



Intelligence Community Technical Specification

XML Data Encoding Specification for Originator Control Need-To-Know Profile

Version 1

6 September 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
1.7.1 - Standalone and Convenience Packages	4
1.8 - Conformance	5
1.9 - Version Policies	5
1.9.1 - XML Namespace Policy	5
1.9.2 - Version Numbering	6
Chapter 2 - Development Guidance	7
2.1 - Understanding Access Control	7
2.2 - Relationship to Abstract Data Definition and other encodings	8
2.3 - Additional Guidance	8
2.3.1 - Basic Usage	8
Chapter 3 - Definitions, Interfaces, and Constraints	10
3.1 - Constraint Rule Types	10
3.2 - "Living" Constraint Rules	10
3.3 - Classified or Controlled Constraint Rules	10
3.4 - Terminology	10
3.5 - Errors and Warnings	11
3.6 - Rule Identifiers	11
3.7 - Data Validation Constraint Rules	11
3.7.1 - Purpose	11
3.7.2 - Schematron	11
3.7.3 - Non-null Constraints	12
3.7.4 - Value Enumeration Constraints	12
3.7.5 - Additional Constraints	12
3.7.6 - Constraint Rules	12
3.8 - Data Rendering Constraint Rules	13
3.8.1 - Purpose	13
3.8.2 - Rendering Constraint Rules	13
Chapter 4 - Conformance Validation	14
4.1 - Business Rule Validation	14
Chapter 5 - Generated Guides	15
5.1 - Schema Guide	15
5.2 - Schematron Guide	16
Appendix A - Feature Summary	17
A.1 - OC-NTK Feature Summary	17
Appendix B - Change History	18
Appendix C - Acronyms	19
Appendix D - Bibliography	25
Appendix E - Points of Contact	28

Appendix F - IC CIO Approval Memo	29
---	----

List of Tables

Table 1 - Dependencies	4
Table 2 - Constraint Rules	13
Table 3 - Feature Summary Legend	17
Table 4 - OC-NTK Feature comparison	17
Table 5 - DES Version Identifier History	18
Table 6 - Acronyms	19

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Originator Control Need-To-Know Profile* (OC-NTK.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode OC-NTK data. This Data Encoding Specification (DES) defines the use of XML elements and attributes from NTK, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing OC-NTK data concepts using XML.

These metadata are used to represent the organizations for which dissemination of information marked ORCON has been approved by the originator. This list is intended for use in making access control decisions regarding the information.

1.2 - Scope

This specification profile 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.

Originator Controlled (ORCON) information requires a dissemination list that includes organizations for which the originator has determined dissemination of the information is allowable. This profile defines a specification that uses NTK for conveying that list.

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* [\[6\]](#) grants the IC CIO the authority and responsibility to:

- Develop an IC enterprise architecture.
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, deconflicted, interoperable enterprise standards into the enterprise architecture.
- Certify that IC elements adhere to the architecture and standards.

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

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-

enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[12] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby achieving the IC's data discovery, data sharing, and interoperability goals.

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

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

1.4 - Enterprise Need

Information within the national intelligence enterprise marked with information security markings, particularly those with originator control dissemination, may have a desire to specify the list of approved organizations permitted access to the information. This desire becomes more of a need as the enterprise continues to become more automated and the need to make access control decisions rely heavily on having such information available. Lack of such information could result in important information not getting to the people and groups that need it in a timely manner.

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

- IC Information Technology Enterprise (IC ITE)
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[2]
- 500 Series:
 - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC^[7]
 - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information^[12]
- 200 Series:

- Intelligence Community Directive (ICD) 208, Write for Maximum Utility^[4]
- Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination^[5]
- Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide^[10]
- 700 Series:
 - Intelligence Community Directive (ICD) 710, Classification and Control Markings System^[8]
 - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control^[9]

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*,^[11] 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^[13]. These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

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 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 Need-To-Know (NTK.XML.V8+)</i> ^[14]	Depends on Need-To-Know (NTK). The version of NTK imported is not normative, so any NTK version 8 or above may be used.
ISO Schematron ^[16] implementation by Rick Jelliffe (2010-04-14)	Conformance to the logic of the business rules listed in this DES is normative. The business rules are expressed in the Schematron language in terms of the features and behavior of the ISO implementation. While the use of Schematron is informative, any conformant implementation of this specification MUST match the behavior of the ISO Schematron implementation for validation.
<i>XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML.V1+)</i> ^[3]	Depends on Intelligence Community Identifier (IC-ID) Specification. Any IC-ID version 1 or above may be used.
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 OC-NTK CVEs is normative.

