



Intelligence Community Technical Specification

XML Data Encoding Specification for Need-To-Know Metadata

Version 2015-AUG

August 13, 2015

Distribution Notice:

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

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	3
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	4
1.6.3 - Terminology	4
1.6.4 - XML Namespaces	4
1.7 - Dependencies	4
1.7.1 - Standalone and Convenience Packages	7
1.8 - Conformance	8
Chapter 2 - Development Guidance	9
2.1 - Understanding Access Control	9
2.2 - Relationship to Abstract Data Definition and other encodings	10
2.3 - NTK and Access Control	10
2.4 - Additional Guidance	11
2.4.1 - Integration into a schema	11
2.4.2 - Basic usage model	12
2.4.3 - Guidance for the specification of constraints for a particular access system	12
2.4.4 - Guidance for systems processing data containing NTK metadata	13
2.4.4.1 - Potential Data Spill procedures	13
Chapter 3 - Definitions, Interfaces, and Constraints	15
3.1 - Constraint Rule Types	15
3.2 - "Living" Constraint Rules	15
3.3 - Classified or Controlled Constraint Rules	15
3.4 - Constraint Terminology	15
3.5 - Errors and Warnings	16
3.6 - Rule Identifiers	16
3.7 - Data Validation Constraint Rules	16
3.7.1 - Purpose	16
3.7.2 - Schematron	16
3.7.3 - Non-null Constraints	17
3.7.4 - Inherited Constraints	17
3.7.5 - Value Enumeration Constraints	17
3.7.6 - Additional Constraints	18
3.7.6.1 - DES Constraints	18
3.7.7 - Constraint Rules	18
3.8 - Data Rendering Constraint Rules	18
3.8.1 - Purpose	18
3.8.2 - Rendering Constraint Rules	18
3.8.2.1 - [NTK-RENDER-00001]	18
3.8.2.2 - [NTK-RENDER-00002]	18
3.8.2.3 - [NTK-RENDER-00003]	19

3.8.2.4 - [NTK-RENDER-00004]	19
3.8.2.5 - [NTK-RENDER-00005]	19
Chapter 4 - Conformance Validation	20
4.1 - Schema Validation	20
4.2 - Business Rule Validation	20
Chapter 5 - Access Profiles	21
5.1 - Access Profile Structures	21
5.1.1 - Agency Dissemination	21
5.1.2 - Data Sphere	21
5.1.3 - Group and Individual	21
5.2 - Profile DES	21
5.3 - Vocabulary Types	22
5.3.1 - Abstract Root Types	22
5.3.2 - Vocabulary Types	23
5.3.2.1 - Built-In Vocabulary Types	23
5.3.2.2 - Further Defining Built-In Vocabulary Types	24
5.4 - Pre-Defined Access Profiles	25
5.4.1 - Exclusive Distribution (EXDIS)	25
5.4.2 - Intelligence Community Only (ICO)	26
5.4.3 - License	26
5.4.4 - Mission Need Profile	26
5.4.5 - No Distribution (NODIS)	26
5.4.6 - Originator Controlled (ORCON)	27
5.4.7 - Permissive	27
5.4.8 - Proprietary Information (PROPIN)	27
5.4.9 - Restrictive	28
Chapter 6 - Generated Guides	29
6.1 - Schema Guide	29
6.2 - Schematron Guide	30
Appendix A - Feature Summary	31
A.1 - NTK Feature Summary	31
Appendix B - Change History	33
B.1 - V2015-AUG Change Summary	33
B.2 - V10 Change Summary	36
B.3 - V9 Change Summary	37
B.4 - V8 Change Summary	37
B.5 - V7 Change Summary	38
B.6 - V6 Change Summary	39
B.7 - V5 Change Summary	39
B.8 - V4 Change Summary	40
B.9 - V3 Change Summary	40
B.10 - V2 Change Summary	41
Appendix C - List of Abbreviations	42
Appendix D - Bibliography	45
Appendix E - Points of Contact	48
Appendix F - IC CIO Approval Memo	49

List of Figures

Figure 1 - Related Specifications	7
Figure 2 - Three-legged Stool of Access Decisions	9

List of Tables

Table 1 - XML Namepaces	4
Table 2 - Dependencies	5
Table 3 - NTK Profile DES Values	22
Table 4 - NTK Dependency over Time	31
Table 5 - Feature Summary Legend	31
Table 6 - NTK Feature Comparison	31
Table 7 - DES Version Identifier History	33
Table 8 - Data Encoding Specification V2015-AUG Change Summary	34
Table 9 - Data Encoding Specification V10 Change Summary	37
Table 10 - Data Encoding Specification V9 Change Summary	37
Table 11 - Data Encoding Specification V8 Change Summary	38
Table 12 - Data Encoding Specification V7 Change Summary	38
Table 13 - Data Encoding Specification V6 Change Summary	39
Table 14 - Data Encoding Specification V5 Change Summary	39
Table 15 - Data Encoding Specification V4 Change Summary	40
Table 16 - Data Encoding Specification V3 Change Summary	40
Table 17 - Data Encoding Specification V2 Change Summary	41

List of Examples

5.1 - Individual identified by IC PKI Distinguished Name	23
5.2 - Individual identified by CAD PKI Distinguished Name	23
5.3 - Individual identified by ACSS PKI Distinguished Name	23
5.4 - Group from the IAA Service Provider Entitlement Management Service system	23
5.5 - Agencies from the USAgency.CES ^[21] specification	24
5.6 - Issues from the Mission Need ^[18] CES specification	24
5.7 - Regions from the Mission Need ^[18] CES specification	24
5.8 - Licenses from the License CES ^[17] specification	24
5.9 - Declaring USAgency Version	24
5.10 - Agency Dissem Access Profile	25

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 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 Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* ^[6] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

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

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community

Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[13] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

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

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

1.4 - Enterprise Need

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 by system and could include lists of individuals or groups permitted access, descriptions of subject matter in terms defined by the access policy, 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.

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

- IC Information Technology Enterprise (IC ITE):
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[1]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[6]

- 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^[13]
- 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^[11]
- 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]
 - Intelligence Community Policy Guidance (ICPG) 710.2, Application of Dissemination Controls: Foreign Disclosure and Release Markings^[10]

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*, ^[12] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

1.6 - Conventions

Certain technical and presentation conventions were used in the creation of this document to ensure readability and understanding.

1.6.1 - Language

The keywords "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this technical specification are to be interpreted as described in the IETF RFC 2119.^[14] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.6.3 - Terminology

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

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

1.6.4 - XML Namespaces

Namespaces referenced in this document and the prefixes used to represent them are listed in the following table. The namespace prefix of any XML Qualified Name used in any example in this document should be interpreted using the information below.

Table 1 - XML Namespaces

Prefix	URI
ntk	urn:us:gov:ic:ntk

1.7 - Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 2](#). The dependencies listed below are directly referenced in this specification (e.g. Schema, Schematron), and are normative or informative as indicated.

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the IC CIO specifications related to this specification. The graphic depicts direct and transitive dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all transitive dependencies.

