



Intelligence Community Technical Specification

CVE Encoding Specification for Geopolitical Entities, Names, and Codes

Version 2021-NOV

December 1, 2022

Distribution Notice:

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

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Enterprise Need	2
1.4 - Conventions	2
1.4.1 - XML Namespaces	3
1.5 - Dependencies	3
1.5.1 - Specification Dependencies	3
1.5.2 - Inverse Dependencies	5
Chapter 2 - Development Guidance	7
2.1 - Relationship to Abstract Data Definition and other encodings	7
2.2 - Understanding Access Control	7
2.3 - Additional Guidance	7
2.3.1 - The CVEs	7
2.3.2 - The Schematron Abstract Pattern	8
Chapter 3 - Constraints	9
3.1 - “Living” Constraint Rules	9
3.2 - Data Validation Constraint Rules	9
3.2.1 - Vocabulary Enumeration Constraints	9
3.2.2 - Additional Constraints	9
3.2.2.1 - CES Constraints	9
3.2.3 - Constraint Rules	10
3.3 - Data Rendering Constraint Rules	10
3.3.1 - Purpose	10
3.3.2 - Rendering Constraint Rules	10
Appendix A - Feature Summary	11
A.1 - IC-GENC Feature Summary	11
A.1.1 - Features from V2019-MAR to V2021-NOV	11
A.1.2 - Features from V2016-SEP to V2019-MAR	11
A.1.3 - Features from V1 to V2016-SEP	12
Appendix B - Change History	13
B.1 - V2021-NOV Change Summary	13
B.2 - V2019-SEP Change Summary	14
B.3 - V2019-JUN Change Summary	14
B.4 - V2019-MAR Change Summary	14
B.5 - V2017-SEP Change Summary	15
B.6 - V2017-JUL Change Summary	16
B.7 - V2016-SEP Change Summary	17
B.8 - V2015-MAY Change Summary	17
Appendix C - List of Abbreviations	19
Appendix D - Bibliography	20
Appendix E - Points of Contact	23
Appendix F - IC CIO Approval Memo	24

List of Figures

Figure 1 - Related Specifications	5
Figure 2 - Inverse Dependency Specifications	6

List of Tables

Table 1 - XML Namepaces	3
Table 2 - Dependencies	3
Table 3 - Constraint Rules	10
Table 4 - Feature Summary Legend	11
Table 5 - IC-GENC Feature comparison V2019-MAR to V2021-NOV	11
Table 6 - IC-GENC Feature comparison V2016-SEP to V2019-MAR	11
Table 7 - IC-GENC Feature comparison V1 to V2016-SEP	12
Table 8 - CES Version Identifier History	13
Table 9 - V2021-NOV Change Summary	14
Table 10 - V2019-SEP Change Summary	14
Table 11 - V2019-JUN Change Summary	14
Table 12 - V2019-MAR Change Summary	15
Table 13 - V2017-SEP Change Summary	15
Table 14 - Data Encoding Specification V2017-JUL Change Summary	16
Table 15 - Data Encoding Specification V2016-SEP Change Summary	17
Table 16 - Data Encoding Specification V2015-MAY Change Summary	18

Chapter 1 - Introduction

1.1 - Purpose

This *CVE Encoding Specification for Geopolitical Entities, Names, and Codes* (IC-GENC.CES) defines detailed implementation guidance using several encoding formats including Extensible Markup Language (XML), Comma Separated Value (CSV) and JavaScript Object Notation (JSON) to encode IC-GENC.CES controlled vocabulary. This Controlled Vocabulary Enumeration 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 a variety of formats.

