Intelligence Community Technical Specification

XML CVE Encoding Specification for Geopolitical Entities, Names, and Codes

Version 1

09 May 2014

Table of Contents

Chapter 1 - Introduction 1
1.1 - Purpose 1
1.2 - Scope 1
1.3 - Background 1
1.4 - Enterprise Need 2
1.5 - Audience and Applicability 3
1.6 - Conventions 4
1.6.1 - Language 4
1.6.2 - Typography 4
1.6.3 - XML Namespaces 4
1.7 - Dependencies 4
1.7.1 - Standalone and Convenience Packages 6
1.8 - Conformance 6
1.9 - Version Policies 7
1.9.1 - XML Namespace Policy 7
1.9.2 - Version Numbering 7
Chapter 2 - Development Guidance 8
2.1 - Relationship to Abstract Data Definition and other encodings 8
2.2 - Understanding Access Control 8
2.3 - Additional Guidance 9
2.3.1 - The CVEs 10
2.3.2 - The Schematron Abstract Pattern 10
Chapter 3 - Definitions, Interfaces, and Constraints 11
3.1 - Constraint Rule Types 11
3.2 - “Living” Constraint Rules 11
3.3 - Classified or Controlled Constraint Rules 11
3.4 - Terminology 11
3.5 - Errors and Warnings 12
3.6 - Rule Identifiers 12
3.7 - Data Validation Constraint Rules 12
3.7.1 - Purpose 12
3.7.2 - Schematron 12
3.7.3 - Non-null Constraints 13
3.7.4 - Vocabulary Enumeration Constraints 13
3.7.5 - Additional Constraints 14
3.7.5.1 - CES Constraints 14
3.7.6 - Constraint Rules 14
3.8 - Data Rendering Constraint Rules 14
3.8.1 - Purpose 14
3.8.2 - Rendering Constraint Rules 14
Chapter 4 - Conformance Validation 15
4.1 - Schema Validation 15
4.2 - Business Rule Validation 15
Chapter 5 - Generated Guides 16
5.1 - Schema Guide 16
5.2 - Schematron Guide 17

Appendix A - Feature Summary 18
A.1 - GENC Feature Comparison 18
Appendix B - Change History 19
Appendix C - GENC Baseline Code-Space Code-Value Mappings 20
C.1 - GENC Baseline 1-1 20
C.2 - GENC Baseline 1-2 28
C.3 - GENC Baseline ed1 37
Appendix D - Glossary 46
Appendix E - Bibliography 48
Appendix F - Points of Contact 51
Appendix G - IC CIO Approval Memo 52

List of Tables

Table 1 - XML Namepaces 4
Table 2 - Dependencies 5
Table 3 - Constraint Rules 14
Table 4 - Feature Summary Legend 18
Table 5 - GENC Feature comparison 18
Table 6 - CES Version Identifier History 19
Table 7 - Codespace: ge:GENC:3:1-1 20
Table 8 - Codespace: ge:ISO1:3:VI-14 27
Table 9 - Codespace: ge:GENC:3:1-2 28
Table 10 - Codespace: ge:ISO1:3:VI-15 36
Table 11 - Codespace: ge:GENC:3:ed1 37
Table 12 - Codespace: ge:ISO1:3:VI-13 41

Chapter 1 - Introduction

1.1 - Purpose

This *XML CVE Encoding Specification for Geopolitical Entities, Names, and Codes* (GENC.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode Geopolitical Entities, Names, and Codes (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 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.[16] 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 Number (URN) based codespaces with the three-character codes.

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 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* [7] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture.
- Lead the IC’s identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.

[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.[1]

- Certify that IC elements adhere to the architecture and standards.

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

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* [13] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby achieving the IC 's data discovery, data sharing, and interoperability goals.

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

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

1.4 - Enterprise Need

Many IC encoding specifications use Controlled Vocabulary Enumerations (CVE)s 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 a CVE that contains the GENC country codes allowing this specification to revise in tandem with the GENC standard. 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 CVE s, 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[3]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[7]
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[8]
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[13]
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[5]
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[6]
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide[11]
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System[9]
  - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control[10]

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 conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance,* [12] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

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

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

1.6 - Conventions

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

1.6.1 - Language

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

1.6.2 - Typography

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

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

1.6.3 - 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

This technical specification depends on the technical specifications, documentation, and implementations listed in the following table. The dependencies listed below are referenced in this encoding specification, and are normative or informative as indicated in the dependencies table.

Table 2 - Dependencies

Name	Dependency Description
Schematron[19]	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[25] query binding.
XSLT 2.0[25] implementation of Schematron[19] 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 GENC CVE is normative.
The GENC Standard out of the Country Code Working Group[2]	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.

1.7.1 - Standalone and Convenience Packages

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

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

1.8 - Conformance

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

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

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron[19] rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[14] is considered normative within the scope of the sentence. All other parts of this document are informative.