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Information Security Marking</i> (ISM.XML.V2015-AUG+) ^[15]	Depends on Information Security Markings (ISM). Starting with ISM v9, the version of ISM imported is no longer normative.
<i>XML CVE Encoding Specification for US Agency</i> (USAgency.CES.V2+) ^[21]	Depends on the US Agency (US Agency) Specification. Any US Agency version 2015-FEB or above may be used.
<i>XML CVE Encoding Specification for Mission-Need</i> (MN.CES.V2015-AUG+) ^[18]	Depends on the Mission Need (MN) Specification. Any MN version 2015-AUG or above may be used.
<i>XML CVE Encoding Specification for License</i> (LIC.CES.V2015-AUG+) ^[17]	Depends on the License (LIC) Specification. Any LIC version 2015-AUG or above may be used.
Schematron ^[20]	<p>Schematron — ISO/IEC 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use XSLT 2.0^[25] query binding.</p>

Name	Dependency Description
<p>XSLT 2.0^[25] implementation of Schematron^[20] by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>
<p>Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.</p>	<p>Specification uses CVEs to encode controlled vocabularies. The use of the NTK CVEs is normative.</p>

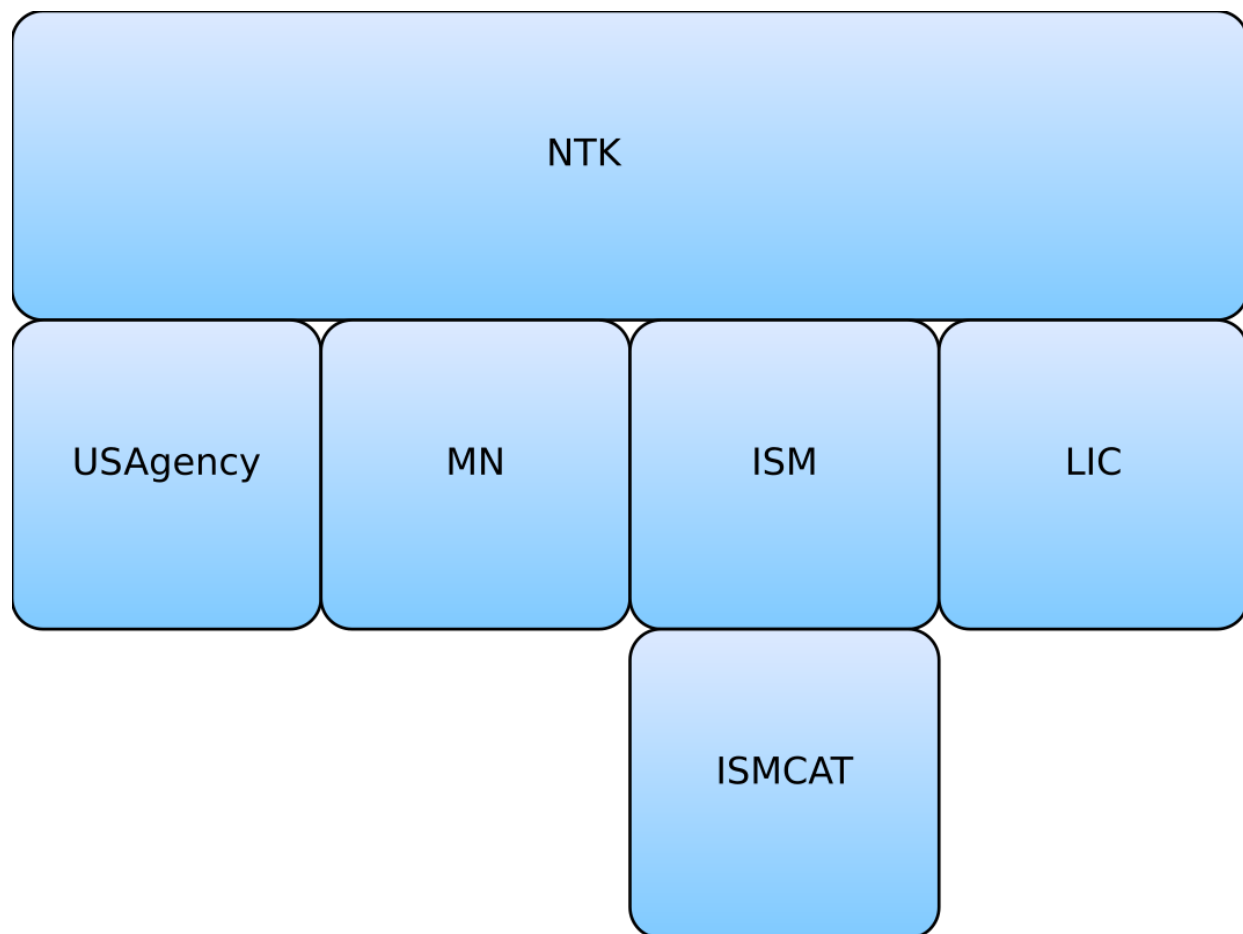


Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions of all transitive dependent specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumerations (CVEs) to validate and operate as intended.

Convenience packages convey all dependencies pre-packaged together and are tested as interoperable. When trying to mix and match versions that have not been pre-packaged together, there may be risk that a particular combination may not be compatible, especially when mixing with versions of specifications that were not available at the time of a specification's release.

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron^[20] rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[14] is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.^[23] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion='9'** to **@ism:DESVersion='10'** in the xsd:schema statement. The ability to import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications such as ISM CVE updates. The decoupling of dependency versions is not retroactive; see the dependency table for allowed dependency versions.

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

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions are based upon 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/repository/application being requested (the Who and What respectively), make up the framework that supports an access control decision. Access Policy SHOULD be constrained to use data attributes, user attributes, and context information. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. An entity MUST meet all criteria in the framework to be granted access. The concept of the access control decision framework is depicted in [Figure 2](#).

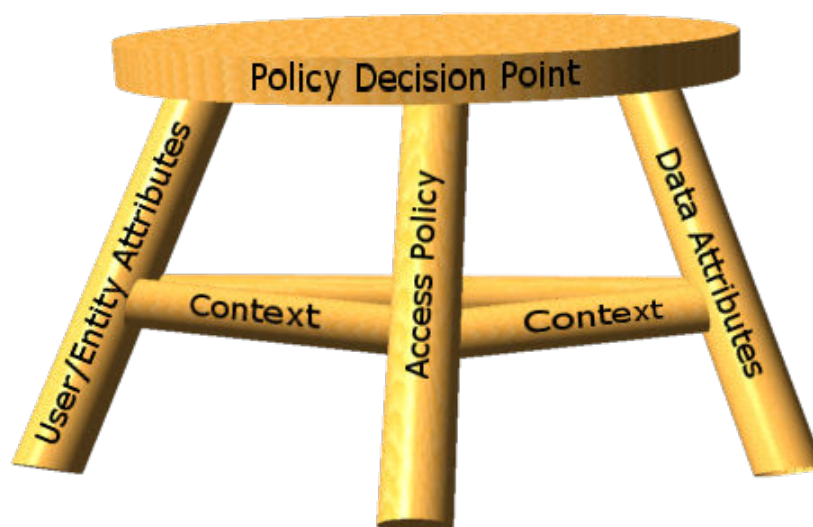


Figure 2 : Three-legged Stool of Access Decisions

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 IC CIO 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), and Need-To-Know Metadata (NTK), (which includes, but is not limited to, profiles for Intelligence Community Only, Originator Control, and Proprietary Information).