In September 2, 2008, the U.S. Federal Government moved away from National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 10-4 standard, *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*^[1])¹ of identifying different country locations using a two-character code base. The FIPS 10-4^[1] standard was identified to be replaced by the open standard International Organization for Standardization (ISO) 3166-1, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*^[14]. 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 3166-1^[14] called Geopolitical Entities, Names, and Codes (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. IC-GENC.CES will use ISO 3166-1^[14] 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^[2] 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^[2] Registry, not to be confused with the GENC Standard. Country codes have been part of the GENC^[2] Registry since GENC^[2] Edition 1 and thus allowing the use of the newer codespaces is actually still holding to conformance with the GENC^[2] Ed 1 standard regardless of Edition or version that might be represented in the codespace.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[4]) defines the basic conceptual structure and outlines the core philosophy of IC technical specifications. For convenience, a copy of this framework is included in every package.

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].

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 - Enterprise Need

Many IC encoding specifications use Controlled Vocabulary Enumeration (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 CVEs that contain the GENC country codes allowing this specification to revise in tandem with the GENC^[2] 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 Specification (DES).

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 200 Series:
 - Intelligence Community Directive (ICD) 206, *Sourcing Requirements for Disseminated Analytic Products* ^[5]
 - ICD 208, *Write for Maximum Utility* ^[6]
 - ICD 209, *Tearline Production and Dissemination* ^[7]
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide* ^[10]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[8]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* ^[9]
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* ^[11]
 - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[12]
- Federal Laws & Regulations:
 - *Public Law 242-80th Congress* ^[15]

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the "Specification Conventions" chapter in the IC-SF.XML^[4].

1.4.1 - XML Namespaces

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

Table 1 - XML Namespaces

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

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML^[4].

1.5.1 - 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
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[4])	This specification does not depend on a specific version of IC-SF.XML ^[4] ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.

Name	Dependency Description
Schematron ^[16]	<p>Schematron — ISO/International Electrotechnical Commission (IEC) 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use Transformations (XSLT) 2.0^[17] query binding.</p>
<p>XSLT 2.0^[17] implementation of Schematron^[16] by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>
The GENC Registry out of the Country Code Working Group ^[2] .	Depends on GENC which is the US Government profile of ISO 3166-1, <i>Codes for the representation of names of countries and their subdivisions – Part 1: Country codes</i> ^[14] .

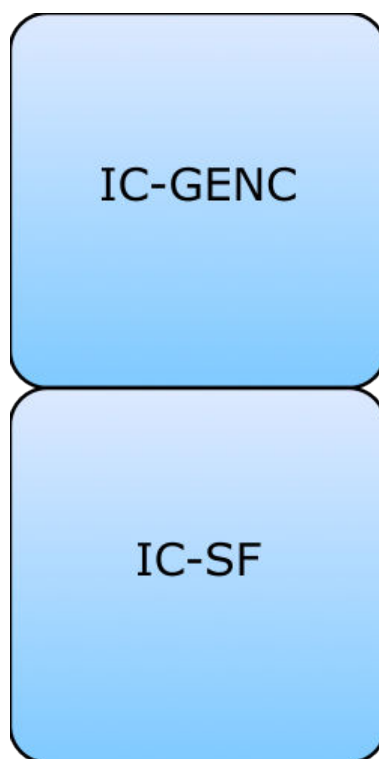


Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

Generally, it is only necessary to think of the *dependencies* in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies*, 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 (specifications that uses the given specification).

Since this specification is one such specification that is used by other specifications released by the Intelligence Community Chief Information Officer (IC CIO), the [Figure 2](#) has been included to assist readers in understanding all of the inverse dependency relationships and how changes in this given specification may impact others specifications. This diagram is representative of direct and transitive inverse dependencies at the time of the release of this specification, but are subject to change over time and is presented in a list format that is different than [Figure 1](#).

