Intelligence Community Technical Specification

CVE Encoding Specification for Geopolitical Entities, Names, and Codes

Version 2017-SEP

September 29, 2017

Table of Contents

List of Figures

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This CVE Encoding Specification for Geopolitical Entities, Names, and Codes (IC-GENC.CES) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode Geopolitical Entities, Names, and Codes (IC-GENC) data. This CVE Encoding Specification (CES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing IC-GENC data concepts using XML.

In September 2, 2008, the U.S. Federal Government moved away from NIST Federal Information Processing Standard (FIPS) 10-4 standard [1] of identifying different country locations using a two-character code base. The FIPS 10-4 standard was identified to be replaced by the open standard International Standards Organization (ISO) 3166.[21] ISO 3166-1 country code elements are based on United Nations recognition and the names of countries provided by member states. U.S. organizations are transitioning to a profile of ISO 3166 called GENC, based on three-character codes to ease the transition. The profile is considered the authoritative set of country codes and names for use by the Federal Government for information exchange. GENC will use ISO 3166 code elements whenever possible, but will be modified where necessary to comply with U.S. law and U.S. Government recognition policy.

This specification provides a subset of the permissible GENC codespaces and code values that are used in the Intelligence Community (IC). Specifically, this specification only utilizes the short Uniform Resource Name(URN) based codespaces with the three-character codes from the GENC Registry which aligns the specifications with the names defined by the Board of Geographic Names mandated by Federal Law.

Note

This specification aligns with the codes and names of countries within the GENC Registry, not to be confused with the GENC Standard. Country codes have been part of the GENC Registry since GENC Edition 1 and thus allowing the use of the newer codespaces is actually still holding to conformance with the GENC Ed 1 standard regardless of Edition or version that might be represented in the codespace.

1.2 - Scope

This specification is applicable to the IC and information produced by, stored, or shared within the IC. This CES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the CES 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)

[1] NIST announced the Secretary of Commerce's approval to withdraw FIPS 10-4 in the Federal Register Vol. 73, No. 170, dated Tuesday, September 2, 2008.[4]

500, *Director of National Intelligence Chief Information Officer* [11] 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* [18] 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 a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* [2]. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID[7] defines a plain-text format for IC Identifiers as well as an associated XML structure.

1.4 - Enterprise Need

Many IC encoding specifications use Controlled Vocabulary Enumerations (CVEs) to define allowable values for various elements and attributes. Over time, several encoding specifications became dependent on the same list of values, and dual (or more) maintenance was required to keep the lists aligned. Additionally, any changes to a specification's CVEs caused an entire new version of that specification to be created. In order to remove the need for dual maintenance and to remove the need to revision a specification when a CVE was updated, a new type of encoding specification, the CVE Encoding Specification, was created to decouple the vocabulary from the specifications. Each CES contains one or more CVEs and optionally a master schema defining elements and attributes limited to the allowable values and/or any Schematron rules that enforce the vocabulary in specifications that define their own elements or attributes.

This CES defines CVEs that contain the GENC country codes allowing this specification to revise in tandem with the GENC country code registry. The goal is to allow this specification to revise as needed while allowing other specifications to use various versions of this specification for their country code CVEs, thus preventing an excessive number of revisions of the Data Encoding Specifications.

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[6]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[11]
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[12]
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[18]
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[9]
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[10]
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide[16]
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System[13]
  - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control[14]
  - Intelligence Community Policy Guidance (ICPG) 710.2, Application of Dissemination Controls: Foreign Disclosure and Release Markings[15]

1.5 - Audience and Applicability

CESs 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 governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance,* [17] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,[3] requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

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

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels.” [19] When these words appear in regular case, 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 Namepaces

Prefix	URI
ism	urn:us:gov:ic:ism
xsd	http://www.w3.org/2001/XMLSchema

1.7 - Dependencies

1.7.1 - Types of Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. Dependencies play an important role in functionality or provide informational relationships between the various artifacts. The following terms are defined to help assist with understanding how the various artifacts work together:

Dependency Directly or transitively influenced by.

	Examples: 1. A is influenced by B therefore B is a dependency of A. 2. A is influenced by B and B is influenced by C; therefore C is a dependency of A.
Direct Dependency	Explicit influence. Example: A influences B.
Inverse Dependency	Directly or transitively influences. Example: B influences A.