2.2 - Relationship to Abstract Data Definition and other encodings

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

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

2.3 - NTK and Access Control

This section defines the relationship NTK has to ISM and Policy Encoding Documents for the purposes of automated access control. An ISM/ NTK access control system relies on three core elements:

1. Markings about the resource such as classification:

ISM represents the security markings describing the classification, dissemination, and caveats about the resource in accordance with the IC Markings System Register & Manual. [\[2\]](#)

NTK represents metadata about a resource that impact an access control decision beyond its ISM classification markings. These metadata may supplement classification markings, as with agency dissemination NTK for Originator Controlled (ORCON) data, or provide other legal, administrative, and/or system-specific information for determining access to a given resource. To ensure data stability, NTK metadata should describe, categorize, label, and refine the resource itself instead of defining the mechanisms by which it is accessed.

Access control policies, including the Access Control Encoding Specifications (ACES) for ISM and NTK, may evolve independently of the data and entity attributes used to enforce them.

2. Markings about the Person or Non-Person Entity (NPE) desiring access:

IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) is an example of an attribute specification about Persons and NPEs.

3. Rules or policy for granting access based on the markings (ISM-ACES, NTK Policies):

The ACES associated with ISM is the Access Control Encoding Specification for ISM (ISM-ACES).

NTK metadata is expressed with one or more **ntk:AccessProfile** elements. Each **ntk:AccessProfile** MUST have an **ntk:AccessPolicy** element that contains the URN of an access profile for that NTK statement. The **ntk:AccessPolicy** URN may be used to trigger Schematron rules, and it provides a pointer to a specific section of the NTK ACES. Each statement may also contain an **ntk:ProfileDes**, which contains a URN defined in this specification. The **ntk:ProfileDes** may conditionally be required depending on the specific access policy value. A profile DES defines structural constraints for an access profile, and the URN may be used to trigger additional Schematron rules. Each **ntk:AccessProfile** must be taken into account for access to a resource based on its location within either the **ntk:RequiresAllOf** element or the **ntk:RequiresAnyOf** element.

If a system receives a resource that is protected with any NTK metadata that is not supported by that system, the resource MUST immediately be rejected, and the system MUST follow [Section 2.4.4.1 - Potential Data Spill procedures](#) if:

- The unsupported NTK Access Profile is a member of **ntk:RequiresAllOf** and not contained in an **ntk:RequiresAnyOf**, or
- The unsupported NTK Access Profile is a member of a **ntk:RequiresAnyOf** and there are unsupported NTK Access Profiles as members of the **ntk:RequiresAnyOf**.

2.4 - 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.

2.4.1 - 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).^[15] The basic process for incorporation is as follows:

- Import this schema into the “resource” schema
- Define a namespace prefix
- Allow for the **@ntk:DESVersion** attribute to be used in the “resource” schema
- Ensure (Information Security Marking Metadata) ISM is incorporated into the “resource” schema

- Add the **ntk:Access** element to the “resource” schema model at an appropriate location

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

2.4.2 - Basic usage model

This model should be used to help ensure this DES is effectively implemented in the enterprise.

- Systems that provide access control services to the enterprise must understand the NTK parameters defined in this specification. Access systems may also require custom NTK access profile structures including new parameters and syntax. Custom NTK structures are known as extensions. NTK extensions intended for exchange outside of a single agency should be coordinated with the IC CIO for publishing. Coordination with the IC CIO will help make information accessible and ensure uniform access control across the enterprise. Extensions to NTK should be documented as per [Section 2.4.3 - Guidance for the specification of constraints for a particular access system](#).
- To utilize a specific access control system, resources must be marked in accordance with the requirements of that system, including any required NTK extensions. NTK may be specified in terms of more than one access requirement in separate access profiles.

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

To utilize this DES to document how access information should be specified by resource producers, an access system owner shall define an NTK Access Profile that contains:

- The URI of the access requirement to be used; this value will be defined via the element **ntk:AccessPolicy**
- A syntax, pattern, or CVE for the **ntk:AccessProfileValue** elements.
- The URI to the NTK-Profile via the element **ntk:ProfileDes**
- Guidance on encoding, in the syntax of this DES, for all parameters necessary to be specified on the resource, other than those encoded via ISM.

Data producers and owners who wish to place resources within the access system are responsible for including the NTK Access Profile.

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.

2.4.4 - 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 access system requirement is considered separately. Logical structures are used to describe situations where more than one access requirement is needed ("AND"), or where any one of multiple access requirements ("OR") is sufficient for access:

- The element **ntk:RequiresAllOf** indicates that all of the access requirements specified must be present in order to have access to the resource.
- The element **ntk:RequiresAnyOf** is used to indicate that any one of the access requirements must be present in order to have access to the resource.

These logical structures are used within the NTK structure with the following restrictions:

- The **ntk:Access** and **ntk:ExternalAccess** elements must contain either a **ntk:RequiresAllOf** or **ntk:RequiresAnyOf** element as the first child element.
- A **ntk:RequiresAllOf** element may optionally have one **ntk:RequiresAnyOf** child element.
- A **ntk:RequiresAnyOf** element may not include any **ntk:RequiresAllOf** or **ntk:RequiresAnyOf** elements as child elements.
- **ntk:RequiresAllOf** and **ntk:RequiresAnyOf** elements require at least one **ntk:AccessProfile** element as a child element. There may be one or more access elements, each with its own access policy.

Systems handling data containing NTK metadata MUST assess and understand the NTK metadata in order to protect data appropriately. Receiving systems MUST be able to interpret and be authorized for all NTK access profiles necessary to make an access control decision. The following cases detail requirements based on the NTK logic structure:

1. When a logic structure is present indicating all of the access profiles are mandatory, the receiving system MUST understand all of the access profiles listed within this structure. If any NTK metadata is not understandable by the system, the system MUST follow [Section 2.4.4.1 - Potential Data Spill procedures](#).
2. When a logic structure exists indicating at least one access profile is required, then the receiving system MUST understand at least one of the access profiles listed in the structure. If no understandable NTK metadata is present, the system MUST follow [Section 2.4.4.1 - Potential Data Spill procedures](#).

2.4.4.1 - Potential Data Spill procedures

If a resource has unknown NTK metadata required to be understood based on the NTK logic structure, then there is the potential of a data spill. The following steps outline the required actions a system MUST take:

1. The files MUST be segregated and protected via the most restrictive manner available.
2. The cognizant Information Systems Security Manager (ISSM) MUST be contacted.
3. The submitter MUST be contacted to facilitate assessment of the potential spill.

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body for resolution. Rendering constraint rules define constraints on the display and rendering of documents. While expressed in a similar manner to the data validation constraint rules, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

3.2 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of business rules addressed by authoritative guidance. These rules will be expanded and modified as the model matures, and as applicable security marking policies change.