1.7.1 - Standalone and Convenience Packages

The standalone packaging of this specification does not include the specifications that it is dependent on since the version that may be used could be later than this packaging. There is a convenience packaging of the specification that includes all the most recent versions of the dependent specifications at the time it's generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change but it will not be signed as a formal package. In order to obtain all the necessary standalone packages you will have to follow this specification's dependencies, and subsequently, their dependencies. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and CVE to work. Should you mix versions of the CVE schema you will have to separate the sets of CVEs by Schema or edit the CVEs to point to the correct schema file.

Convenience packages are the easier way to go as they come with all dependencies pre-packaged together and are tested as interoperable. When trying to mix and match versions that have not been pre-packaged together there is always risk that a particular combination may not

be compatible, especially when mixing with versions of specifications that were not available at the time of this specification's release.

1.8 - Conformance

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

Normative: considered to be prescriptive and necessary to conform to the standard.

Informative: serving to instruct or enlighten or inform.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron^[16] code version of the constraint rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[13] is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.^[20] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of `ism:DESVersion='9'` to `ism:DESVersion='10'` in the `xsd:schema` statement. The ability to import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications such as ISM CVE updates. The decoupling of dependency versions is not retroactive; see the dependency table for allowed dependency versions.

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

1.9 - Version Policies

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from "The Disposition of Names in an XML Namespace"^[17]. This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 "Versioning and XML namespace policy" of "Architecture of the World Wide Web, Volume One"^[18].

In a fashion similar to DocBook there is a "version" attribute (i.e., DESVersion, CESVersion, version) defined in each namespace defined in an IC-CIO specification used to capture the

version number assigned to each revision of the specification. The DESVersion attribute is the only indicator in an instance document as to what revision of a particular specification the author intended the instance to be valid to. Since the namespace does not change the "version" attribute is required to fully understand the instance document

As changes to the specification are released the version number to be captured in the "version" attribute increments. See [Section 1.9.2 - Version Numbering](#) for information on the numbering scheme.

This XML namespace policy only applies to the namespaces defined in this specification, any namespaces that are included by reference should define their own namespace policy.

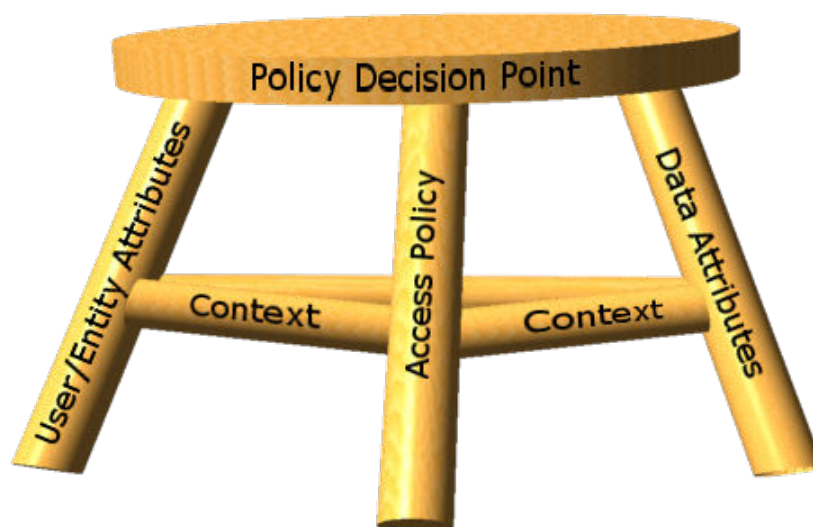
1.9.2 - Version Numbering

The version numbering of this encoding is an integer that increments by one for each release. This eliminates debates about minor vs major changes. It was decided that "Change is Change". This was due in large part to the acknowledgement that what is minor to user X could be major to user Y since the major/minor designation is generally a matter of perspective.

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

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



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

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

2.2 - Relationship to Abstract Data Definition and other encodings

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

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

2.3 - Additional Guidance

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.

2.3.1 - Basic Usage

The OC-NTK profile utilizes AccessProfile elements in NTK to hold the list of approved organizations for dissemination. To specify that the profile being used is OC-NTK, simply specify the AccessPolicy element with the appropriate ACES IC-ID, `guide://2020/oc-ntk.aces`, as the value. The version is denoted by the value of the ProfileDes element specifying the IC-ID, `guide://2020/oc-ntk.des.v1`, of the DES as its value.