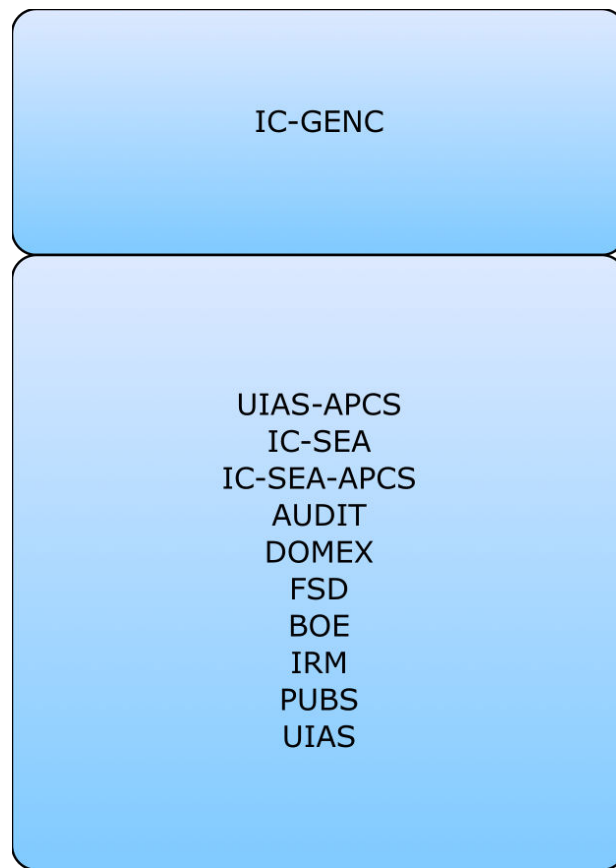


Figure 2 : Inverse Dependency Specifications

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 Abstract Data Definition (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

This specification participates in the Data Attributes and User/Entity Attributes legs of the access control framework either as a primary specification or as a dependency of a primary specification. For more information, please see the “Components of Access Control Decisions” chapter in the IC-SF.XML^[4] framework document.

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.CES 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^[2] 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 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.



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 Document and Media Exploitation (DOMEX), are retired. Developers SHOULD NOT use these patterns in new work.

Chapter 3 - Constraints

3.1 - “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, *Sourcing Requirements for Disseminated Analytic Products* [5]. 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.

3.2 - Data Validation Constraint Rules

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.

3.2.1 - 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 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.

3.2.2 - Additional Constraints

3.2.2.1 - CES Constraints

The CES version for this specification is defined in the *XML Data Encoding Specification for Information Security Markings* (ISM.XML^[13]) 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.

3.2.3 - Constraint Rules

The detailed constraint rules for the IC-GENC.CES schema can be found in a separate document inside the Documents/IC-GENC directory, in the “IC-GENC_Rules.pdf” file. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron. Obsolete rule numbers are listed in the “IC-GENC_Rules.pdf” file.

3.3 - Data Rendering Constraint Rules

3.3.1 - 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.

3.3.2 - Rendering Constraint Rules

The following table contains the information for the IC-GENC.CES 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.			

Appendix A Feature Summary

The following table summarizes major features by version for IC-GENC.CES 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, *Intelligence Community Markings System Register and Manual* ^[3], the date is often one year after the date of publication. Executive Orders, Information Security Oversight Office (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. IC-GENC Feature Summary

A.1.1. Features from V2019-MAR to V2021-NOV

Table 5 - IC-GENC Feature comparison V2019-MAR to V2021-NOV

Required date	Feature	V2019-MAR	V2019-JUN	V2019-SEP	V2021-NOV
	Support codes and names for countries and subdivisions consistent with the update through GENC ^[2] Edition 3 Update 10	N	F	F	F
	Support codes and names for countries and subdivisions consistent with the update through GENC ^[2] Edition 3 Update 11	N	N	F	F

A.1.2. Features from V2016-SEP to V2019-MAR

Table 6 - IC-GENC Feature comparison V2016-SEP to V2019-MAR

Required date	Feature	V2016-SEP	V2017-JUL	V2017-SEP	V2019-MAR
	Support codes and names for countries and subdivisions consistent with the update through GENC ^[2] Edition 3 Updates 5 and 6	N	F	F	F
	Support codes and names for countries and subdivisions consistent with the update through GENC ^[2] Edition 3 Update 7	N	N	F	F
	Support codes and names for countries and subdivisions consistent with the update through GENC ^[2] Edition 3 Updates 8 and 9	N	N	N	F