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

3.3 - Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the encoding specification artifacts wherever they are located.

3.4 - Constraint Terminology

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

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

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

3.5 - Errors and Warnings

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

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

3.6 - Rule Identifiers

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

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

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.

3.7.2 - Schematron

Schematron^[20] is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document **MUST** meet, exactly as English may be used to convey normative criteria.

It is not necessary for implementers to use the specific Schematron encoding in this specification, and implementers **MAY** use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator **MUST** find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

For better understanding, the Schematron^[20] rules for this specification may be executed in *Oxygen*[®]^[19] or with an XSLT 2.0^[25]-compliant processor using the XSLT 2.0^[25] transforms in the

Schematron implementation from Rick Jelliffe (see [XSLT 2.0 implementation of Schematron by Rick Jelliffe](#) in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0^[24] and XSLT 2.0^[25] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:^[16]

By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this.



Note

For convenience, the specification package provides the XSLT 2.0^[25] implementation of Schematron^[20] along with a compiled version of the rules.

3.7.3 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content, meaning elements can be empty or null. According to this specification, all required elements (and certain conditional elements) **MUST** have content, other than white space.¹ Elements, which are allowed to only have text content, **MUST** have text content specified.

3.7.4 - Inherited Constraints

In an instance of 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 1.7 - Dependencies](#).

3.7.5 - Value Enumeration Constraints

Several elements and attributes of the NTK.XML model use 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.

¹“White space” is defined in XML 1.0^[22] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

3.7.6 - Additional Constraints

3.7.6.1 - DES Constraints

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

3.7.7 - 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.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display 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.

3.8.2 - Rendering Constraint Rules

3.8.2.1 - [NTK-RENDER-00001]

- Severity: [Error]
- Description: If an NTK assertion with an ntk:AccessPolicy value of `urn:us:gov:ic:aces:ntk:oc` exists, then
 - The value of ntk:AccessProfileValue with attribute ntk:qualifier="originator" MUST be rendered as the originating agency.
 - The values of all ntk:AccessProfileValue elements with attribute ntk:qualifier="dissemto" MUST be rendered as the list of agencies authorized for access.
- Human Readable Description: Systems used for rendering data containing ORCON MUST produce rendered documents that comply with ICPG 710.1^[9], and any guidelines described therein.

3.8.2.2 - [NTK-RENDER-00002]

- Severity: [Warning]
- Description: If an NTK assertion with an ntk:AccessPolicy value of `urn:us:gov:ic:aces:ntk:nd` exists, then

- The values of ntk:AccessProfileValue elements with ntk:vocabulary attributes that start with 'group:' SHOULD be rendered as groups authorized for access.
- The values of ntk:AccessProfileValue elements with ntk:vocabulary attributes that start with 'individual:' SHOULD be rendered as individuals authorized for access.
- Human Readable Description: Systems used for rendering data containing No Distribution (NODIS) SHOULD produce rendered documents that display the groups and/or individuals authorized for access.

3.8.2.3 - [NTK-RENDER-00003]

- Severity: [Warning]
- Description: If an NTK assertion with an ntk:AccessPolicy value of `urn:us:gov:ic:aces:ntk:xd` exists, then
 - The value of ntk:AccessProfileValue with attribute ntk:qualifier="originator" SHOULD be rendered as the originating agency.
 - The values of all ntk:AccessProfileValue elements with attribute ntk:qualifier="dissemto" SHOULD be rendered as the list of agencies authorized for access.
- Human Readable Description: Systems used for rendering data containing Exclusive Distribution (EXDIS) SHOULD produce rendered documents that display the originator and agencies authorized for access.

3.8.2.4 - [NTK-RENDER-00004]

- Severity: [Warning]
- Description: If an NTK assertion with an ntk:AccessPolicy value that starts with `urn:us:gov:ic:aces:ntk:propin:` exists, then
 - The values of ntk:AccessProfileValue elements with ntk:vocabulary attributes that start with 'group:' SHOULD be rendered as groups authorized for access.
 - The values of ntk:AccessProfileValue elements with ntk:vocabulary attributes that start with 'individual:' SHOULD be rendered as individuals authorized for access.
- Human Readable Description: Systems used for rendering data containing Proprietary Information (PROPIN) SHOULD produce rendered documents that display the groups and/or individuals authorized for access.

3.8.2.5 - [NTK-RENDER-00005]

- Severity: [Warning]
- Description: For NTK assertions not defined above and in the absence of specific rendering guidance, render the Access Policy URN and ntk:AccessProfileValues grouped by Vocabulary Type.
- Human Readable Description: Systems used for rendering data containing NTK assertions not defined above and in the absence of specific rendering guidance, SHOULD produce rendered documents that display the Access Policy URN and ntk:AccessProfileValues grouped by Vocabulary Type.

Chapter 4 - Conformance Validation

An instance document conforms with this specification if it conforms to all normative guidance of this specification and this specification's dependencies and it passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

4.1 - Schema Validation

An instance document **MUST** comply with the schemas for this specification and this specification's dependencies, and schema validation **SHOULD** occur prior to other validation steps. If schema validation fails, results from later steps may be indeterminate.

4.2 - Business Rule Validation

An instance document **MUST** comply with the business rules expressed in this specification and those expressed in this specification's dependencies. The business rules in this specification are expressed in Schematron, but it is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers **MAY** use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator **MUST** find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

Chapter 5 - Access Profiles

5.1 - Access Profile Structures

NTK provides a set of predefined access profile structures to help meet many enterprise requirements for need-to-know metadata. The predefined structures are Data Sphere, Group & Individual, and Agency Dissemination. Each structure is designated with a specific **ntk:ProfileDes** URN. For example, the use of the Agency Dissemination profile DES value — `urn:us:gov:ic:ntk:profile:agencydissem` — allows for the use of a list of authorized recipients by government agency.

While certain access profile structures are needed within the enterprise, caution should be exercised when applying these structures to data. Implementers should recognize that the use of Group and Individual access profile structures will carry a long-term maintenance tail that could result in loss of access to data over time.

5.1.1 - Agency Dissemination

The Agency Dissemination structure is used for need-to-know metadata based on Government agencies and top-level organizations. It consists of a list that specified the originating agency and any other agencies to which the information may be disseminated. ORCON is an example of data that would need to use the Agency Dissemination structure.

5.1.2 - Data Sphere

The Data Sphere structure is used for need-to-know metadata based on data attributes. These attributes are sometimes called “data sensitivities” and are considered to be an inherent part of the data. Data Sphere assertions are used to express access restrictions based on these inherent data attributes such as licensing, mission need, etc.

5.1.3 - Group and Individual

The Group and Individual structure is used for need-to-know metadata based on groups and/or individuals, which may be used to represent many types of person-based labels or categories including roles, COIs, etc. For the purposes of the Group NTK structure, groups on data map to the concept of some person-based categorization provisioned in an authoritative attribute source. Individuals are commonly identified by fully-qualified Distinguished Name (DN). Some sources that might be used to find a DN are IC Public Key Infrastructure (PKI), Cryptologic Agencies Domain (CAD) PKI, and Allied Collaborate Shared Services (ACSS) PKI. A vocabulary MAY be defined that uses any authoritative source that provides person or group-based labels or categorization. For example, IAA Service Provider Entitlement Management Service is an authoritative attribute source for entitlements that may be used as a source for a Group structure.