1.7.2 - Specification 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.

Table 2 - Dependencies

Name	Dependency Description
Schematron[24]	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. 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. Note: The Schematron rules in this specification use XSLT 2.0[30] query binding.

Name	Dependency Description
XSLT 2.0[30] implementation of Schematron[24] by Rick Jelliffe (2010-04-14) 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/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the *behavior* of the implementation created by Mr. Jelliffe is normative. 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.
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this CES.	Specification uses CVEs to encode controlled vocabularies. The use of the IC-GENC CVE is normative.
The GENC Registry out of the Country Code Working Group[5]	Depends on Geopolitical Entities, Names,and Codes(GENC) which is the US Government profile of ISO 3166-1 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

1.7.3 - Inverse Dependencies

Generally, it is only necessary to think of the *direct dependencies* (see Direct Dependency) in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies* (see Inverse Dependency), for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies.

Since this specification is one such specification that is used by other specifications released by the IC CIO, the Figure 1 has been included to assist readers in understanding all of the dependency relationships and how changes in a specification may impact others. This diagram is representative of dependencies at the time of the release of this specification, but are subject to change over time.

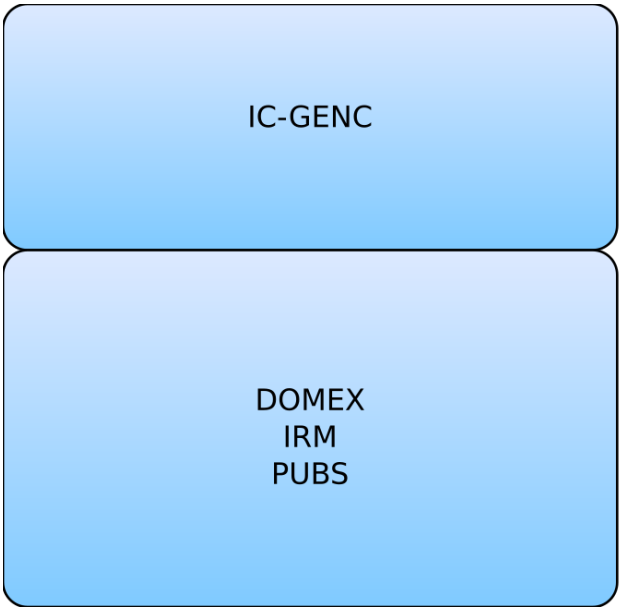

Figure 1 : Inverse Dependency Specifications

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron[24] 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 PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[19] 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.[28] 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 specify which version of a dependent specification to import enables the configuration change control of parent specifications (such as PUBS and TDF) to be "decoupled" from the configuration change control of dependent specifications (such as ISM CVE updates). This "decoupling" method has not been in place for all versions of these parent specifications; therefore, please verify with the dependency table to ensure use of allowed dependency versions.

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

1.9 - Version Policies

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from “The Disposition of Names in an XML Namespace.”[25] This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 “Versioning and XML namespace policy” of “Architecture of the World Wide Web, Volume One.”[26]

There is a version attribute (e.g. **@DESVersion**, **@CESVersion**, **@TESVersion**, **@version**) for each namespace defined in an IC CIO specification. Version attributes are used to capture the specification version number the specification author intends an instance to conform to. Namespaces do not change, so the version attribute is required to fully understand an instance document.

As changes to the specification are released, the version number captured in the “version” attribute increments. See Section 1.9.2 - Version Numbering for information on the numbering scheme.

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

1.9.2 - Version Numbering

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-MMM). This provides a temporal representation of when the specification was released. Revisions to a version of the specification also use a year-month structure (e.g., YYYY-MMM). When the version number is used in the version attribute, the expression follows the Augmented Backus–Naur Form[1] below:

Version Format when used in the version attribute:

```
[1]          Version : := Year Month["." Revision ] ["-" CustomizationSuffix ]
[2]    VersionYear : := 4( DIGIT )
[3]  VersionMonth : := 2( DIGIT )
[4] Customization : := 1*23(ALPHA / DIGIT / "_" )
                Suffix
[5]  RevisionYear : := 4( DIGIT )
[6]  RevisionMont : := 2( DIGIT )
                   h
[7]        Revision : := Year Month
```

Version in XML Lexicon

The following vocabulary helps explain the meaning of terms used in the version documentation, and it may further constrain the set of allowable values:

Version	The version number as it might be expressed in a DESVersion, CESVersion or other XML attribute for indicating the version/revision being referenced.
VersionYear	The four digit year from the version of the specification being referenced.
VersionMonth	The 2 digit month from the version of the specification being referenced.
CustomizationSuffix	An optional suffix used when customizing a version of a specification. This would be used to indicate that you have extended the specification in some fashion for a particular use case.
RevisionYear	The four digit year from the revision of the specification being referenced.
RevisionMonth	The 2 digit month from the revision of the specification being referenced.
Revision	The Year and Month from the revision of the specification being referenced. Revisions are modifications to Versions.

