



Intelligence Community Technical Specification

XML Data Encoding Specification for Enterprise Audit Exchange

Version 4

14 December 2011

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	2
1.6 - Conventions	2
1.7 - Conformance	3
1.8 - Dependencies	3
Chapter 2 - Development Guidance	4
2.1 - Mapping of Abstract Data Elements to Physical XML Elements	4
2.2 - Additional Guidance	4
Chapter 3 - Data Validation Constraint Rules	5
3.1 - Basics	5
3.1.1 - Schematron	5
3.1.2 - "Living" Constraint Rules	5
3.1.3 - Classified or Controlled Constraint Rules	6
3.1.4 - Terminology	6
3.1.5 - Rule Identifiers	6
3.1.6 - Errors and Warnings	6
3.2 - Non-null Constraints	7
3.3 - Inherited Constraints	7
3.4 - Value Enumeration Constraints	7
3.5 - Additional Constraints	7
3.5.1 - DES Constraints	7
3.6 - Constraint Rules	7
3.7 - Obsolete Constraint Rules	8
Chapter 4 - Data Rendering Constraint Rules	9
4.1 - Basics	9
4.1.1 - "Living" Constraint Rules	9
4.1.2 - Classified or Controlled Constraint Rules	9
4.1.3 - Rule Identifiers	9
4.1.4 - Errors and Warnings	9
4.2 - Constraint Rules	10
4.3 - Obsolete Constraint Rules	10
Chapter 5 - Generated Guides	11
5.1 - Schema Guide	11
5.2 - Schematron Guide	12
Appendix A - Change History	13
A.1 - V4 Change Summary	13
A.2 - V3 Change Summary	14
A.3 - V2 Change Summary	15
Appendix B - Acronyms	17
Appendix C - Bibliography	19
Appendix D - Points of Contact	22
Appendix E - IC CIO Approval Memo	23

List of Tables

Table 1 - Dependencies	3
Table 2 - Obsolete Rules	8
Table 3 - Constraint Rules	10
Table 4 - Obsolete Rules	10
Table 5 - DES Version Identifier History	13
Table 6 - Change Summary	13
Table 7 - Change Summary	14
Table 8 - Change Summary	15
Table 9 - Acronyms	17

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Enterprise Audit Exchange* (AUDIT.XML) defines detailed specifications for using Extensible Markup Language (XML) to encode AUDIT.XML data in compliance with the *Intelligence Community Abstract Data Definition* (IC.ADD). This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing AUDIT.XML data concepts using XML.

This technical specification is linked to Intelligence Community Standard (ICS) 500-27, *Collection and Sharing of Audit Data for Intelligence Community (IC) Information Resources by IC Elements*. The technical specification detailed herein is the codification of the payload of an audit record exchange as defined in ICS 500-27. The architecture, interface specifications, design, and implementation of the enterprise audit collection and exchange services are outside the scope of this technical specification. This technical specification only applies to the payload of an audit record exchange.

1.2 - Scope

This specification is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This DES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the DES should be closely scrutinized and differences separately documented and assessed for applicability.

1.3 - Background

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

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

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

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

enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse.

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

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

1.4 - Enterprise Need

Needs and Requirements that are either classified or have handling controls can be found in separate annexes closely associated with the DES artifacts wherever they are located.

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 and applicability for this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, Intelligence Community Enterprise Standards Compliance, defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

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

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

1.6 - Conventions

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

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

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

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

1.7 - Conformance

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

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

Informative: serving to instruct or enlighten or inform.

The XML schemas, CVE values from the XML CVE files, and the Schematron code version of the constraint rules are normative for this DES. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative.

Additionally, the use of keywords defined in IETF RFC 2119 is considered normative within the scope of the sentence. All other parts of this document are informative.

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

1.8 - Dependencies

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

Table 1 - Dependencies

Name
ICS 500-27, <i>Collection and Sharing of Audit Data for Intelligence Community Information Resource by IC Elements</i>
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V7)
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V5)
ISO Schematron implementation by Rick Jelliffe (2010-04-14)
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.