5.2 - Profile DES

Access profile structures are indicated by the use of an appropriate **ntk:ProfileDES** value. The **ntk:ProfileDES** value unambiguously defines the allowable structures, and these rules are enforced by Schematron rules. New **ntk:ProfileDES** values must be defined in order to use

combinations of access profile structures not already defined (i.e. only one profile DES may be used at a time). NTK has three pre-defined **ntk:ProfileDES** values.

Table 3 - NTK Profile DES Values

Profile DES	URN
Agency Dissem	urn:us:gov:ic:ntk:profile:agencydissem
Data Sphere	urn:us:gov:ic:ntk:profile:datasphere
Group & Individual	urn:us:gov:ic:ntk:profile:grp-ind

5.3 - Vocabulary Types

Vocabulary Types define a vocabulary's source, including version or other identifying information. The **@ntk:vocabulary** attribute provides the identifier for the Vocabulary Type of an **ntk:AccessProfileValue** value; it is a required attribute.

NTK assertions may use built-in Vocabulary Types or new VocabularyTypes defined according to agency or mission use cases. Vocabularies are declared with the **ntk:VocabularyType** element. The **ntk:VocabularyType** element has three attributes: **@ntk:name**, **@ntk:source**, and **@ntk:sourceVersion**.

@ntk:name	<p>The unique identifier of a Vocabulary (required)</p> <p>Vocabulary Type names MUST inherit from a vocabulary root type using the appropriate root type prefix.</p>
@ntk:source	<p>The source of a Vocabulary</p> <p>A vocabulary source may be a CVE, system, or other source. For an IC CIO defined CVE, the @ntk:source value should be the XML namespace defined for the CVE. This value is required for user-defined vocabularies and optional for predefined vocabularies. If a value is specified for a predefined vocabulary, the value must match the source definition in this specification.</p>
@ntk:sourceVersion	<p>The version or other identifying attribute of a Vocabulary (optional)</p> <p>For IC CIO defined CVEs, the @ntk:sourceVersion should be the value of the @cve:CVEVersion attribute defined in the CVE.</p>

5.3.1 - Abstract Root Types

There are four vocabulary root types, each with a corresponding prefix to be used in Vocabulary Type names. Root types provide built-in, abstract concepts that must be sub-classed for a

Vocabulary Type instance. Sub-classing enables typing for all **ntk:AccessProfileValue** values. Root types MUST be defined in this DES; custom root types are forbidden. The four root types are

- Individual (prefix `individual:`)
- Group (prefix `group:`)
- Organization (prefix `organization:`)
- Data Sphere (prefix `datasphere:`)

Individual and Group are for vocabularies based on people. Data Sphere is for vocabularies based on data attributes such as content indicators or categorization information. Organization is for vocabularies based on agency affiliation. Organization can be considered to straddle the line between people and data attributes. In the world of attribute-based access control, it is generally considered preferable to utilize data attributes instead of directly using person or group based restrictions, so Data Sphere may be preferred from an Attribute Based Access Control(ABAC) perspective.

5.3.2 - Vocabulary Types

Vocabulary types are derived from root types and provide the ability to define a concrete vocabulary type.

5.3.2.1 - Built-In Vocabulary Types

To facilitate ease of use and reduce common repetitive information in instances of NTK.XML, there are several built-in subclasses defined in this DES.

Built-In Individual Vocabulary Types

Example 5.1. Individual identified by IC PKI Distinguished Name

```
<ntk:VocabularyType ntk:name="individual:icpki" ntk:source="IC-PKI:DN"/>
```

Example 5.2. Individual identified by CAD PKI Distinguished Name

```
<ntk:VocabularyType ntk:name="individual:cadpki" ntk:source="CAD-PKI:DN"/>
```

Example 5.3. Individual identified by ACSS PKI Distinguished Name

```
<ntk:VocabularyType ntk:name="individual:acsspki" ntk:source="ACSS-PKI:DN"/>
```

Built-In Group Vocabulary Types

Example 5.4. Group from the IAA Service Provider Entitlement Management Service system

```
<ntk:VocabularyType ntk:name="group:iaaems" ntk:source="JWICS:IAAEMS"/>
```

Built-In Organization Vocabulary Types

Example 5.5. Agencies from the USAgency.CES^[21] specification

```
<ntk:VocabularyType ntk:name="organization:usa-agency"
  ntk:source="urn:us:gov:ic:cvenum:usagency:agencyacronym"/>
```

Built-In DataSphere Vocabulary Types

Example 5.6. Issues from the Mission Need^[18] CES specification

```
<ntk:VocabularyType ntk:name="datasphere:mn:issue"
  ntk:source="urn:us:gov:ic:cvenum:mn:issue"/>
```

Example 5.7. Regions from the Mission Need^[18] CES specification

```
<ntk:VocabularyType ntk:name="datasphere:mn:region"
  ntk:source="urn:us:gov:ic:cvenum:mn:region"/>
```

Example 5.8. Licenses from the License CES^[17] specification

```
<ntk:VocabularyType ntk:name="datasphere:license"
  ntk:source="urn:us:gov:ic:cvenum:lic:license"/>
```

5.3.2.2 - Further Defining Built-In Vocabulary Types

For built-in vocabulary types based on CVEs, it is necessary to specify the source version using the **@ntk:sourceVersion** attribute of an **ntk:VocabularyType** element. The **@ntk:name** attribute of the **ntk:VocabularyType** element must be identical to the built-in type. If specified, the **@ntk:source** attribute must be identical to the built-in source. Once a source or a version is specified, it is not possible to override those values. It is not necessary to specify a source version for other types of vocabularies (e.g. `group:iaaems` does not require a source version since it is not based on a CVE). Currently, the source version must be specified for `organization:usa-agency`, `datasphere:mn:issue`, `datasphere:mn:region`, and `datasphere:license` built-in vocabulary types.