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

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

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.”[20] 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.”[21]

In a fashion similar to DocBook there is a “version” attribute (i.e., **DESVersion**, **CESVersion**, **version**) defined in each namespace defined in an IC CIO specification used to capture the version number assigned to each revision of the specification. The **DESVersion** attribute is the only indicator in an instance document as to what revision of a particular specification the author intended the instance to be valid to. Since the namespace does not change, the “version” attribute is required to fully understand the instance document

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

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

1.9.2 - Version Numbering

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

Chapter 2 - Development Guidance

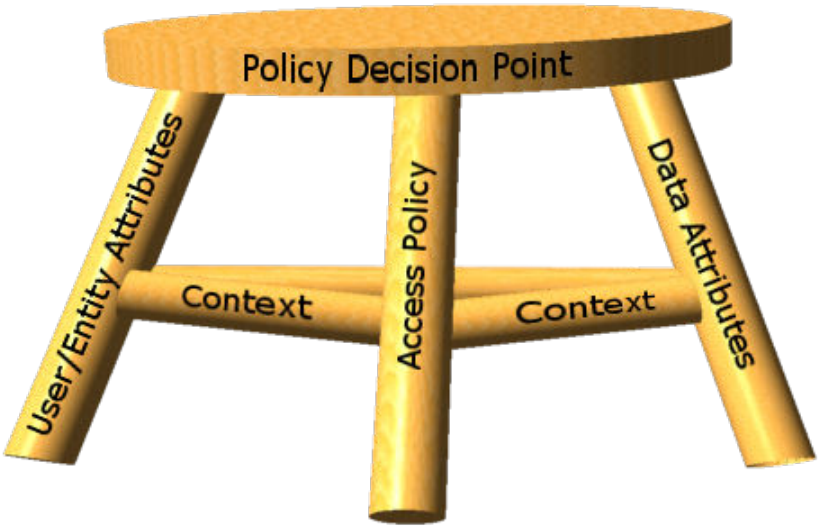
2.1 - Relationship to Abstract Data Definition and other encodings

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



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

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

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.

For a mapping of GENC versions, codespaces, and code values please see Appendix C - GENC Baseline Code-Space Code-Value Mappings .

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 CVE file 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.

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.[4] 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 - Terminology

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

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

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

3.5 - Errors and Warnings

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

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

3.6 - Rule Identifiers

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

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

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

The GENC.XML 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[19] 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[19] rules for this specification may be executed in *Oxygen*® [18] or with an XSLT 2.0[25]-compliant processor using the XSLT 2.0[25] transforms in the Schematron implementation from Rick Jelliffe (see XSLT 2.0 implementation of Schematron by Rick Jelliffe in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0[24] and XSLT 2.0[25] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:[17]

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

Note

For convenience, the specification package provides the XSLT 2.0[25] implementation of Schematron[19] 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 GENC.XML 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 not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

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

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

3.7.5 - Additional Constraints

3.7.5.1 - CES Constraints

The CES version for this specification is defined in the ISM . XML [15] 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 GENC.XML at this time.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

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

3.8.2 - Rendering Constraint Rules

The following table contains the information for the GENC.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.			

Chapter 4 - Conformance Validation

An instance document conforms with this specification if 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. 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.

Chapter 5 - Generated Guides

5.1 - Schema Guide

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

The guide was generated with a commercially available product named *oXygen*®,[18] 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 GENC.XML Schematron rules can be found in a separate document named *GENC_Rules.pdf,* which is located inside the Schematron/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 4 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can’t comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

A.1. GENC Feature Comparison

Table 5 - GENC Feature comparison

GENC Feature Comparison		
Required date	**Feature**	**V1**
	Defines the allowable values for Country Codes	F

Appendix B Change History

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

Table 6 - CES Version Identifier History

Version	Date	Purpose
1	14 March 2014	Initial Release

Appendix C GENC Baseline Code-Space Code-Value Mappings

This appendix is designed to simplify tracing codespace associations through the different baselines of the GENC standard.

C.1 - GENC Baseline 1-1

Promulgation Date: 2013-04-03

Table 7 - Codespace: ge:GENC:3:1-1

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
AFG	AFGHANISTAN
XQZ	AKROTIRI
ALB	ALBANIA
DZA	ALGERIA
ASM	AMERICAN SAMOA
AND	ANDORRA
AGO	ANGOLA
ATG	ANTIGUA AND BARBUDA
ARG	ARGENTINA
ARM	ARMENIA
ABW	ARUBA
XAC	ASHMORE AND CARTIER ISLANDS
AUS	AUSTRALIA
AUT	AUSTRIA
AZE	AZERBAIJAN
BHS	BAHAMAS, THE
BHR	BAHRAIN
XBK	BAKER ISLAND
BGD	BANGLADESH
XBI	BASSAS DA INDIA
BLR	BELARUS
BEL	BELGIUM
BEN	BENIN
BTN	BHUTAN
BOL	BOLIVIA
BES	BONAIRE, SINT EUSTATIUS, AND SABA
BWA	BOTSWANA

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
BRA	BRAZIL
IOT	BRITISH INDIAN OCEAN TERRITORY
BRN	BRUNEI
BGR	BULGARIA
BFA	BURKINA FASO
MMR	BURMA
BDI	BURUNDI
KHM	CAMBODIA
CMR	CAMEROON
CAN	CANADA
CPV	CAPE VERDE
CYM	CAYMAN ISLANDS
CAF	CENTRAL AFRICAN REPUBLIC
TCD	CHAD
CHL	CHILE
CHN	CHINA
CXR	CHRISTMAS ISLAND
CPT	CLIPPERTON ISLAND
CCK	COCOS (KEELING) ISLANDS
COL	COLOMBIA
COM	COMOROS
COG	CONGO (BRAZZAVILLE)
COD	CONGO (KINSHASA)
COK	COOK ISLANDS
XCS	CORAL SEA ISLANDS
CRI	COSTA RICA
CIV	CÔTE D'IVOIRE
HRV	CROATIA
CUB	CUBA
CUW	CURAÇAO
CYP	CYPRUS
CZE	CZECH REPUBLIC
DNK	DENMARK
XXD	DHEKELIA