Chapter 2 - Development Guidance

This chapter covers two primary topics:

- Mappings of the XML element and attributes defined within this DES to appropriate IC.ADD data elements
- Descriptions of how particular encoding situations should be handled using the features provided by this DES.

2.1 - Mapping of Abstract Data Elements to Physical XML Elements

The mapping of abstract data elements from the *Intelligence Community Abstract Data Definition* (IC.ADD) to the corresponding physical XML structures defined by this DES is shown in AUDIT FOUO Annex, which reflect the groupings in the IC.ADD. These mappings are provided for reference only. The complete set of DES artifacts, both normative and informative, should be consulted.

This mapping and additional mappings in other DESs provide a starting point for the development of automated transformations between formats defined by the DESs. However, it should be noted that when these transformations are used between formats with different levels of detail, there might be some data loss. Please refer to the annex for the mapping table.

2.2 - Additional Guidance

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

There is no additional guidance at this time.

Chapter 3 - Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for AUDIT.XML. They provide additional restrictions (i.e., constraints) on how the data should be structured and encoded, especially for criteria that exceed the constraints implemented in the XML Schema. These rules are written in plain English phrases; however, knowledge of the AUDIT.XML schemas is required to understand the rules. Complex constraint rules may be followed by text labeled *Human Readable*. This text is intended to inform the intent of the more formal language above it. Implementers are intended to implement the formal language, and should there be a perception of conflict, bring it to the attention of the appropriate configuration control body to be resolved. To date, AUDIT.XML does not contain any constraint rules but they can be added if deemed necessary in subsequent versions.

3.1 - Basics

The AUDIT.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.

This DES pertains to the technical implementation of a data model for sharing audit data from collaborative systems.

3.1.1 - Schematron

Schematron was selected as the language in which to encode these additional rules. The provided Schematron is used to define the constraint rules; it is NOT a required implementation. Implementers can use any tools at their disposal as long as the data complies with the rules expressed. To facilitate testing and understanding of the rules they are executable in either *oXygen®* or the XSLT2 implementation of ISO Schematron provided by Rick Jelliffe at <http://schematron.com/>. Constraint rules are dependent on XPath 2.0 and XSLT 2.0 features. According to Mr. Jelliffe, the editor of Schematron for ISO:

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

Included in the package are the ISO Schematron implementation XSLT files provided as a convenience along with a compiled version of the rules.

3.1.2 - “Living” Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by

authoritative security marking guidance, specifically Classification and Control Markings as defined by ICD 710 implemented in the Register and Implementation Manual, ISOO Directive 1, Executive Order (E.O.) 13526, and E.O. 12829, as amended. These rules will be expanded and modified as the model matures, the CAPCO Register is modified to reflect IC security marking implementation changes, 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.

3.1.3 - Classified or Controlled Constraint Rules

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

3.1.4 - Terminology

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

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

3.1.5 - Rule Identifiers

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

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

3.1.6 - Errors and Warnings

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

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

3.2 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content — which, allows for empty (or null) content. According to this Specification, all required elements (and certain conditional elements) must have content, other than white space. If an element, defined in this Specification, used in an XML instance is required (or conditional in certain cases), and that element may possibly contain only text content, then the element must have content in order to be Constraint Rules Valid.

3.3 - Inherited Constraints

In an instance of AUDIT.XML, the use of attributes and elements from supplementary data encoding specifications must be fully conformant with the constraint rules defined in those specifications. For a full list of supplementary specifications, see Section 1.8 - [Dependencies](#) .

3.4 - Value Enumeration Constraints

Several elements and attributes of the AUDIT.XML model use Controlled Vocabulary Enumerations (CVEs) to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE. Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

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

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

3.5 - Additional Constraints

This section provides additional constraints.

3.5.1 - DES Constraints

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

3.6 - Constraint Rules

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

3.7 - Obsolete Constraint Rules

The following table contains the information for the AUDIT.XML rules that have been removed or replaced by other rules.