For example, when using the built-in `organization:usa-agency` vocabulary, it is necessary to specify the USAgency CES version. The instance document must declare the version with an **ntk:VocabularyType**. If the instance document used the 2015-FEB version of USAgency^[21], it would declare the version in the following way:

Example 5.9. Declaring USAgency Version

```
<ntk:VocabularyType ntk:name="organization:usa-agency"
  ntk:sourceVersion="201502"/>
```

The full instance might look something like:

Example 5.10. Agency Dissem Access Profile

```
<ntk:Access ism:classification="U" ism:ownerProducer="USA">
  <ntk:RequiresAnyOf>
    <ntk:AccessProfileList>
      <ntk:AccessProfile ism:classification="U" ism:ownerProducer="USA">
        <ntk:AccessPolicy>urn:us:gov:ic:aces:ntk:oc</ntk:AccessPolicy>
        <ntk:ProfileDes
          >urn:us:gov:ic:ntk:profile:agencydissem</ntk:ProfileDes>
        <ntk:VocabularyType ntk:name="organization:usa-agency"
          ntk:sourceVersion="201502"/>
        <ntk:AccessProfileValue ntk:vocabulary="organization:usa-agency"
          qualifier="originator">CIA</ntk:AccessProfileValue>
        <ntk:AccessProfileValue ntk:vocabulary="organization:usa-agency"
          qualifier="dissemto">DNI</ntk:AccessProfileValue>
        <ntk:AccessProfileValue ntk:vocabulary="organization:usa-agency"
          qualifier="dissemto">NSA</ntk:AccessProfileValue>
        </ntk:AccessProfile>
      </ntk:AccessProfileList>
    </ntk:RequiresAnyOf>
  </ntk:Access>
```

5.4 - Pre-Defined Access Profiles

NTK provides a number of pre-defined Access Profiles, which are indicated by an **ntk:AccessPolicy** value. An access policy may provide additional restrictions on structure and vocabulary defined by the Profile DES. For example, the Restrictive profile requires the Group & Individual Profile DES, but it forbids the use of individuals in an assertion. Access Profiles may define new Schematron rules, which trigger on a specific **ntk:AccessPolicy** value. These new rules are in addition to any rules defined for the associated Profile DES.

Access control decisions must conform to the logic defined in an ACES, and specific access control logic for these profiles is defined in the NTK ACES. Implementers are free to develop an ACES and define new access profiles for use in local exchanges, but systems **MUST** reject information marked with a profile that is not defined for that system. The following sections provide the Access Policy URN, the associated Profile DES, and any restrictions for use of profile structures and vocabularies. The following sections are for descriptive purposes and are not intended as a substitute for the NTK ACES.

5.4.1 - Exclusive Distribution (EXDIS)

Access Policy: urn:us:gov:ic:aces:ntk:xd

Profile DES: urn:us:gov:ic:ntk:profile:agencydissem

EXDIS is a Department of State marking that restricts a resource from being shared outside of the originating agency without prior approval of the originating agency. The XD-NTK access profile is used to mark information that must be protected in accordance with the EXDIS policies defined in the NTK ACES. XD-NTK requires the Agency Dissemination Profile DES. There are no additional restrictions.

This access profile is limited in use to the `organization:usa-agency` vocabulary.

5.4.2 - Intelligence Community Only (ICO)

Access Policy: `urn:us:gov:ic:aces:ntk:ico`

Profile DES: N/A

The Intelligence Community Only (ICO) profile is used to mark information that must be protected in accordance with the ICO policies defined in the NTK ACES. ICO is used without a Profile DES value since no additional structure is required.

5.4.3 - License

Access Policy: `urn:us:gov:ic:aces:ntk:license`

Profile DES: `urn:us:gov:ic:ntk:profile:datasphere`

The License profile is used to mark information that must be protected in accordance with a licensing agreement as defined in an ACES. License is used with the Data Sphere Profile DES. There are no additional restrictions.

This access profile is limited to use of vocabularies `datasphere:license` for the access profile values.

5.4.4 - Mission Need Profile

Access Policy: `urn:us:gov:ic:aces:ntk:mn`

Profile DES: `urn:us:gov:ic:ntk:profile:datasphere`

Mission Need (MN) is used to express issues and regions that affect access control in accordance with the MN policies defined in the NTK ACES. Mission Need Profile is used with the Data Sphere Profile DES. Mission Need Profile assertions are restricted to `datasphere:mn:issue` and `datasphere:mn:region` vocabularies.

This access profile is limited to use of vocabularies `datasphere:mn:issue` and `datasphere:mn:region` for the access profile values.

5.4.5 - No Distribution (NODIS)

Access Policy: `urn:us:gov:ic:aces:ntk:nd`

Profile DES: `urn:us:gov:ic:ntk:profile:grp-ind`

NODIS is a Department of State (DOS) marking that restricts the distribution of a resource to named individuals. The ND-NTK access profile is used to mark information that must be protected

in accordance with the NODIS policies defined in the NTK ACES. NODIS is used with the Group & Individual Profile DES. There are no additional restrictions.

This access profile is limited to use with vocabularies that start with `group:` or `individual:` for the access profile values.

5.4.6 - Originator Controlled (ORCON)

Access Policy: `urn:us:gov:ic:aces:ntk:oc`

Profile DES: `urn:us:gov:ic:ntk:profile:agencydissem`

ORCON restricts a resource from being shared outside of the originating agency without prior approval of the originating agency. The IC Markings System Register & Manual^[3] states this marking allows originators to maintain knowledge, supervision, and control of the distribution of the ORCON information beyond its original dissemination, and further dissemination of ORCON information requires advance permission from the originator. The ORCON access profile is used to mark information that must be protected in accordance with the ORCON policies defined in the NTK ACES. ORCON must be used with the Agency Dissem Profile DES. There are no additional restrictions.

This access profile is limited in use to the `organization:usa-agency` vocabulary.

5.4.7 - Permissive

Access Policy: `urn:us:gov:ic:aces:ntk:permissive`

Profile DES: `urn:us:gov:ic:ntk:profile:grp-ind`

The Permissive profile provides an association mechanism for groups or individuals. The Permissive profile is used to mark information that must be protected in accordance with the Permissive group policies defined in the NTK ACES. Permissive MUST be used with the Group & Individual Profile DES. There are no additional restrictions.

This access profile is limited to use with vocabularies that start with `group:` or `individual:` for the access profile values.

5.4.8 - Proprietary Information (PROPIN)

Access Policies:

`urn:us:gov:ic:aces:ntk:propin:1`

`urn:us:gov:ic:aces:ntk:propin:2`

Any that start with `urn:us:gov:ic:aces:ntk:propin:`

Profile DES: `urn:us:gov:ic:ntk:profile:grp-ind` (NOTE: Profile DES required for profile 2. Profile DES required for profile 1 only if groups or individuals are used.)

PROPIN is a marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value, as defined by the IC Markings System Register & Manual^[3]. The PROPIN profile is used to mark data that must be protected in accordance with the PROPIN policies defined in the NTK ACES. PROPIN is used with the Group & Individual Profile DES. Multiple access policies are defined in the NTK ACES, and each access policy may define additional restrictions on the use groups and individuals. The second access policy of PROPIN (`urn:us:gov:ic:aces:ntk:propin:2`) requires at least one group or individual.

Both of the profiles defined here are limited to use with vocabularies starting with `group:` or `individual:` for access profile values.

5.4.9 - Restrictive

Access Policy: `urn:us:gov:ic:aces:ntk:restrictive`

Profile DES: `urn:us:gov:ic:ntk:profile:grp-ind`

The Restrictive profile provides an association mechanism for groups. The Restrictive profile is used to mark information that must be protected in accordance with the Restrictive group policies defined in the NTK ACES. Restrictive MUST be used with the Group & Individual Profile DES, but Restrictive may only be used with groups. That is, the use of individuals with Restrictive is forbidden.

This access profile is solely restricted to use with vocabularies that start with `group:` for access profile values.

Chapter 6 - Generated Guides

6.1 - 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@^[19]*, 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.