Chapter 2 - Development Guidance

2.1 - 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.

2.2 - 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.

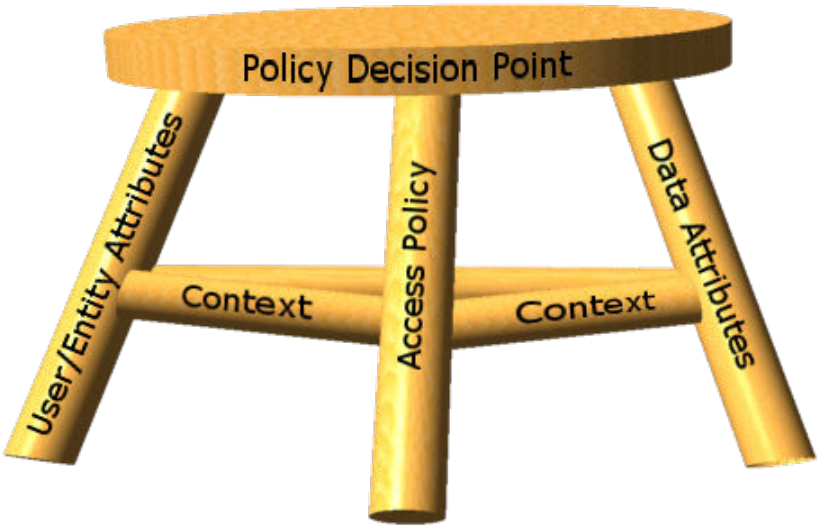

Figure 2 : Three-legged Stool of Access Decisions

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).

The data attributes component of the policy framework provides a common understanding of IC metadata to enable precise access control decisions. Without this common understanding the IC Enterprise is missing a crucial data attribute component to make accurate, reliable, and automated access control decisions. The IC-GENC specification provides a common encoding (e.g. common understanding) and foundation for data attributes specifications that use country codes.

2.3 - Additional Guidance

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

2.3.1 - The CVEs

This specification is comprised of multiple CVE files. Each CVE is the keeper of all code values belonging to a particular GENC codespace. As GENC evolves over time and the number of codespaces grow, so too will the number of CVEs in this specification. The split on the codespace is to limit the size of each individual CVE.

Since GENC[5] Edition 3, the need to maintain all of the codespaces is no longer necessary so a standalone country code CVE has been added which should be used in place of the codespace specific CVEs. However, since not all specifications dependent on IC-GENC.CES are being updated/retired, this specification will continue to maintain the codespace based CVEs until all specifications that depend on it are retired. In addition, edition 3 also saw the addition of subdivision codes which are now being included in this specification in a single CVE file.

2.3.2 - The Schematron Abstract Pattern

Part of this specification is a Schematron abstract pattern that can be used in other rule sets such as those of other encoding specifications. The abstract pattern has parameters for the context, codespace, code value, and error message; context, searchCodespace, searchTerm, and errMsg respectively. In the given context; using the codespace parameter the pattern determines which CVEfile to choose. Then performs a search of the chosen CVE for the designated code, or searchTerm. If the code value is present in the CVE then the pattern will pass as valid. However, if the code value is not present in the CVE then the pattern will fail producing a validation error and returning the error message passed in via the errMsg parameter.

Warning

The use of abstract patterns across specifications is being phased out. Abstract patterns are retained in IC-GENC.CES until older dependent specifications that use abstract patterns, such as DOMEX, are retired. Developers SHOULD NOT use these patterns in new work.

2.4 - CSV Notes

There are Comma Separated Value files provided for all of the CVEs. They are in the CVE folder with the XML and JSON versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence.