Table 2 - Obsolete Rules

Rule Number	Removed/ Replaced	Version
There are no obsolete data rendering constraint rules at this time		

Chapter 4 - Data Rendering Constraint Rules

The constraint rules in this chapter define constraints on the rendering of AUDIT.XML documents. The intent is to inform the development of systems capable of rendering or displaying AUDIT.XML data for use by individuals not familiar with the details of the AUDIT.XML markup. While expressed in a similar manner to the data validation constraint rules above, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

4.1 - Basics

4.1.1 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by authoritative security marking guidance, specifically Classification and Control Markings as defined by ICD 710 implemented in the Register and Implementation Manual, ISOO Directive 1, Executive Order (E.O.) 13526, and E.O. 12829, as amended. These rules will be expanded and modified as the model matures, the CAPCO Register is modified to reflect IC security marking implementation changes, 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.

4.1.2 - Classified or Controlled Constraint Rules

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

4.1.3 - Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified 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. AUDIT.XML data rendering constrain rule IDs are prefixed with "AUDIT-RENDER-"

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

4.1.4 - Errors and Warnings

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

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

4.2 - Constraint Rules

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

Table 3 - Constraint Rules

Rule Number	Severity	Description	Human Readable Description
There are no data rendering constraint rules at this time			

4.3 - Obsolete Constraint Rules

The following table contains the information for the AUDIT.XML data rendering rules that have been removed or replaced by other rules.

Table 4 - Obsolete Rules

Rule Number	Removed/ Replaced	Version
There are no obsolete data rendering constraint rules at this time		

Chapter 5 - Generated Guides

5.1 - Schema Guide

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

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

The guide provides an interactive index to:

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

Where applicable, the guide provides:

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

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

5.2 - Schematron Guide

The detailed description and reference documentation for the AUDIT.XML Schematron rules can be found in a separate document named *AUDIT_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 Change History

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

Table 5 - DES Version Identifier History

Version	Date	Purpose
1.0	5 August 2010	Initial Release
2	11 April 2011	Routine revision to technical specification. For details of changes, see Section A.3 - V2 Change Summary
3	9 August 2011	Routine revision to technical specification. For details of changes, see Section A.2 - V3 Change Summary
4	14 December 2011	Routine revision to technical specification. For details of changes, see Section A.1 - V4 Change Summary

A.1 - V4 Change Summary

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

Table 6 - Change Summary

Change	Artifacts changed	Compatibility Notes
@ntk:DESVersion attribute was added to the AuditRootNode-AttributeGroup	Schema	Data generation and ingestion systems need to be updated to include the required attributes.
Added new elements, NTPServer and NTPLastUpdate . These are new optional elements if the IC Element has access to an NTP (Network Time Protocol) service.	Schema	Data generation systems should be updated to use the attribute if they need the feature. Ingestion systems need to use the new specification, including schema.
Simplified and cleaned identifier elements and complex types. There are only two identifier elements: GenericIdentifierType and IdentityIdentifierType , the latter specifically for Person and Non-Person Entities only. The option to add the scope for each identifier has been added (e.g., global, local to IC Element, local to only a small subnet).	Schema	Data generation and ingestion systems need to be updated to include the required attributes.

Change	Artifacts changed	Compatibility Notes
Modified date/time elements (i.e., DateTime , NTPLastUpdate , CreateDate , PublishDate) to use <code>xsd:dateTime</code>	Schema	Data generation and ingestion systems need to be updated to include the required attributes.
Combined AuditRecordType , AbstractEventType , and ActionEventType into AuditRecordType	Schema	Data generation and ingestion systems need to be updated to include the required attributes.
Combined ResourceType and AbstractResourceType into ResourceType	Schema	Data generation and ingestion systems need to be updated to include the required attributes.
Removed IC-Common Reference	Schema	Data generation and ingestion systems need to be updated to include the required attributes.