6.2 - 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 4 - NTK Dependency over Time

Dependent DES	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V2015-AUG
ISM	V3	V4	V5	V6	V7	V8	V9	V9+	V9+	V9+	V2015-AUG+
LIC											V2015-AUG+
MN											V2015-AUG+
USAgency											V2015-FEB+

The following table summarizes major features by version for NTK.

Table 5 - 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. NTK Feature Summary

Table 6 - NTK Feature Comparison

NTK Feature Comparison												
Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V2015-AUG
	Schematron ^[20] Implementation of rules	N	N	F	F	F	F	F	F	F	F	F
	Portion Level NTK	N	N	N	N	N	N	F	F	F	F	F
	Support multiple versions of ISM.XML	N	N	N	N	N	N	N	F	F	F	F
	Support AllOf and AnyOf structures	N	N	N	N	N	N	N	N	F	F	F
	Agency Dissem Profile	N	N	N	N	N	N	N	N	N	N	F
	Data Sphere Profile	N	N	N	N	N	N	N	N	N	N	F
	Group & Individual Profile	N	N	N	N	N	N	N	N	N	N	F
	NTK Profiles consolidated into NTK	N	N	N	N	N	N	N	N	N	N	F
	EXDIS access profile	N	N	N	N	N	N	N	N	N	N	F
	ICO access profile	N	N	N	N	N	N	N	N	N	N	F
	License access profile	N	N	N	N	N	N	N	N	N	N	F

NTK Feature Comparison												
Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V2015-AUG
	MN access profile	N	N	N	N	N	N	N	N	N	N	F
	NODIS access profile	N	N	N	N	N	N	N	N	N	N	F
	ORCON access profile	N	N	N	N	N	N	N	N	N	N	F
	Permissive access profile	N	N	N	N	N	N	N	N	N	N	F
	PROPIN access profile	N	N	N	N	N	N	N	N	N	N	F
	Restrictive access profile	N	N	N	N	N	N	N	N	N	N	F
	Ability to define custom vocabulary types	N	N	N	N	N	N	N	N	N	N	F
	Built-in Vocabulary Types	N	N	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.10 - V2 Change Summary
3	6 December 2010	Routine revision to technical specification. For details of changes, see Section B.9 - V3 Change Summary
4	11 April 2011	Routine revision to technical specification. For details of changes, see Section B.8 - V4 Change Summary
5	19 September 2011	Routine revision to technical specification. For details of changes, see Section B.7 - V5 Change Summary
6	27 February 2012	Routine revision to technical specification. For details of changes, see Section B.6 - V6 Change Summary
7	17 July 2012	Routine revision to technical specification. For details of changes, see Section B.5 - V7 Change Summary
8	21 January 2013	Routine revision to technical specification. For details of changes, see Section B.4 - V8 Change Summary
9	5 April 2013	Routine revision to technical specification. For details of changes, see Section B.3 - V9 Change Summary
10	16 August 2013	Routine revision to technical specification. For details of changes, see Section B.2 - V10 Change Summary
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.1 - V2015-AUG Change Summary

B.1 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Combine profiles into unified specification
- Create profiles to support community requirements

The following table summarizes the changes made to V10 in developing V2015-AUG.

Table 8 - Data Encoding Specification V2015-AUG Change Summary

Change	Artifacts changed	Compatibility Notes
Dropped ntk:AccessIndividualList and ntk:AccessGroupList elements	Schematron NTK-ID-00002 modified	Data generation and ingestion systems need to be updated to use the modified rule.
Incorporate OC-NTK, ICO-NTK, PROPIN-NTK	DES	No impact to data generation or ingestion systems.
Update NTK schema to support moving profiles into NTK	Schema	Data generation and ingestion systems need to be updated to use the new schema.
Added Schematron rules to enforce built-in vocabulary requirements.	Schematron NTK-ID-00029 added NTK-ID-00032 added NTK-ID-00033 added	Data generation and ingestion systems need to be updated to use the new rules.
Added Schematron rules to enforce general profile constraints	Schematron NTK-ID-00006 modified NTK-ID-00007 modified NTK-ID-00009 modified NTK-ID-00018 added NTK-ID-00019 added NTK-ID-00020 added NTK-ID-00023 added NTK-ID-00024 added NTK-ID-00025 added NTK-ID-00027 added NTK-ID-00041 added NTK-ID-00042 added NTK-ID-00043 added NTK-ID-00044 added NTK-ID-00045 added	Data generation and ingestion systems need to be updated to use the new rules.

Change	Artifacts changed	Compatibility Notes
Added Schematron rules to support Agency Dissemination profile	Schematron NTK-ID-00028 added NTK-ID-00035 added	Data generation and ingestion systems need to be updated to use the new rules.
Added Schematron rules to support Data Sphere profile	Schematron NTK-ID-00021 added NTK-ID-00022 added	Data generation and ingestion systems need to be updated to use the new rules.
Added Schematron rules to support new Group & Individual profile	Schematron NTK-ID-00016 added NTK-ID-00017 added	Data generation and ingestion systems need to be updated to use the new rules.
Added EXDIS access profile (utilizes Agency Dissemination profile)	Schematron NTK-ID-00040 added	Data generation and ingestion systems need to be updated to use the new rules.
Incorporated ICO access profile (use of a profile DES not permitted)	Schematron NTK-ID-00026 added	Data generation and ingestion systems need to be updated to use the new rules.
Added License access profile (utilizes Data Sphere profile)	DES	Data generation and ingestion systems need to be updated to use the new rules.
Added MN access profile (uses Data Sphere profile)	Schematron NTK-ID-00010 added NTK-ID-00011 added NTK-ID-00012 added NTK-ID-00013 added NTK-ID-00030 added NTK-ID-00031 added	Data generation and ingestion systems need to be updated to use the new rules.
Added ND access profile (uses Group & Individual profile)	DES	Data generation and ingestion systems need to be updated to use the new rules.
Incorporated ORCON access profile (utilizes Agency Dissemination profile)	Schematron NTK-ID-00039 added	Data generation and ingestion systems need to be updated to use the new rules.
Added Permissive access profile (utilizes Group & Individual profile)	Schematron NTK-ID-00034 added	Data generation and ingestion systems need to be updated to use the new rules.

Change	Artifacts changed	Compatibility Notes
Added PROPIN Schematron rules	Schematron NTK-ID-00014 added NTK-ID-00015 added NTK-ID-00036 added	Data generation and ingestion systems need to be updated to use the new rules.
Added Restrictive access profile (utilizes Group & Individual profile)	Schematron NTK-ID-00037 added NTK-ID-00038 added	Data generation and ingestion systems need to be updated to use the new rules.
Updated code descriptions to improve readability	Schematron	No impact to data generation and ingestion systems.
Removed support for @ntk:access portion marking	DES Schema Schematron NTK-ID-00008 removed	Data generation and ingestion systems need to be updated to only use the element structure.
Added support for built-in vocabulary types	DES Schematron NTK_XML.sch modified	Data generation and ingestion systems need to be updated to support the built-in vocabulary types.
Add a rule that requires text for NTK elements AccessPolicy, ProfileDes, and AccessProfileValue	Schematron NTK-ID-00048 added	Data generation and ingestion systems need to be updated to support the built-in vocabulary types.
Add rules so that ORCON and EXDIS profiles require ProfileDes with type agencydissem	Schematron NTK-ID-00049 added NTK-ID-00050 added	Data generation and ingestion systems need to be updated to support the built-in vocabulary types.
Add rule to enforce restriction of ProfileDes values for IC CIO Reserved Portion.	Schematron NTK-ID-00051 added	Data generation and ingestion systems need to be updated to support the built-in vocabulary types.