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
DGA	DIEGO GARCIA
DJI	DJIBOUTI
DMA	DOMINICA
DOM	DOMINICAN REPUBLIC
ECU	ECUADOR
EGY	EGYPT
SLV	EL SALVADOR
XAZ	ENTITY 1
XCR	ENTITY 2
XCY	ENTITY 3
XKM	ENTITY 4
XKN	ENTITY 5
GNQ	EQUATORIAL GUINEA
ERI	ERITREA
EST	ESTONIA
ETH	ETHIOPIA
XQP	ETOROFU, HABOMAI, KUNASHIRI, AND SHIKOTAN ISLANDS
XEU	EUROPA ISLAND
FLK	FALKLAND ISLANDS (ISLAS MALVINAS)
FRO	FAROE ISLANDS
FJI	FIJI
FIN	FINLAND
FRA	FRANCE
GUF	FRENCH GUIANA
PYF	FRENCH POLYNESIA
ATF	FRENCH SOUTHERN AND ANTARCTIC LANDS
GAB	GABON
GMB	GAMBIA, THE
XGZ	GAZA STRIP
GEO	GEORGIA
DEU	GERMANY
GHA	GHANA
XGL	GLORIOSO ISLANDS
GRC	GREECE

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
GLP	GUADELOUPE
GUM	GUAM
AX2	GUANTANAMO BAY NAVAL BASE
GTM	GUATEMALA
GGY	GUERNSEY
GIN	GUINEA
GNB	GUINEA-BISSAU
GUY	GUYANA
HTI	HAITI
HMD	HEARD ISLAND AND MCDONALD ISLANDS
HND	HONDURAS
HKG	HONG KONG
XHO	HOWLAND ISLAND
ISL	ICELAND
IND	INDIA
IDN	INDONESIA
IRN	IRAN
IRQ	IRAQ
ISR	ISRAEL
ITA	ITALY
XJM	JAN MAYEN
XJV	JARVIS ISLAND
JEY	JERSEY
XJA	JOHNSTON ATOLL
JOR	JORDAN
XJN	JUAN DE NOVA ISLAND
KAZ	KAZAKHSTAN
KEN	KENYA
XKR	KINGMAN REEF
KIR	KIRIBATI
PRK	KOREA, NORTH
KOR	KOREA, SOUTH
XKS	KOSOVO
KWT	KUWAIT

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
KGZ	KYRGYZSTAN
LAO	LAOS
LVA	LATVIA
LBN	LEBANON
LSO	LESOTHO
LBR	LIBERIA
LIE	LIECHTENSTEIN
LTU	LITHUANIA
LUX	LUXEMBOURG
MAC	MACAU
MKD	MACEDONIA
MDG	MADAGASCAR
MWI	MALAWI
MYS	MALAYSIA
MDV	MALDIVES
MLI	MALI
MLT	MALTA
MHL	MARSHALL ISLANDS
MTQ	MARTINIQUE
MRT	MAURITANIA
MUS	MAURITIUS
MYT	MAYOTTE
MEX	MEXICO
FSM	MICRONESIA, FEDERATED STATES OF
XMW	MIDWAY ISLANDS
MDA	MOLDOVA
MCO	MONACO
MNG	MONGOLIA
MAR	MOROCCO
MOZ	MOZAMBIQUE
NAM	NAMIBIA
NRU	NAURU
XNV	NAVASSA ISLAND
NPL	NEPAL

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
NLD	NETHERLANDS
NCL	NEW CALEDONIA
NZL	NEW ZEALAND
NIC	NICARAGUA
NER	NIGER
NGA	NIGERIA
XXX	NO MAN'S LAND
NFK	NORFOLK ISLAND
MNP	NORTHERN MARIANA ISLANDS
NOR	NORWAY
OMN	OMAN
PAK	PAKISTAN
PLW	PALAU
PSE	PALESTINIAN TERRITORY
XPL	PALMYRA ATOLL
PAN	PANAMA
PNG	PAPUA NEW GUINEA
XPR	PARACEL ISLANDS
PRY	PARAGUAY
PER	PERU
PHL	PHILIPPINES
PCN	PITCAIRN ISLANDS
POL	POLAND
PRT	PORTUGAL
PRI	PUERTO RICO
QAT	QATAR
REU	REUNION
RUS	RUSSIA
RWA	RWANDA
BLM	SAINT BARTHELEMY
SHN	SAINT HELENA, ASCENSION, AND TRISTAN DA CUNHA
KNA	SAINT KITTS AND NEVIS
MAF	SAINT MARTIN
SPM	SAINT PIERRE AND MIQUELON

