	N	N	N	F	F	F
DNI ORCON Memo [14] March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F
ISOO Marking Booklet[12] December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	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
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	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
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
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
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	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
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of KDK SubCompartments and Sub-SubCompartments	N	N	N	N	N	N	N	N	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of SI SubCompartments and Sub-SubCompartments	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 Annex A	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F
IC-CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[1] February 2012	COMSEC Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[1] February 2012	Support for NNPI	N	N	N	N	N	N	N	N	F

Appendix B Change History

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

Table 7 - DES Version Identifier History

Version	Date	Purpose
1	11 May 2010	Initial Release
2	7 September 2010	Routine revision to technical specification. For details of changes, see Section B.6 - V2 Change Summary
3	6 December 2010	Routine revision to technical specification. For details of changes, see Section B.5 - V3 Change Summary
4	11 April 2011	Routine revision to technical specification. For details of changes, see Section B.4 - V4 Change Summary
5	19 September 2011	Routine revision to technical specification. For details of changes, see Section B.3 - V5 Change Summary
6	27 February 2012	Routine revision to technical specification. For details of changes, see Section B.2 - V6 Change Summary
7	17 July 2012	Routine revision to technical specification. For details of changes, see Section B.1 - V7 Change Summary

B.1 - V7 Change Summary

Significant drivers for Version 7 include:

- See ISM V9 drivers

The following table summarizes the changes made to V6 in developing V7

Table 8 - Data Encoding Specification V7 Change Summary

Change	Artifacts changed	Compatibility Notes
Update ISM to V9	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification.
Update mapping to ADD	DES	Should not impact data
Added support for alphanumeric **@DESVersion** identifiers [artf12167].	Schema	Should not impact data but ingestion systems may need to account for it.
Changed declaration of AccessProfileValueType from complextContent to simpleContent [artf12153].	Schema	Should only impact some code generation systems.

Change	Artifacts changed	Compatibility Notes
Added external reference attribute to indicate ntk refers to external content	Schema	Ingest and data generation systems should be updated
Added support for **@ntk:access** portion marking group [artf12287].	Schema NTK-ID-00005 Added NTK-ID-00005 Removed	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Added support for **@DESVersion** and Need to Know for external documents [artf12449].	Schema NTK-ID-00006 Added NTK-ID-00007 Added	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Added ntk:ExternalAccess element for use when the NTK is about an external resource.	Schema NTK-ID-00002	Data Ingestions systems need to be updated to properly enforce the new element and associated constraints.

B.2 - V6 Change Summary

Significant drivers for Version 6 include:

- See ISM V8 drivers

The following table summarizes the changes made to V5 in developing V6

Table 9 - Data Encoding Specification V6 Change Summary

Change	Artifacts changed	Compatibility Notes
Update ISM to V8	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification.

B.3 - V5 Change Summary

Significant drivers for Version 5 include:

- See ISM V7 drivers

The following table summarizes the changes made to V4 in developing V5

Table 10 - Data Encoding Specification V5 Change Summary

Change	Artifacts changed	Compatibility Notes
Update ISM to V7	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification.
Fixed type errors generated when using a schema-aware processor.	Constraint Rules	Should not affect data.

B.4 - V4 Change Summary

Significant drivers for Version 4 include:

- See ISM V6 drivers

The following table summarizes the changes made to V3 in developing V4

Table 11 - Data Encoding Specification V4 Change Summary

Change	Artifacts changed	Compatibility Notes
Change encoding of constraint rules from text to Schematron.	Documentation Constraint Rules	Other than rules whose changes are noted below this should only result in more clarity of definition for the rules.
Use ISM V6	Schema	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Replaced NTK-ID-00001 with NTK-ID-00004	Documentation NTK-ID-00001 Remove NTK-ID-00004 Add	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule Note: Data valid under previous releases may not be valid under this release.

B.5 - V3 Change Summary

Significant drivers for Version 3 include:

- See ISM V5 drivers

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

Table 12 - Data Encoding Specification V3 Change Summary

Change	Artifacts changed	Compatibility Notes
Use ISM V5	Schema	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Remove Appendix H Reading the Schematics	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.

B.6 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V4 drivers

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

Table 13 - Data Encoding Specification V2 Change Summary

Change	Artifacts changed	Compatibility Notes
Use ISM V4	Schema	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Use schema to enforce DES version number	NTK-ID-00003	Data Ingestion systems need to be updated to use the new schema instead of constraint rules.

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 14 - Acronyms

Name	Definition
ATO	Authority To Operate
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CVE	Controlled Vocabulary Enumeration
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
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 ESB	Intelligence Community Enterprise Standards Baseline
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization

Name	Definition
ISOO	Information Security Oversight Office
KA	Knowledge Assertion
KOS	Knowledge Organization System
MIME	Multipurpose Internet Mail Extensions
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NGT	Next Generation Trident
NSI	National Security Information
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PK	Private Key
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RFC	Request for Comments
SSD	Special Security Directorate
SSL	Secure Socket Layer
SOAP	Simple Object Access Protocol
TGN	Thesaurus of Geographic Names
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3CDTF	World Wide Web Consortium Date Time Format
XML	Extensible Markup Language

Appendix D Bibliography

Bibliography

[1] DoD Directive 5200.1
Under Secretary of Defence for Intelligence. *DoD Information Security Program:*. 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 Directive 5230.24
Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. 18 March 1987.
Available online at: http://www.dtic.mil/dtic/pdf/submit/523024p.pdf

[3] DoD Directive 5240.01
Secretary of Defense. *DoD Intelligence Activities*. 5240.01. August 2007.
Available online at: http://www.dtic.mil/dtic/pdf/submit/5240.01.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] 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/electronic_reading_room/ICD_500.pdf

[6] 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/electronic_reading_room/ICD_710.pdf

[7] 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://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS-500-21.aspx

[8] 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://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS-500-21.aspx

[9] 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

[10] 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

[11] 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

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

[13] 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

[14] 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.
Available online at: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf
Attachment A: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20A.doc.pdf
Attachment B: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20B.pdf
Attachment C: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20C.pdf

[15] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. version 13.2.
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.
Available online at: http://www.schematron.com/

[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] 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/

[19] 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.[7]