B.2 - V10 Change Summary

Significant drivers for Version 10 include:

- Access Control Policy URIs
- Profile URIs

The following table summarizes the changes made to V9 in developing V10.

Table 9 - Data Encoding Specification V10 Change Summary

Change	Artifacts changed	Compatibility Notes
New attribute additionalAccessControlReference added to reference relevant access control policies.	Schema	Data generation and ingestion systems need to be updated to use the new attribute.
New element Profile added to AccessGroupType, AccessIndividualType, and AccessProfileType. This element is an IC-ID reference to the Profile used by the NTK statement. Currently, it also contains attributes with human readable values for the Profile name and version number.	Schema	Data generation and ingestion systems need to be updated to use the new element.

B.3 - V9 Change Summary

Significant drivers for Version 9 include:

- CMSTT for addition of AND logic

The following table summarizes the changes made to V8 in developing V9.

Table 10 - Data Encoding Specification V9 Change Summary

Change	Artifacts changed	Compatibility Notes
Added RequiresAnyOf and RequiresAllOf elements and portion marking "AND" delimiter	Schema Examples Schematron NTK-ID-00002 Changed	Data generation and ingestion systems need to be updated to use the new values and adhere to the new rule.
Changed element name from "AccessSystemName" to "AccessPolicy"	DES Schema Examples	Data generation and ingestion systems need to be updated to use the new value.

B.4 - V8 Change Summary

Significant drivers for Version 8 include:

- See ISM V10 drivers

The following table summarizes the changes made to V7 in developing V8.

Table 11 - Data Encoding Specification V8 Change Summary

Change	Artifacts changed	Compatibility Notes
Added schematron rules to ensure that the versions of the imported specs meet the minimum allowed versions.	Schematron NTK-ID-00009 Added	Data generation and ingestion systems need to be updated enforce the new rules.
Update ISM to V10	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification.
Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISMv9	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.

B.5 - 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 12 - 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 complexContent to simpleContent [artf12153].	Schema	Should only impact some code generation systems.
Added external reference attribute to indicate ntk refers to external content	Schema	Ingest and data generation systems should be updated

Change	Artifacts changed	Compatibility Notes
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.6 - 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 13 - 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.7 - 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 14 - 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.

Change	Artifacts changed	Compatibility Notes
Fixed type errors generated when using a schema-aware processor.	Constraint Rules	Should not affect data.

B.8 - 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 15 - 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.9 - 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 16 - 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

Change	Artifacts changed	Compatibility Notes
Remove Appendix H Reading the Schematics	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.

B.10 - 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 17 - 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 List of Abbreviations

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

ABAC	Attribute Based Access Control
ACSS	Allied Collaborative Shared Services
ACES	Access Control Encoding Specification
ADD	Abstract Data Definition
ARH	Access Rights and Handling
CAD	Cryptologic Agencies Domain
CES	Controlled Vocabulary Enumeration Encoding Specification
CMSTT	Common Metadata Standards Tiger Team
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DN	Distinguished Name
DNI	Director of National Intelligence
DOS	U.S. Department of State
EXDIS	Exclusive Distribution
FOUO	For Official Use Only
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
IC-ID	IC Identifier
ICD	Intelligence Community Directive
ICO	Intelligence Community Only
ICPG	Intelligence Community Program Guidance

ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISM	Information Security Markings
ISM-ACES	Access Control Encoding Specification for Information Security Marking
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
IT	Information Technology
MN	Mission Need Profile
No Distribution	Data Encoding Specification for No Distribution Need-To-Know
NPE	Non-Person Entity
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
ORCON	See OC.
PDF	Portable Document Format
PDP	Policy Decision Point
PKI	Public Key Infrastructure
PROPIN	Proprietary Information
PUBS	Intelligence Publications
TDF	Trusted Data Format
UIAS	Unified Identity Attribute Set
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name

XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

Bibliography

[1] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at: <http://go.ic.gov/4X6TOc1>

[2] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. Available online Intelink-TS at: <http://go.ic.gov/qBpc2JN>
Available online Intelink-U at: <https://intelshare.intelink.gov/sites/odni/cio/ea/library/Technical%20Specifications/TechSpec%20Policy%20Regs/IC%20Markings/default.aspx>

[3] IC Markings DEC 2014

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2014.
Available online Intelink-TS at: <http://go.ic.gov/T6ez94Z>

[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%20209%20Tearline%20Production%20and%20Dissemination.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/5Ot5sbK>
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

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

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

[10] ICPG 710.2

Director of National Intelligence. *Application of Dissemination Controls: Foreign Disclosure and Release Markings*. Intelligence Community Policy Guidance 710.2. 20 March 2014.

Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710-2_403-5.pdf

[11] 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>

[12] ICS 500-20

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

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

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

[13] ICS 500-21

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

Available online Intelink-TS at: <http://go.ic.gov/cWYv9nw>

Available online Intelink-U at: <http://www.purl.org/ic/standards/policy/ICS500-21>

[14] IETF-RFC 2119

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

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

[15] ISM.XML

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

Available online Intelink-TS at: <http://go.ic.gov/3oipfOY>

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

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

[16] Jelliffe

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

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

[17] LIC.CES

- Office of the Director of National Intelligence. *XML CVE Encoding Specification for License (LIC.CES)*.
Available online Intelink-U at:<http://purl.org/IC/Standards/LIC>
Available online at:<http://purl.org/IC/Standards/public>
- [18] MN.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Mission-Need (MN.CES)*.
Available online Intelink-U at:<http://purl.org/IC/Standards/MN>
Available online at:<http://purl.org/IC/Standards/public>
- [19] Oxygen
SyncRO Soft. <oXygen/> XML Editor.
Available online at: <http://www.oxygenxml.com/>
- [20] Schematron
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*.
ISO/IEC 19757-3:2006.
ISO Spec Available online at:<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
StyleSheets for compiling Available online at:<http://code.google.com/p/schematron/>
- [21] USAgency.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.
Available online Intelink-TS at:<http://go.ic.gov/MmBEpFU> [<http://go.ic.gov/>]
Available online Intelink-U at:<http://purl.org/IC/Standards/USAgency>
Available online at:<http://purl.org/IC/Standards/public>
- [22] 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>
- [23] 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>
- [24] 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/>
- [25] 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 the following DNI-sponsored web sites.

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

Intelshare: <http://purl.org/ic/standards/data-specs>

Direct all inquiries about this IC technical specification, IC technical specification collaboration and coordination forums, or IC element representatives involved in those forums, to the IC CIO.

E-mail: ic-standards-support@ugov.gov.

Appendix 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.^[12]