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
VCT	SAINT VINCENT AND THE GRENADINES
WSM	SAMOA
SMR	SAN MARINO
STP	SAO TOME AND PRINCIPE
SAU	SAUDI ARABIA
SEN	SENEGAL
SRB	SERBIA
SYC	SEYCHELLES
SLE	SIERRA LEONE
SGP	SINGAPORE
SXM	SINT MAARTEN
SVK	SLOVAKIA
SVN	SLOVENIA
SLB	SOLOMON ISLANDS
SOM	SOMALIA
ZAF	SOUTH AFRICA
SGS	SOUTH GEORGIA AND SOUTH SANDWICH ISLANDS
SSD	SOUTH SUDAN
ESP	SPAIN
XSP	SPRATLY ISLANDS
LKA	SRI LANKA
SDN	SUDAN
SUR	SURINAME
XSV	SVALBARD
SWZ	SWAZILAND
SWE	SWEDEN
CHE	SWITZERLAND
SYR	SYRIA
TWN	TAIWAN
TJK	TAJIKISTAN
TZA	TANZANIA
THA	THAILAND
TLS	TIMOR-LESTE
TGO	TOGO

Codespace: ge:GENC:3:1-1	
Code Value	**Name**
TON	TONGA
TTO	TRINIDAD AND TOBAGO
XTR	TROMELIN ISLAND
TUN	TUNISIA
TUR	TURKEY
TCA	TURKS AND CAICOS ISLANDS
UGA	UGANDA
UKR	UKRAINE
ARE	UNITED ARAB EMIRATES
GBR	UNITED KINGDOM
USA	UNITED STATES
AX1	UNKNOWN
URY	URUGUAY
UZB	UZBEKISTAN
VUT	VANUATU
VAT	VATICAN CITY
VEN	VENEZUELA
VNM	VIETNAM
VGB	VIRGIN ISLANDS, BRITISH
VIR	VIRGIN ISLANDS, U.S.
XWK	WAKE ISLAND
WLF	WALLIS AND FUTUNA
XWB	WEST BANK
ESH	WESTERN SAHARA
YEM	YEMEN
ZMB	ZAMBIA
ZWE	ZIMBABWE

Table 8 - Codespace: ge:ISO1:3:VI-14

Codespace: ge:ISO1:3:VI-14	
Code Value	**Name**
AIA	ANGUILLA
ATA	ANTARCTICA
BRB	BARBADOS

Codespace: ge:ISO1:3:VI-14	
Code Value	**Name**
BLZ	BELIZE
BMU	BERMUDA
BIH	BOSNIA AND HERZEGOVINA
BVT	BOUVET ISLAND
GIB	GIBRALTAR
GRL	GREENLAND
GRD	GRENADA
HUN	HUNGARY
IRL	IRELAND
IMN	ISLE OF MAN
JAM	JAMAICA
JPN	JAPAN
LBY	LIBYA
MNE	MONTENEGRO
MSR	MONTSERRAT
NIU	NIUE
ROU	ROMANIA
LCA	SAINT LUCIA
TKL	TOKELAU
TKM	TURKMENISTAN
TUV	TUVALU

C.2 - GENC Baseline 1-2

Promulgation Date: 2013-06-30

Table 9 - Codespace: ge:GENC:3:1-2

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
AFG	AFGHANISTAN
XQZ	AKROTIRI
ALB	ALBANIA
DZA	ALGERIA
ASM	AMERICAN SAMOA
AND	ANDORRA
AGO	ANGOLA

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
ATG	ANTIGUA AND BARBUDA
ARG	ARGENTINA
ARM	ARMENIA
ABW	ARUBA
XAC	ASHMORE AND CARTIER ISLANDS
AUS	AUSTRALIA
AUT	AUSTRIA
AZE	AZERBAIJAN
BHS	BAHAMAS, THE
BHR	BAHRAIN
XBK	BAKER ISLAND
BGD	BANGLADESH
XBI	BASSAS DA INDIA
BLR	BELARUS
BEL	BELGIUM
BEN	BENIN
BTN	BHUTAN
BOL	BOLIVIA
BES	BONAIRE, SINT EUSTATIUS, AND SABA
BWA	BOTSWANA
BRA	BRAZIL
IOT	BRITISH INDIAN OCEAN TERRITORY
BRN	BRUNEI
BGR	BULGARIA
BFA	BURKINA FASO
MMR	BURMA
BDI	BURUNDI
KHM	CAMBODIA
CMR	CAMEROON
CAN	CANADA
CPV	CAPE VERDE
CYM	CAYMAN ISLANDS
CAF	CENTRAL AFRICAN REPUBLIC
TCD	CHAD

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
CHL	CHILE
CHN	CHINA
CXR	CHRISTMAS ISLAND
CPT	CLIPPERTON ISLAND
CCK	COCOS (KEELING) ISLANDS
COL	COLOMBIA
COM	COMOROS
COG	CONGO (BRAZZAVILLE)
COD	CONGO (KINSHASA)
COK	COOK ISLANDS
XCS	CORAL SEA ISLANDS
CRI	COSTA RICA
CIV	CÔTE D'IVOIRE
HRV	CROATIA
CUB	CUBA
CUW	CURAÇAO
CYP	CYPRUS
CZE	CZECH REPUBLIC
DNK	DENMARK
XXD	DHEKELIA
DGA	DIEGO GARCIA
DJI	DJIBOUTI
DMA	DOMINICA
DOM	DOMINICAN REPUBLIC
ECU	ECUADOR
EGY	EGYPT
SLV	EL SALVADOR
XAZ	ENTITY 1
XCR	ENTITY 2
XCY	ENTITY 3
XKM	ENTITY 4
XKN	ENTITY 5
GNQ	EQUATORIAL GUINEA
ERI	ERITREA