A.1.3. Features from V1 to V2016-SEP

Table 7 - IC-GENC Feature comparison V1 to V2016-SEP

Required date	Feature	V1	V2015-MAY	V2016-SEP
	Support codes and names for countries consistent with the update of the GENC ^[2] registry promulgated on 2013-11-15	N	F	F
	Support codes and names for countries consistent with the update of the GENC ^[2] registry promulgated on 2013-12-30	N	F	F
	Support codes and names for countries consistent with the update of the GENC ^[2] registry promulgated on 2014-03-31	N	F	F
	Support codes and names for countries consistent with the update of the GENC ^[2] registry promulgated on 2014-06-30	N	F	F
	Support codes and names for countries consistent with the update of the GENC ^[2] registry promulgated on 2014-12-31	N	F	F
	Support codes and names for countries consistent with the update through GENC ^[2] Edition 3 Update 4	N	N	F
	Support codes and names for subdivisions consistent with the update through GENC ^[2] Edition 3 Update 4	N	N	F

Appendix B Change History

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

Table 8 - CES Version Identifier History

Version	Date	Purpose
1	March 14, 2014	Initial Release
2015-MAY	May 15, 2015	Routine revision to technical specification. For details of changes, see Section B.8 - V2015-MAY Change Summary
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see Section B.7 - V2016-SEP Change Summary
2017-JUL	July 21, 2017	Routine revision to technical specification. For details of changes, see Section B.6 - V2017-JUL Change Summary
2017-SEP	September 29, 2017	Routine revision to technical specification. For details of changes, see Section B.5 - V2017-SEP Change Summary
2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see Section B.4 - V2019-MAR Change Summary
2019-JUN	June 19, 2019	Routine revision to technical specification. For details of changes, see Section B.3 - V2019-JUN Change Summary
2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see Section B.2 - V2019-SEP Change Summary
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see Section B.1 - V2021-NOV Change Summary

B.1 - V2021-NOV Change Summary

Significant drivers for Version 2021-NOV include:

- Community Change Request.

The following table summarizes the changes made to V2019-SEP in developing V2021-NOV.

Table 9 - V2021-NOV Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated the Enterprise Needs table with the appropriate policies. (CR-2019-167)	Documentation	No impact to systems.

B.2 - V2019-SEP Change Summary

Significant drivers for Version 2019-SEP include:

- Updating to be aligned with the content of the GENC^[2] Edition 3 Update 11.

The following table summarizes the changes made to V2019-JUN in developing V2019-SEP.

Table 10 - V2019-SEP Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Update IC-GENC with Update 11 of the GENC Ed3.0 (CR-2019-133)	CVEs	Data generation and ingestion systems need to be updated to handle the added GENC updates.
2	Update chapters for consistency with other specifications. (CR-2019-099)	Documentation	No impact to systems.
3	Identify the lack of a root node in the Schema Guide. (CR-2019-119)	Schema	No impact to systems.

B.3 - V2019-JUN Change Summary

Significant drivers for Version 2019-JUN include:

- Updating to be aligned with the content of the GENC^[2] Edition 3 Update 10.

The following table summarizes the changes made to V2019-MAR in developing V2019-JUN.

Table 11 - V2019-JUN Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Update IC-GENC with Update 10 of the GENC Ed3.0 (CR-2019-069)	CVEs	Data generation and ingestion systems need to be updated to handle the added GENC updates.

B.4 - V2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- Updating to be aligned with the content of the GENC^[2] Edition 3 Updates 8 and 9.

The following table summarizes the changes made to V2017-SEP in developing V2019-MAR.

Table 12 - V2019-MAR Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated documentation to use the specification framework. (CR-2018-126, CR-2018-069)	Documentation	No impact to systems.
2	Update IC-GENC with Updates 8 and 9 of the GENC Ed3.0 (CR-2019-002, CR-2018-127)	CVEs	Data generation and ingestion systems need to be updated to handle the added GENC updates.
3	Added ISM.XML attributes to Schematron files to mark up the documentation. (CR-2017-301)	Schematron	No impact to systems.
4	Added schema PDF. (CR-2018-013)	Documentation	No impact to systems.
5	Updated CSV generation to include a column for deprecation date information. (CR-2018-080)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.
6	Updated Purpose section to be less XML centric. (CR-2019-004)	Documentation	No impact to systems.