Specifying organizations is done by using the AccessProfileValue elements, but these values can be limited to a specific listing. Define the namespace of the list you are using in a vocabulary attribute along with the version as the value of that element. That list will be applied to the value of the other AccessProfileValue elements within the AccessProfile. These other elements are identified by using different namespaces within the vocabulary attributes, and the allowable values are specified in the CVEnumOcNtkVocab.xml CVE file. Note that a regular expression has been also included in the CVEnumOcNtkVocab list for non-USA country organizations for which no official list has been provided.

The vocabulary URI `[urn:us:gov:ic:ntk:profile:oc:originator]` specifies the originating agency of the ORCON marking while the vocabulary URI `[urn:us:gov:ic:ntk:profile:oc:authorizedDissem]` specifies agencies to which dissemination has been pre-authorized by the originating agency.

Example usage:

```
<ntk:AccessProfile ism:classification="U" ism:ownerProducer="USA">
  <ntk:AccessPolicy ism:classification="U" ism:ownerProducer="USA">guide://
2020/oc-ntk.aces</ntk:AccessPolicy>
```

```
<ntk:ProfileDes ism:classification="U" ism:ownerProducer="USA">guide://  
2020/oc-ntk.des.v1</ntk:ProfileDes>  
  <ntk:AccessProfileValue  
ntk:vocabulary="urn:us:gov:ic:cvenum:usagency:agencyacronym"  
    ism:classification="U" ism:ownerProducer="USA">1</  
ntk:AccessProfileValue>  
  <ntk:AccessProfileValue  
ntk:vocabulary="urn:us:gov:ic:ntk:profile:oc:originator"  
    ism:classification="U" ism:ownerProducer="USA">CIA</  
ntk:AccessProfileValue>  
  <ntk:AccessProfileValue  
ntk:vocabulary="urn:us:gov:ic:ntk:profile:oc:authorizedDissem"  
    ism:classification="U" ism:ownerProducer="USA">CIA</  
ntk:AccessProfileValue>  
</ntk:AccessProfile>
```

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body 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 encoding specification artifacts wherever they are located.

3.4 - Terminology

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

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

- The term “must not be specified” indicates that an attribute must not be applied to an element.

3.5 - Errors and Warnings

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

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

3.6 - Rule Identifiers

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

3.7.2 - 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 XML Stylesheet Language for Transformation (XSLT) 2.0^[22] implementation of International Organization for Standardization (ISO) Schematron^[16] provided by Rick Jelliffe at <http://schematron.com/> [<http://schematron.com/>]. Constraint rules are dependent on XPath 2.0^[21] and XSLT 2.0^[22] features. According to Mr. Jelliffe, one of the editors 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^[22] 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, meaning elements can be empty or null. According to this specification, all required elements (and certain conditional elements) must have content, other than white space.¹ Elements, which are allowed to only have text content, must have text content specified.

3.7.4 - Value Enumeration Constraints

Several elements and attributes of the OC-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.

3.7.5 - Additional Constraints

There are no additional constraints at this time.

3.7.6 - Constraint Rules

The detailed constraint rules for the OC-NTK.XML schema can be found in a separate document inside the SchematronGuide directory, in the OC-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^[19] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of OC-NTK.XML documents. The intent is to inform the development of systems capable of rendering or displaying OC-NTK.XML data for use by individuals not familiar with the details of the OC-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.

3.8.2 - Rendering Constraint Rules

The following table contains the information for the OC-NTK.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 the 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 - Business Rule Validation

As this specification has no normative schema the only necessary compliance validation step is to ensure that an instance document complies with the business rules expressed in this specification. 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 OC-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 OC-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 (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 OC-NTK.XML Schematron rules can be found in a separate document named *OC-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 summarizes major features by version for OC-NTK and all dependent specs. The "Required date" is the date when systems should support a feature based on the specified driver. For those changes driven by the CAPCO Register and Manual^[1] the date is often one year after the date of Register and Manual. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

Table 3 - 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. OC-NTK Feature Summary

Table 4 - OC-NTK Feature comparison

OC-NTK Feature Comparison		
Required Date	Feature	V1
	Identify Originating Agency	F
	Identify Agencies Permitted for Dissemination	F
	Identify Agency Acronym Vocabulary	F