Important

The CSV files on many systems will open “automatically” in Microsoft Excel; the default opening however, will not correctly read UTF-8 special characters. These are found in some country names such as “Republic of Côte d’Ivoire”. If you need to use a CVE that contains such special characters, or you think may contain such characters in Excel, you should:

- Open Excel to a blank sheet

- Under the Data menu choose to get external data from a text file
- Choose UTF-8 as the file origin
- Choose delimited as the format
- Choose next
- Change from tab to Comma as the delimiter
- Finish import to get the data in with the UTF-8 Characters properly encoded in Excel.

2.5 - JSON Notes

There are JSON format files provided for all of the CVEs. They are in the CVE folder with the XML and CSV versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence. The JSON files are formatted using JSON-LD based on a proposed method for JSON in NIEM.

2.6 - RELAX NG Notes

There are RELAX NG format files provided for all of the CVEs. They are in the CVE folder with the XML, JSON and CSV versions of the information.They are provided as a convenience to developers who wish to import IC Specification CVEs into other XML specifications that utilize RELAX NG. They will not affect specifications that do not utilize RELAX NG and there are no new requirements because of their existence. RELAX NG is an alternative schema language for XML and it provides both an XML syntax and a compact non-XML syntax. The XML syntax format fragments are provided with the .rng file name extension and the Compact syntax fragments are provided with the .rnc file name extensions.

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 starter set and do not attempt to address the full scope tradecraft and business rules addressed by multiple policy drivers including Sourcing Requirements for Disseminated Intelligence Products as defined by ICD 206.[8] These rules will be expanded and modified as the model matures, and as applicable documentation and tradecraft policies change.

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

3.3 - 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 identifier, indicated in brackets preceding the constraint rule description. IC-GENC.CES data validation constraint rule identifiers are prefixed with "IC-GENC-ID-" and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in Table 3. As the constraint rules are managed over time, IDs from deleted rules will not be reused.

Table 3 - Numerical Rule Identifier Ranges

Rule Identifier Range		Description
Start	End	
00001	09999	Reserved for Unclassified constraint rules
10001	19999	Reserved for Unclassified but For Official Use Only (FOUO) constraint rules
20001	20999	Reserved for constraint rules classified at the “Secret//REL USA, FVEY” level
21001	21999	Reserved for constraint rules classified at the “Secret//NF” level
22001	29999	Reserved for constraint rules classified at the “Secret//TBD” level
30001 and above		Reserved for constraint rules classified with other classifications

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

The IC-GENC.CES specification does not contain a master schema, but does contain several schemas generated from the CVEs. These schemas define the data elements, attributes, cardinalities and parent-child relationships for which XML instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified in applicable IC policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints.

3.7.2 - Schematron

Schematron[24] 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[24] rules for this specification may be executed in *Oxygen®* [23] or with an XSLT 2.0-compliant processor using the XSLT 2.0[30] 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[29] and XSLT 2.0[30] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:[22]

> 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[30] implementation of Schematron[24] 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 - Vocabulary Enumeration Constraints

The purpose of the IC-GENC.CES specification is to define the CVE list for allowable Country Codes.

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

[1] “White space” is defined in XML 1.0[27] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

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

3.7.5 - Additional Constraints

3.7.5.1 - CES Constraints

The CES version for this specification is defined in the ISM.XML[20] specification. The **CESVersion** 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.

3.7.6 - Constraint Rules

There are no Schematron rules defined for IC-GENC.CES at this time.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

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

3.8.2 - Rendering Constraint Rules

The following table contains the information for the IC-GENC.CES data rendering constraint rules.

Table 4 - Constraint Rules

Rule Number	Severity	Description	Human Readable Description
There are no Data Rendering Constraint rules at this time.			

Chapter 4 - Conformance Validation

An instance 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 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the IC-GENC.CES 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 IC-GENC.CES schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen®*,[23] produced by SyncRO Soft.