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
EST	ESTONIA
ETH	ETHIOPIA
XQP	ETOROFU, HABOMAI, KUNASHIRI, AND SHIKOTAN ISLANDS
XEU	EUROPA ISLAND
FLK	FALKLAND ISLANDS (ISLAS MALVINAS)
FRO	FAROE ISLANDS
FJI	FIJI
FIN	FINLAND
FRA	FRANCE
GUF	FRENCH GUIANA
PYF	FRENCH POLYNESIA
ATF	FRENCH SOUTHERN AND ANTARCTIC LANDS
GAB	GABON
GMB	GAMBIA, THE
XGZ	GAZA STRIP
GEO	GEORGIA
DEU	GERMANY
GHA	GHANA
XGL	GLORIOSO ISLANDS
GRC	GREECE
GLP	GUADELOUPE
GUM	GUAM
AX2	GUANTANAMO BAY NAVAL BASE
GTM	GUATEMALA
GGY	GUERNSEY
GIN	GUINEA
GNB	GUINEA-BISSAU
GUY	GUYANA
HTI	HAITI
HMD	HEARD ISLAND AND MCDONALD ISLANDS
HND	HONDURAS
HKG	HONG KONG
XHO	HOWLAND ISLAND
ISL	ICELAND

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
IND	INDIA
IDN	INDONESIA
IRN	IRAN
IRQ	IRAQ
ISR	ISRAEL
ITA	ITALY
XJM	JAN MAYEN
XJV	JARVIS ISLAND
JEY	JERSEY
XJA	JOHNSTON ATOLL
JOR	JORDAN
XJN	JUAN DE NOVA ISLAND
KAZ	KAZAKHSTAN
KEN	KENYA
XKR	KINGMAN REEF
KIR	KIRIBATI
PRK	KOREA, NORTH
KOR	KOREA, SOUTH
XKS	KOSOVO
KWT	KUWAIT
KGZ	KYRGYZSTAN
LAO	LAOS
LVA	LATVIA
LBN	LEBANON
LSO	LESOTHO
LBR	LIBERIA
LIE	LIECHTENSTEIN
LTU	LITHUANIA
LUX	LUXEMBOURG
MAC	MACAU
MKD	MACEDONIA
MDG	MADAGASCAR
MWI	MALAWI
MYS	MALAYSIA

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
MDV	MALDIVES
MLI	MALI
MLT	MALTA
MHL	MARSHALL ISLANDS
MTQ	MARTINIQUE
MRT	MAURITANIA
MUS	MAURITIUS
MYT	MAYOTTE
MEX	MEXICO
FSM	MICRONESIA, FEDERATED STATES OF
XMW	MIDWAY ISLANDS
MDA	MOLDOVA
MCO	MONACO
MNG	MONGOLIA
MAR	MOROCCO
MOZ	MOZAMBIQUE
NAM	NAMIBIA
NRU	NAURU
XNV	NAVASSA ISLAND
NPL	NEPAL
NLD	NETHERLANDS
NCL	NEW CALEDONIA
NZL	NEW ZEALAND
NIC	NICARAGUA
NER	NIGER
NGA	NIGERIA
XXX	NO MAN'S LAND
NFK	NORFOLK ISLAND
MNP	NORTHERN MARIANA ISLANDS
NOR	NORWAY
OMN	OMAN
PAK	PAKISTAN
PLW	PALAU
PSE	PALESTINIAN TERRITORY

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
XPL	PALMYRA ATOLL
PAN	PANAMA
XPR	PARACEL ISLANDS
PRY	PARAGUAY
PER	PERU
PHL	PHILIPPINES
PCN	PITCAIRN ISLANDS
POL	POLAND
PRT	PORTUGAL
PRI	PUERTO RICO
QAT	QATAR
REU	REUNION
RUS	RUSSIA
RWA	RWANDA
BLM	SAINT BARTHELEMY
SHN	SAINT HELENA, ASCENSION, AND TRISTAN DA CUNHA
KNA	SAINT KITTS AND NEVIS
MAF	SAINT MARTIN
SPM	SAINT PIERRE AND MIQUELON
VCT	SAINT VINCENT AND THE GRENADINES
WSM	SAMOA
SMR	SAN MARINO
STP	SAO TOME AND PRINCIPE
SAU	SAUDI ARABIA
SEN	SENEGAL
SRB	SERBIA
SYC	SEYCHELLES
SLE	SIERRA LEONE
SGP	SINGAPORE
SXM	SINT MAARTEN
SVK	SLOVAKIA
SVN	SLOVENIA
SLB	SOLOMON ISLANDS
SOM	SOMALIA