Appendix B Change History

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

Table 5 - DES Version Identifier History

Version	Date	Purpose
1	16 August 2013	Initial Release

Appendix C Acronyms

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

Table 6 - Acronyms

Name	Definition
A&A	Assessment and Authorization
AAS	Authoritative Attribute Sources
ABAC	Attribute Based Access Control
ABNF	Augmented Backus-Naur Form
ACSS	Allied Collaborative Shared Services
ADD	Abstract Data Definition
AICP	Authorized IC Person
AOI	Area of Interest
AOR	Area of Responsibility
API	Applications Programming Interface
APS	Attribute Practice Statement
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BBOX	Bounding Box
BNF	Backus-Naur Form
CA	Certification Authority
CAPCO	Controlled Access Program Coordination Office
CAT	Catalog Services Interface Standard
CDR	Content Discovery and Retrieval
CF-NetCDF	Climate and Forecast - Network Common Data Format
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CMS	Cryptographic Message Syntax
CNWDI	Critical Nuclear Weapons Design Information
COMET	Completely Open Mapping Environment
CONOPS	Concept of Operations
CORBA	Common Object Request Broker Architecture

Name	Definition
CQL	Common Catalog Query Language (CQL)
CRL	Certificate Revocation List
CSW	Catalog Service for Web
CTM	Conformance Test Matrix
CUI	Controlled Unclassified Information
CVE	Controlled Vocabulary Enumeration
D & R	Discovery and Retrieval
DAA	Designated Approval Agent
DC MES	Dublin Core Metadata Element Set
DCMI	Dublin Core Metadata Initiative
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DI	Digital Identifier
DIA	Defense Intelligence Agency
DISR	DoD Information Technology Standards Registry
DN	Distinguished Name
DNI	Director of National Intelligence
DNS	Domain Name System
DOD	Department of Defense
DOE	Department of Energy
DOI	Digital Object Identifier
DOMEX	Document and Media Exploitation
EA	Enterprise Architecture
EI&A	Enterprise Integration and Architecture
E.O.	Executive Order
EBNF	Extended Backus-Naur Form
EDH	Enterprise Data Header
EPR	Endpoint Reference
ES&IS	Enterprise Search & Integration Services
ESB	Enterprise Standards Baseline
FD&R	Foreign Disclosure & Release
FOUO	For Official Use Only
FSD	Full Service Directory
FTP	File Transfer Protocol
FY	Fiscal Year

Name	Definition
GENC	Geopolitical Entities, Names, and Codes
GeoRSS	Geographic Really Simple Syndication
GeoTIFF	Geographic Tagged Image File Format
GIF	Graphics Interchange Format
GIS	Geospatial Information System
GML	Geography Markup Language
GNS	Geographic Names Server
GUIDE	Globally Unique Identifiers for Everything
GVS	GEOINT Visualization Services
HDF-EOS	Hierarchical Data Format - Earth Observing System
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
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
ICSR	Intelligence Community Standards Registry
ICTS	Intelligence Community Technical Specification
IdAM	Identity and Access Management
IDM	Interface Data Model
IDMView	Interface Data Model View
IETF	Internet Engineering Task Force
IOC	Initial Operating Capability
IP	Internet Protocol
IPT	Integrated Project Team
IRM	Information Resource Metadata
ISBN	International Standard Book Number
ISM	Information Security Marking

Name	Definition
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
ITE	Information Technology Enterprise
JPEG	Joint Photographic Experts Group
JPIP	JPEG 2000 Interactive Protocol
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWICS	Joint Worldwide Intelligence Communications System
JWT	JSON Web Token
KA	Knowledge Assertion
KML	Keyhole Markup Language
KOS	Knowledge Organization System
KVP	Key Value Pair
LDAP	Lightweight Directory Access Protocol
LIMDIS	Limited Distribution
LNI	Library of National Intelligence
MAC	Multi Audience Collection
MC&GIL	Mapping, Charting, and Geodesy Information Library
MC&GView	Mapping, Charting, and Geodesy View
MIME	Multipurpose Internet Mail Extensions
MTOM	Message Transmission Optimization Mechanism
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NGA	National Geospatial Intelligence Agency
NGDS	Net-Centric GEOINT Discovery Services
NGIC	National Ground Intelligence Center
NGT	Next Generation Trident
NIPRNet	Non-Classified Internet Protocol Router Network
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NPE	Non-Person Entity
NMEC	National Media Exploitation Center
NRO	National Reconnaissance Office