A.2 - V3 Change Summary

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

Table 7 - Change Summary

Change	Artifacts changed	Compatibility Notes
Updated ISM to V7 and included NTK V5.	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in these sub-specifications.
Changed references to ISM attribute groups from optional to required.	Schema	Data generation and ingestion systems need to be updated to include the required attributes. Note: Data valid under previous releases may not be valid under this release.
Included ntk:Access as optional element in AuditRecordListType and AuditRecordType	Schema	Data generation systems should be updated to use the element if they need the feature.
Replaced audit:NoticeList , audit:Notice , and audit:NoticeText with their ISM equivalents.	Schema	Data generation and ingestion systems need to be updated to use the new elements. Note: Data valid under previous releases may not be valid under this release.

Change	Artifacts changed	Compatibility Notes
In CVEEnumAUDITActionType.xml, removed [ROLE_ESCALATE] and added [RESTART] to differentiate a reboot from [SHUTDOWN].	CVE	Data generation and ingestion systems need to be updated to use the new elements. Note: Data valid under previous releases may not be valid under this release.

A.3 - V2 Change Summary

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

Table 8 - Change Summary

Change	Artifacts changed	Compatibility Notes
Added [LOOK] value to enumeration for ActionType	Schema Schema Guide	Data generation systems should be updated to use the attribute if they need the feature. Ingestion systems need to use the new specification, including schema.
Added ability for instance documents to specify DES versions used.	Schema Schema Guide	Data generation systems need to be updated to include DES version(s) in output. Ingestion systems need to be updated to properly handle the new data.
Change authentication enumeration value from [AUTHENTICATION] to [AUTHENTICATE]	Schema Schema Guide	Data generation systems need to be updated to include this enumeration in output. Ingestion systems need to be updated to properly handle the new data.
Schema now references ISM.XML.V6	Schema Schema Guide	Data generation systems should be updated to use the attribute if they need the feature. Ingestion systems need to use the new specification, including schema.
Added 5 subclasses of audit record	Schema Schema Guide	Data generation systems need to be updated to include these classes in output. Ingestion systems need to be updated to properly handle the new data.

Change	Artifacts changed	Compatibility Notes
Added types in 500-27 to ActionType . Deleted all the _MULTIPLE actions.	Schema Schema Guide	Data generation systems need to be updated to include this enumeration in output. Ingestion systems need to be updated to properly handle the deprecated data.
Renamed ActionType to AuditActionType to conform to the model	Schema Schema Guide	Data generation systems need to be updated to include the new name in output. Ingestion systems need to be updated to properly handle the new data.
Deleted IdentityCategory element from IdentityReferenceType	Schema Schema Guide	Data generation systems need to be updated to remove the name in output. Ingestion systems need to be updated to properly handle the deprecated data.
Renamed element IdentityReferenceType to TypeOfIdentityReference on IdentityReferenceType	Schema Schema Guide	Data generation systems need to be updated to include the new name in output. Ingestion systems need to be updated to properly handle the new data.
Renamed IdentityCategoryType to be TypeOfIdentityReference	Schema Schema Guide	Data generation systems need to be updated to include the new name in output. Ingestion systems need to be updated to properly handle the new data.
Changed values of TypeOfIdentityReference to be consistent with model	Schema Schema Guide	Data generation systems need to be updated to include the new values in output. Ingestion systems need to be updated to properly handle the new data.
Renamed GenericAuditRecord to AuditRecord . Added auditRecordType and removed specific typeAuditRecord elements	Schema Schema Guide	Data generation systems need to be updated to include the new values in output. Ingestion systems need to be updated to properly handle the new data.