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
ZAF	SOUTH AFRICA
SGS	SOUTH GEORGIA AND SOUTH SANDWICH ISLANDS
SSD	SOUTH SUDAN
ESP	SPAIN
XSP	SPRATLY ISLANDS
LKA	SRI LANKA
SDN	SUDAN
SUR	SURINAME
XSV	SVALBARD
SWZ	SWAZILAND
SWE	SWEDEN
CHE	SWITZERLAND
SYR	SYRIA
TWN	TAIWAN
TJK	TAJIKISTAN
TZA	TANZANIA
THA	THAILAND
TLS	TIMOR-LESTE
TGO	TOGO
TON	TONGA
TTO	TRINIDAD AND TOBAGO
XTR	TROMELIN ISLAND
TUN	TUNISIA
TUR	TURKEY
TCA	TURKS AND CAICOS ISLANDS
UGA	UGANDA
UKR	UKRAINE
ARE	UNITED ARAB EMIRATES
GBR	UNITED KINGDOM
USA	UNITED STATES
AX1	UNKNOWN
URY	URUGUAY
UZB	UZBEKISTAN
VUT	VANUATU

Codespace: ge:GENC:3:1-2	
Code Value	**Name**
VAT	VATICAN CITY
VEN	VENEZUELA
VNM	VIETNAM
VGB	VIRGIN ISLANDS, BRITISH
VIR	VIRGIN ISLANDS, U.S.
XWK	WAKE ISLAND
WLF	WALLIS AND FUTUNA
XWB	WEST BANK
ESH	WESTERN SAHARA
YEM	YEMEN
ZMB	ZAMBIA
ZWE	ZIMBABWE

Table 10 - Codespace: ge:ISO1:3:VI-15

Codespace: ge:ISO1:3:VI-15	
Code Value	**Name**
AIA	ANGUILLA
ATA	ANTARCTICA
BRB	BARBADOS
BLZ	BELIZE
BMU	BERMUDA
BIH	BOSNIA AND HERZEGOVINA
BVT	BOUVET ISLAND
GIB	GIBRALTAR
GRL	GREENLAND
GRD	GRENADA
HUN	HUNGARY
IRL	IRELAND
IMN	ISLE OF MAN
JAM	JAMAICA
JPN	JAPAN
LBY	LIBYA
MNE	MONTENEGRO
MSR	MONTSERRAT

Codespace: ge:ISO1:3:VI-15	
Code Value	**Name**
NIU	NIUE
PNG	PAPUA NEW GUINEA
ROU	ROMANIA
LCA	SAINT LUCIA
TKL	TOKELAU
TKM	TURKMENISTAN
TUV	TUVALU

C.3 - GENC Baseline ed1

Promulgation Date: 2012-09-01

Table 11 - Codespace: ge:GENC:3:ed1

Codespace: ge:GENC:3:ed1	
Code Value	**Name**
AFG	AFGHANISTAN
XQZ	AKROTIRI
ALB	ALBANIA
ASM	AMERICAN SAMOA
ATG	ANTIGUA AND BARBUDA
ABW	ARUBA
XAC	ASHMORE AND CARTIER ISLANDS
AUS	AUSTRALIA
BHS	BAHAMAS, THE
XBK	BAKER ISLAND
BGD	BANGLADESH
XBI	BASSAS DA INDIA
BLR	BELARUS
BOL	BOLIVIA
BES	BONAIRE, SINT EUSTATIUS, AND SABA
BRA	BRAZIL
IOT	BRITISH INDIAN OCEAN TERRITORY
BRN	BRUNEI
BGR	BULGARIA
BFA	BURKINA FASO
MMR	BURMA

Codespace: ge:GENC:3:ed1	
Code Value	**Name**
CPV	CAPE VERDE
CAF	CENTRAL AFRICAN REPUBLIC
CHL	CHILE
CHN	CHINA
CXR	CHRISTMAS ISLAND
CPT	CLIPPERTON ISLAND
CCK	COCOS (KEELING) ISLANDS
COL	COLOMBIA
COM	COMOROS
COG	CONGO (BRAZZAVILLE)
COD	CONGO (KINSHASA)
XCS	CORAL SEA ISLANDS
CRI	COSTA RICA
CUB	CUBA
CUW	CURAÇAO
CYP	CYPRUS
CZE	CZECH REPUBLIC
XXD	DHEKELIA
DGA	DIEGO GARCIA
ECU	ECUADOR
XAZ	ENTITY 1
XCR	ENTITY 2
XCY	ENTITY 3
XKM	ENTITY 4
XKN	ENTITY 5
GNQ	EQUATORIAL GUINEA
XQP	ETOROFU, HABOMAI, KUNASHIRI, AND SHIKOTAN ISLANDS
XEU	EUROPA ISLAND
FLK	FALKLAND ISLANDS (ISLAS MALVINAS)
FRA	FRANCE
GUF	FRENCH GUIANA
PYF	FRENCH POLYNESIA
ATF	FRENCH SOUTHERN AND ANTARCTIC LANDS
GMB	GAMBIA, THE