The guide provides an interactive index to:

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

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

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

5.2 - Schematron Guide

The detailed description and reference documentation for the IC-GENC.CES Schematron rules can be found in a separate document named *IC-GENC_Rules.pdf,* which is located inside the Schematron/IC-GENC directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Appendix A Feature Summary

The following table summarizes major features by version for IC-GENC and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. For those changes driven by the IC Markings System Register and Manual, the date is often one year after the date of publication. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

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. IC-GENC Feature Comparison

Table 6 - IC-GENC Feature comparison

IC-GENC Feature Comparison						
Required date	**Feature**	**V1**	**V2015-MAY**	**V2016-SEP**	**V2017-JUL**	**V2017-SEP**
	Defines the allowable values for Country Codes	F	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2012-09-01	F	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2013-04-03	F	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2013-06-30	F	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2013-09-30	F	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2013-11-15	N	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2013-12-30	N	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2014-03-31	N	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2014-06-30	N	F	F	F	F
	Support codes and names for countries consistent with the update of the GENC[5] registry promulgated on 2014-12-31	N	F	F	F	F
	Support codes and names for countries consistent with the update through GENC[5] Edition 3 Update 4	N	N	F	F	F

IC-GENC Feature Comparison						
Required date	**Feature**	**V1**	**V2015-MAY**	**V2016-SEP**	**V2017-JUL**	**V2017-SEP**
	Support codes and names for subdivisions consistent with the update through GENC[5] Edition 3 Update 4	N	N	F	F	F
	Support codes and names for countries and subdivisions consistent with the update through GENC[5] Edition 3 Updates 5 and 6	N	N	N	F	F
	Support codes and names for countries and subdivisions consistent with the update through GENC[5] Edition 3 Update 7	N	N	N	N	F

Appendix B Change History

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

Table 7 - CES Version Identifier History

Version	Date	Purpose
1	14 March 2014	Initial Release
2015-MAY	15 May 2015	Routine revision to technical specification. For details of changes, see Section B.4 - V2015-MAY Change Summary
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Section B.3 - V2016-SEP Change Summary
2017-JUL	21 July 2017	Routine revision to technical specification. For details of changes, see Section B.2 - V2017-JUL Change Summary
2017-SEP	29 September 2017	Routine revision to technical specification. For details of changes, see Section B.1 - V2017-SEP Change Summary

B.1 - V2017-SEP Change Summary

Significant drivers for Version 2017-SEP include:

- Updating to be inline with the content of the GENC[5] Edition 3 Update 7.

The following table summarizes the changes made to V2017-JUL in developing V2017-SEP.

Table 8 - V2017-SEP Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Create RelaxNG CVE Fragments for IC-GENC. (CR-2017-172)	CVEs	No impact to systems.
2	Update IC-GENC with Update 7 of the GENC Ed3.0(CR-2017-193)	CVEs	Data generation and ingestion systems need to be updated to handle the added GENC updates.

B.2 - V2017-JUL Change Summary

Significant drivers for Version 2017-JUL include:

- Updating to be inline with the content of the GENC[5] Edition 3 Updates 5 and 6.

The following table summarizes the changes made to V2016-SEP in developing V2017-JUL.

Table 9 - Data Encoding Specification V2017-JUL Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Create JSON version of CVEs in IC-GENC (CR-2017-053)	CVEs	No impact to systems.
2	Create CSV version of CVEs in IC-GENC (CR-2017-031)	CVEs	No impact to systems.
3	Added CESVersion enforcement rule as warning (CR-2017-080)	Schema Schematron IC-GENC-ID-00001 added IC-GENC_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.
4	Added update to codes and names promulgated through GENC Ed3 Updates 5 and 6. (CR-2017-021)	CVEs CVEnumGeGENC33-5 added CVEnumGeGENC33-6 added CVEnumCountryCode modified CVEnum-SubDivisionCode modified	Data generation and ingestion systems need to be updated to handle the added GENC updates.
5	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-110)	Documentation	No impact to systems.
6	Added @id and @role to all sch:rule elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-216)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
7	Modified cardinality rendering. (CR-2017-024)	CVEs	No impact to existing systems, documentation rendering change only.
8	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-237)	Documentation	No impact to systems.

B.3 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Updating to be inline with the content of the GENC[5] Edition 3 Update 4 register.

The following table summarizes the changes made to V2015-MAY in developing V2016-SEP.