B.5 - V2017-SEP Change Summary

Significant drivers for Version 2017-SEP include:

- Updating to be inline with the content of the GENC^[2] Edition 3 Update 7.

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

Table 13 - 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.6 - V2017-JUL Change Summary

Significant drivers for Version 2017-JUL include:

- Updating to be inline with the content of the GENC^[2] Edition 3 Updates 5 and 6.

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

Table 14 - 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.

#	Change	Artifacts changed	Compatibility Notes
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.7 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Updating to be inline with the content of the GENC^[2] Edition 3 Update 4 register.

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

Table 15 - Data Encoding Specification V2016-SEP Change Summary

#	Change	Artifacts Changed	Compatibility Notes
1	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.
2	Added CountryCode CVE that will serve as the source of currently correct values and names for country codes. (CR-2015-089)	CVEnum-GENCCountryCode.xml added	Data generation and ingestion systems need to be updated to handle the new CVE.
3	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.
4	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.
5	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.8 - 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 16 - Data Encoding Specification V2015-MAY Change Summary

#	Change	Artifacts Changed	Compatibility Notes
1	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
CES	Controlled Vocabulary Enumeration Encoding Specification
CSV	Comma Separated Value
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOMEX	Document and Media Exploitation
FIPS	Federal Information Processing Standards
GENC	Geopolitical Entities, Names, and Codes
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
URL	Uniform Resource Locator
URN	Uniform Resource Name
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D 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)*. . February 13, 2014.

Available online at: <https://www.niso.org/press-releases/2014/02/call-participation-niso-us-profile-standard-iso-3166-country-codes>

[2] GENC

Country Codes Working Group. *Geopolitical Entities, Names, and Codes*. 3.0.

Available online Intelink-TS at: <https://go.ic.gov/Tuxrlnu> (case sensitive – Tango uniform xray romeo India november uniform)

Available online at: <https://nsgreg.nga.mil/genc/discovery>

[3] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.

Available online Intelink-TS at: <https://go.ic.gov/tGXkwGO> (case sensitive – tango Golf Xray kilo whiskey Golf Oscar)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[4] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pNFyuVg> (case sensitive – papa November Foxtrot yankee uniform Victor golf)

Available online Intelink-U at: <https://w3id.org/ic/standards/IC-SF>

Available online at: <https://w3id.org/ic/standards/public>

[5] 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>

[6] 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

[7] 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>

[8] 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: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima)
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[9] 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: <https://go.ic.gov/FTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra)
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[10] ICPM 2007-200-2

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

[11] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.
Available online Intelink-TS at: <https://go.ic.gov/kh8NMVJ> (case sensitive – kilo hotel 8 November Mike Victor Juliet)
Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[12] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online Intelink-TS at: <https://go.ic.gov/0Agmenr> (case sensitive – 0 Alpha golf mike echo november romeo)
Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-21>

[13] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.
Available online Intelink-TS at: <https://go.ic.gov/qoNICy7> (case sensitive – quebec oscar November India Charlie yankee 7)
Available online Intelink-U at: <https://w3id.org/ic/standards/ISM>
Available online at: <https://w3id.org/ic/standards/public>

[14] 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

[15] Public_Law_80-242

Secretary of the Interior. *Public Law 242-80th Congress*. 1947-07-25.

Available online at: https://geonames.usgs.gov/docs/pubs/Public_Law_242.pdf

[16] Schematron

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

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/>

[17] 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 Director of National Intelligence (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@odni.gov.

Appendix F IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO 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 IC CIO staffing and coordination process leading to signature of the IC CIO Approval Memo. The signature date of the IC CIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the IC CIO 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 Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20^[11].