Name	Definition
NSA	National Security Agency
NSG	National System for Geospatial Intelligence
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
OGC	Open Geospatial Consortium
OGCA	Open Geospatial Consortium Australia
OGCE	Open Geospatial Consortium Europe
ONEMail	Optimized Network Email
OPM	Office of Personnel Management
OWS	OGC Web Services
PAP	Policy Administration Point
PAYL	Payload
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PK	Private Key
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
PUBS	Intelligence Publications
PURL	Persistent Uniform Resource Locator
RA	Reference Architecture
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RFC	Request for Comments
RR-ID	REST Security Encoding Specification for End-to-End Identity Propagation
SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSD	Special Security Directorate

Name	Definition
SSL	Secure Sockets Layer
STIL	St Louis Information Library
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TGN	Thesaurus of Geographic Names
TIFF	Tagged Image File Format
TIN	Triangulated Irregular Network
TLS	Transport Layer Security
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
UIAS	Unified Identity Attribute Set
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
US	United States
UUID	Universal Unique Identifier
VIRT	Virtual Coverage
W3CDTF	World Wide Web Consortium Date Time Format
WARP	Web Based Access and Retrieval Portal
WCS	Web Coverage Service
WFS	Web Feature Service
WMS	Web Map Service
WSDL	Web Service Definition Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XPath	XML Path Language
XPointer	XML Pointer Language
Xquery	XML Query
XSLT	XML Stylesheet Language for Transformations

Appendix D Bibliography

Bibliography

[1] CAPCO Register and Manual

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*.

Version 6.1; Effective: 05 April 2013; FOUO version available Intelink-TS at: <http://go.ic.gov/LtbDzSa>

Version 6.0 Administrative Update; Effective: 05 April 2013; FOUO version available on Interlink-U at: <http://purl.org/ic/standards/capco>

Version 6.0; Effective: 28 February 2013; FOUO version available on Interlink-U at: <http://purl.org/ic/standards/capco>

Version 5.1; Effective: 30 March 2012; Public version available at: http://www.dni.gov/files/documents/FOIA/Public_CAPCO_Register%20and%20Manual%20v5.1.pdf

[2] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.

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

[3] IC-ID.XML

Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.

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

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

[4] 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

[5] ICD 209

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

Available online at: http://www.dni.gov/files/documents/ICD/ICD_209_Tearline_Production_and_Dissemination.pdf [http://www.dni.gov/files/documents/ICD/ICD_209_Tearline_Production_and_Dissemination.pdf]

[6] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <http://go.ic.gov/enm8L9x>

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

[7] ICD 501

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

Available online Intelink-TS at: <http://go.ic.gov/GG61roi>

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

[8] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.

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

[9] ICPG 710.1

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

Available online Intelink-TS at: <http://go.ic.gov/yAqVQ0H>

[10] ICPM 2007-200-2

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

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

[11] ICS 500-20

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

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

Available online Intelink-U at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[12] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-U at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[13] IETF-RFC 2119

Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.

Available online at: <http://tools.ietf.org/html/rfc2119>

[14] NTK.XML

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

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

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

[15] Oxygen

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

[16] Schematron

International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.
Available online at: <http://www.schematron.com/>

[17] TAG-9-Jan-2006

W3C Technical Architecture Group (TAG). *The Disposition of Names in an XML Namespace*. 9 January 2006.
Available online at: <http://www.w3.org/2001/tag/doc/namespaceState.html>

[18] WEBARCH-15-Dec-2004

W3C. *Architecture of the World Wide Web, Volume One*. 15 December 2004.
Available online at: <http://www.w3.org/TR/webarch>

[19] XML 1.0

World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0, Second Edition*. W3C, 6 October 2000.
Available online at: <http://www.w3.org/TR/2000/REC-xml-20001006>

[20] XML Catalogs

The Organization for the Advancement of Structured Information Standards [OASIS]. *XML Catalogs*. Committee Specification 06 Aug 2001.
Available online at: <https://www.oasis-open.org/committees/entity/spec-2001-08-06.html>

[21] XPath2

World Wide Web Consortium (W3C). *XML Path Language (XPath) 2.0 (Second Edition)*. W3C Recommendation 14 December 2010 (Link errors corrected 3 January 2011).
Available online at: <http://www.w3.org/TR/xpath20/>

[22] XSLT2

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

Appendix E Points of Contact

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

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

E-mail: <ic-standards-support@intelink.gov> .

Appendix F IC CIO Approval Memo

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

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

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.^[11]