Appendix B Acronyms

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

Table 9 - Acronyms

Name	Definition
CAPCO	Controlled Access Program Coordination Office
CVE	Controlled Vocabulary Enumeration
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DOI	Digital Object Identifier
DNI	Director National Intelligence
E.O.	Executive Order
GNS	Geographic Names Server
HTML	HyperText Markup Language
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICS	Intelligence Community Standard
ISBN	International Standard Book Number
ISM	Information Security Marking Metadata
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
KA	Knowledge Assertion
KOS	Knowledge Organization System
MIME	Internet Media Types
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NSI	National Security Intelligence
ODNI	Office of the Director of National Intelligence
SSC	Special Security Center
TGN	Thesaurus of Geographic Names
URI	Uniform Resource Identifier

Name	Definition
URL	Uniform Resource Locator
W3CDTF	World Wide Web Consortium Date Time Format
XML	Extensible Markup Language

Appendix C Bibliography

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

(CAPCO Implementation Guide)

Community Classification and Control Markings Implementation Manual. Unclassified FOUO version. Volume 4, Edition 2 (Version 4.2). 31 May 2011. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO). [https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO Implementation%20Manual%20v4%202 MAY 31 2011 FOUO datefixed.pdf](https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO%20Implementation%20Manual%20v4%202%20MAY%2031%202011%20FOUO%20datefixed.pdf).

(CAPCO Register)

Authorized Classification and Control Markings Register. Unclassified FOUO version. Volume 4, Edition 2 (Version 4.2). 31 May 2011. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO). [https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO Register FOUO v4.2 MAY31 2011.pdf](https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO%20Register%20FOUO%20v4.2%20MAY31%202011.pdf).

(DC MES)

Dublin Core Metadata Element Set. Version 1.1. 02 June 2003. Dublin Core Metadata Initiative. <http://dublincore.org/documents/dces/>.

(E.O. 12958, as amended)

Executive Order 12958 – Classified National Security Information, as Amended. Federal Register, Vol. 68, No. 60. 25 March 2003. The White House. <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>.

(E.O. 12829, as amended)

Executive Order 12829 – National Industrial Security Program, as Amended. Federal Register, Vol. 58, No. 240. 16 December 1993. The White House. <http://www.archives.gov/isoo/policy-documents/eo-12829.html>.

(E.O. 13526)

Executive Order 13526 – Classified National Security Information. 29 December 2009. The White House. <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>.

(ICD 206)

Sourcing Requirements for Disseminated Intelligence Products. Intelligence Community Directive Number 206. 17 October 2007. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_206.pdf.

(ICD 500)

Intelligence Community Directive Number 500. Director of National Intelligence Chief Information Officer. 7 August 2008. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_500.pdf.

(ICD 501)

Intelligence Community Directive Number 501. Director of National Intelligence Chief Information Officer. 21 January 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_501.pdf.

(ICD 710)

Classification and Control Markings System. Intelligence Community Directive Number 710. 11 September 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_710.pdf.

(ICD 500-27)

Intelligence Community Standard for Collection and Sharing of Audit Data for IC Information Resources by IC Elements Number 500-27. DRAFT. Office of the Director of National Intelligence.

(ISO 639-2)

Codes for the representation of names of languages – Part 2: Alpha-3 code ISO 639-2:1998. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4767.

(ISO 3166-1)

Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. ISO 3166-1:2006. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719.

(ISO 8601)

Data elements and interchange formats – Information interchange – Representation of dates and times. ISO 8601:2004. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40874.

(ISO 15836)

Information and documentation – The Dublin Core metadata element set. ISO 15836:2009. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142.

(ISO 19757-3:2006)

Information technology - Document Schema Definition Language (DSDL) - Part 3: Rule-based validation - Schematron. 19757-3:2006 International Organization for Standardization (ISO). <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

(ISOO Directive 1)

Classified National Security Information (Directive No. 1); Final Rule. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 68, No. 183. 22 September 2003. Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). <http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.pdf>.

(RFC 3066)

Tags for the Identification of Languages. January 2001. H. Alvestrand. Cisco Systems. <http://www.rfc-editor.org/rfc/rfc3066.txt>.

Marking Classified National Security Information. Information Security Oversight Office. December 2010. <http://www.archives.gov/isoo/training/marketing-booklet.pdf>

<http://www.schematron.com/>.

Appendix D Points of Contact

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

Appendix E 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.