Codespace: ge:GENC:3:ed1	
Code Value	**Name**
XGZ	GAZA STRIP
GEO	GEORGIA
XGL	GLORIOSO ISLANDS
GLP	GUADELOUPE
GUM	GUAM
AX2	GUANTANAMO BAY NAVAL BASE
GGY	GUERNSEY
GUY	GUYANA
HMD	HEARD ISLAND AND MCDONALD ISLANDS
HKG	HONG KONG
XHO	HOWLAND ISLAND
IND	INDIA
IRN	IRAN
ITA	ITALY
XJM	JAN MAYEN
XJV	JARVIS ISLAND
JEY	JERSEY
XJA	JOHNSTON ATOLL
XJN	JUAN DE NOVA ISLAND
XKR	KINGMAN REEF
KIR	KIRIBATI
PRK	KOREA, NORTH
KOR	KOREA, SOUTH
XKS	KOSOVO
LAO	LAOS
MAC	MACAU
MKD	MACEDONIA
MYS	MALAYSIA
MHL	MARSHALL ISLANDS
MTQ	MARTINIQUE
MUS	MAURITIUS
MYT	MAYOTTE
FSM	MICRONESIA, FEDERATED STATES OF
XMW	MIDWAY ISLANDS

Codespace: ge:GENC:3:ed1	
Code Value	**Name**
MDA	MOLDOVA
MNG	MONGOLIA
XNV	NAVASSA ISLAND
NLD	NETHERLANDS
NCL	NEW CALEDONIA
NZL	NEW ZEALAND
XXX	NO MAN'S LAND
NFK	NORFOLK ISLAND
MNP	NORTHERN MARIANA ISLANDS
NOR	NORWAY
OMN	OMAN
PSE	PALESTINIAN TERRITORY
XPL	PALMYRA ATOLL
PNG	PAPUA NEW GUINEA
XPR	PARACEL ISLANDS
PHL	PHILIPPINES
PCN	PITCAIRN ISLANDS
PRI	PUERTO RICO
REU	REUNION
RUS	RUSSIA
BLM	SAINT BARTHELEMY
SHN	SAINT HELENA, ASCENSION, AND TRISTAN DA CUNHA
MAF	SAINT MARTIN
SPM	SAINT PIERRE AND MIQUELON
VCT	SAINT VINCENT AND THE GRENADINES
SAU	SAUDI ARABIA
SRB	SERBIA
SYC	SEYCHELLES
SXM	SINT MAARTEN
SOM	SOMALIA
ZAF	SOUTH AFRICA
SGS	SOUTH GEORGIA AND SOUTH SANDWICH ISLANDS
XSP	SPRATLY ISLANDS
XSV	SVALBARD

Codespace: ge:GENC:3:ed1	
Code Value	**Name**
SYR	SYRIA
TWN	TAIWAN
TZA	TANZANIA
XTR	TROMELIN ISLAND
TUN	TUNISIA
UKR	UKRAINE
ARE	UNITED ARAB EMIRATES
USA	UNITED STATES
AX1	UNKNOWN
URY	URUGUAY
VUT	VANUATU
VAT	VATICAN CITY
VEN	VENEZUELA
VNM	VIETNAM
VGB	VIRGIN ISLANDS, BRITISH
VIR	VIRGIN ISLANDS, U.S.
XWK	WAKE ISLAND
WLF	WALLIS AND FUTUNA
XWB	WEST BANK
ESH	WESTERN SAHARA
YEM	YEMEN

Table 12 - Codespace: ge:ISO1:3:VI-13

Codespace: ge:ISO1:3:VI-13	
Code Value	**Name**
DZA	ALGERIA
AND	ANDORRA
AGO	ANGOLA
AIA	ANGUILLA
ATA	ANTARCTICA
ARG	ARGENTINA
ARM	ARMENIA
AUT	AUSTRIA
AZE	AZERBAIJAN

Codespace: ge:ISO1:3:VI-13	
Code Value	**Name**
BHR	BAHRAIN
BRB	BARBADOS
BEL	BELGIUM
BLZ	BELIZE
BEN	BENIN
BMU	BERMUDA
BTN	BHUTAN
BIH	BOSNIA AND HERZEGOVINA
BWA	BOTSWANA
BVT	BOUVET ISLAND
BDI	BURUNDI
KHM	CAMBODIA
CMR	CAMEROON
CAN	CANADA
CYM	CAYMAN ISLANDS
TCD	CHAD
COK	COOK ISLANDS
CIV	CÔTE D'IVOIRE
HRV	CROATIA
DNK	DENMARK
DJI	DJIBOUTI
DMA	DOMINICA
DOM	DOMINICAN REPUBLIC
EGY	EGYPT
SLV	EL SALVADOR
ERI	ERITREA
EST	ESTONIA
ETH	ETHIOPIA
FRO	FAROE ISLANDS
FJI	FIJI
FIN	FINLAND
GAB	GABON
DEU	GERMANY
GHA	GHANA

Codespace: ge:ISO1:3:VI-13	
Code Value	**Name**
GIB	GIBRALTAR
GRC	GREECE
GRL	GREENLAND
GRD	GRENADA
GTM	GUATEMALA
GIN	GUINEA
GNB	GUINEA-BISSAU
HTI	HAITI
HND	HONDURAS
HUN	HUNGARY
ISL	ICELAND
IDN	INDONESIA
IRQ	IRAQ
IRL	IRELAND
IMN	ISLE OF MAN
ISR	ISRAEL
JAM	JAMAICA
JPN	JAPAN
JOR	JORDAN
KAZ	KAZAKHSTAN
KEN	KENYA
KWT	KUWAIT
KGZ	KYRGYZSTAN
LVA	LATVIA
LBN	LEBANON
LSO	LESOTHO
LBR	LIBERIA
LBY	LIBYA
LIE	LIECHTENSTEIN
LTU	LITHUANIA
LUX	LUXEMBOURG
MDG	MADAGASCAR
MWI	MALAWI
MDV	MALDIVES