Table 10 - Data Encoding Specification V2016-SEP Change Summary

Change	Artifacts Changed	Compatibility Notes
Added update to codes and names promulgated through GENC Ed3 Update 4. (CR-2015-089,CR-2016-041)	CVEs	Data generation and ingestion systems need to be updated to handle the added GENC updates.
Added CountryCode CVE that will serve as the source of currently correct values and names for country codes. (CR-2015-089)	CVEnumGENCCountyCode.xml added	Data generation and ingestion systems need to be updated to handle the new CVE.
Added SubDivisionCode CVE that will serve as the source of currently correct values and names for sub divisions of geopolitical entities. (CR-2015-089, CR-2015-090)	CVEnum-GENCSubDivisionCode.xml added	Data generation and ingestion systems need to be updated to handle the new CVE.
Removing GENC Baseline Code-Space Code-Value Mappings appendix as this is covered by the IC-GENCCVEnums.pdf document.	Documentation	This change has no effect on data generation and ingestion systems. This is merely a removal of duplicated documentation.
Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.4 - V2015-MAY Change Summary

Significant drivers for Version 2015-MAY include:

- Updating to be inline with the current content of the GENC register.

The following table summarizes the changes made to V1 in developing V2015-MAY.

Table 11 - Data Encoding Specification V2015-MAY Change Summary

Change	Artifacts Changed	Compatibility Notes
Added update to codes and names promulgated with GENC Ed1 Update 3 through GENC Ed2 Update 3.	CVEs	Data generation and ingestion systems need to be updated to handle the added GENC updates.

Appendix C List of Abbreviations

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

ADD	Abstract Data Definition
ARH	Access Rights and Handling
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DNI	Director of National Intelligence
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
GENC	Geopolitical Entities, Names, and Codes
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
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology

JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
NIEM	National Information Exchange Model
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PDP	Policy Decision Point
PUBS	Intelligence Publications
RELAX NG	REgular LAnguage for XML Next Generation
RFC	Request for Comments
TDF	Trusted Data Format
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] ABNF
Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.
Available online at: http://tools.ietf.org/html/std68
Also known as: http://www.ietf.org/rfc/rfc5234.txt

[2] ADD
Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*.
Available online Intelink-TS at: http://go.ic.gov/soSC6M8
Available online Intelink-U at: https://w3id.org/ic/standards/ADD
Available online at: https://w3id.org/ic/standards/public

[3] DoD Instruction 8310.01
DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.
Available online at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/831001p.pdf

[4] FIPS 10-4 Transition to GENC
National Institute of Standards and Technology. *Transition of the Geopolitical, Entities, Names and Codes (GENC) Standard from a U.S. Government Standard to a U.S. National Standard (U.S. Profile of ISO 3166 -- CODES FOR THE REPRESENTATION OF NAMES OF COUNTRIES AND THEIR SUBDIVISIONS)*. . December 24, 2013.
Available online at: http://www.niso.org/apps/group_public/download.php/12049/NISO_Proposal_US_Profile_ISO_3166_Voting_Members.pdf

[5] GENC
Country Codes Working Group. *Geopolitical Entities, Names, and Codes*. 3.0.
Available online Intelink-TS at: http://go.ic.gov/QWkfrXy
Available online at: https://nsgreg.nga.mil/genc/discovery

[6] 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

[7] IC-ID.XML
Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.
Available online Intelink-TS at: http://go.ic.gov/mQ4IUDk
Available online Intelink-U at: https://w3id.org/ic/standards/IC-ID
Available online at: https://w3id.org/ic/standards/public

[8] ICD 206
Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Analytic Products*. Intelligence Community Directive 206. 22 January 2015.

Available online at: http://www.dni.gov/files/documents/ICD/ICD%20206.pdf

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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/0d147Ee
Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf

[15] 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

[16] 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

[17] 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: https://w3id.org/ic/standards/policy/ICS500-20

[18] 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: https://w3id.org/ic/standards/policy/ICS500-21

[19] 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

[20] 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: https://w3id.org/ic/standards/ISM
Available online at: https://w3id.org/ic/standards/public

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

[22] Jelliffe
Richard Alan Jelliffe. *FAQ*. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?.
Available online at: http://www.schematron.com

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

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

[25] TAG-9-Jan-2006
W3C Technical Architecture Group (TAG). *The Disposition of Names in an XML Namespace*. 9 January 2006.

Available online at: http://www.w3.org/2001/tag/doc/namespaceState.html

[26] WEBARCH-15-Dec-2004
W3C. *Architecture of the World Wide Web, Volume One*. 15 December 2004.
Available online at: http://www.w3.org/TR/webarch

[27] 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

[28] 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

[29] 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/

[30] 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: https://w3id.org/ic/standards/public

Intelshare: https://w3id.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@iarpa.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.[17]