Codespace: ge:ISO1:3:VI-13	
Code Value	**Name**
MLI	MALI
MLT	MALTA
MRT	MAURITANIA
MEX	MEXICO
MCO	MONACO
MNE	MONTENEGRO
MSR	MONTSERRAT
MAR	MOROCCO
MOZ	MOZAMBIQUE
NAM	NAMIBIA
NRU	NAURU
NPL	NEPAL
NIC	NICARAGUA
NER	NIGER
NGA	NIGERIA
NIU	NIUE
PAK	PAKISTAN
PLW	PALAU
PAN	PANAMA
PRY	PARAGUAY
PER	PERU
POL	POLAND
PRT	PORTUGAL
QAT	QATAR
ROU	ROMANIA
RWA	RWANDA
KNA	SAINT KITTS AND NEVIS
LCA	SAINT LUCIA
WSM	SAMOA
SMR	SAN MARINO
STP	SAO TOME AND PRINCIPE
SEN	SENEGAL
SLE	SIERRA LEONE
SGP	SINGAPORE

Codespace: ge:ISO1:3:VI-13	
Code Value	**Name**
SVK	SLOVAKIA
SVN	SLOVENIA
SLB	SOLOMON ISLANDS
SSD	SOUTH SUDAN
ESP	SPAIN
LKA	SRI LANKA
SDN	SUDAN
SUR	SURINAME
SWZ	SWAZILAND
SWE	SWEDEN
CHE	SWITZERLAND
TJK	TAJIKISTAN
THA	THAILAND
TLS	TIMOR-LESTE
TGO	TOGO
TKL	TOKELAU
TON	TONGA
TTO	TRINIDAD AND TOBAGO
TUR	TURKEY
TKM	TURKMENISTAN
TCA	TURKS AND CAICOS ISLANDS
TUV	TUVALU
UGA	UGANDA
GBR	UNITED KINGDOM
UZB	UZBEKISTAN
ZMB	ZAMBIA
ZWE	ZIMBABWE

Appendix D Glossary

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

ADD	Abstract Data Definition
ARH	Access Rights and Handling
CES	CVE Encoding Specification
CIO	Chief Information Officer
CVE	Controlled Vocabulary Enumeration
DNI	Director of National Intelligence
EI&A	Enterprise Integration and Architecture
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	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICO-NTK	Intelligence Community Only Need-to-Know
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
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
OC-NTK	Originator Controlled Need-to-Know
ODNI	Office of the Director of National Intelligence
PDF	Portable Document Format
PDP	Policy Decision Point
PROPIN	Proprietary Information
PROPIN-NTK	Data Encoding Specification for Proprietary Information Need-To-Know
PUBS	Intelligence Publications
RFC	Request for Comments
TDF	Trusted Data Format
URN	Uniform Resource Name
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix E Bibliography

Bibliography

[1] 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

[2] GENC
Country Codes Working Group. *Geopolitical Entities, Names, and Codes*. 1.0.
Available online at: https://nsgreg.nga.mil/doc/view?i=2324

[3] IC ITE INC1 IMPL
Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at: http://go.ic.gov/HvBHBmY

[4] ICD 206
Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Intelligence Products*. Intelligence Community Directive 206. 17 October 2007.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_206.pdf

[5] 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

[6] ICD 209
Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.
Available online at: http://www.dni.gov/files/documents/ICD/ICD 209 Tearline Production and Dissemination.pdf [http://www.dni.gov/files/documents/ICD/ICD 209 Tearline Production and Dissemination.pdf]

[7] ICD 500
Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.
Available online Intelink-TS at: http://go.ic.gov/enm8L9x
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[8] 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

[9] 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

[10] ICPG 710.1
Assistant Director of National Intelligence for . *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at: http://go.ic.gov/yAqVQ0H

[11] ICPM 2007-200-2
Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2, . 11 December 2007.
Available online at: http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf

[12] ICS 500-20
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.
Available online Intelink-TS at: http://go.ic.gov/QUDIJkZ
Available online Intelink-U at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[13] ICS 500-21
Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online Intelink-U at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[14] IETF-RFC 2119
Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.
Available online at: http://tools.ietf.org/html/rfc2119

[15] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML)*.
Available online Intelink-U at: http://purl.org/IC/Standards/ISM
Available online at: http://purl.org/IC/Standards/public

[16] 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

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

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

[19] 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/ [http://code.google.com/p/schematron//]

[20] 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

[21] 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

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

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

[24] XPath2
World Wide Web Consortium (W3C). *XML Path Language (XPath) 2.0 (Second Edition)*. W3C Recommendation 14 December 2010 (Link errors corrected 3 January 2011).
Available online at: http://www.w3.org/TR/xpath20/

[25] XSLT2
World Wide Web Consortium (W3C). *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.
Available online at: http://www.w3.org/TR/xslt20/

Appendix F Points of Contact

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

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

E-mail: ic-standards-support@intelink.gov [mailto:ic-standards-support@intelink.gov].

Appendix G IC CIO Approval Memo

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

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

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.[12]