



# **Intelligence Community Technical Specification**

---

## **CVE Encoding Specification for Production Metrics**

**Version 2022-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 .....	1
1.4 - Conventions .....	2
1.4.1 - XML Namespaces .....	2
1.5 - Dependencies .....	2
1.5.1 - Specification Dependencies .....	2
1.5.2 - Inverse Dependencies .....	3
Chapter 2 - Development Guidance .....	5
2.1 - Additional Guidance .....	5
2.1.1 - Usage of the PM Schema .....	5
Chapter 3 - Constraints .....	6
3.1 - Data Validation Constraint Rules .....	6
3.1.1 - Purpose .....	6
3.1.2 - Value Enumeration Constraints .....	6
3.1.3 - Additional Constraints .....	6
3.1.3.1 - CES Constraints .....	6
3.1.4 - Constraint Rules .....	6
3.2 - Data Rendering Constraint Rules .....	7
3.2.1 - Purpose .....	7
3.2.2 - Rendering Constraint Rules .....	7
Appendix A - Feature Summary .....	8
A.1 - PM Feature Comparison .....	8
A.1.1 - Features from V2019-MAR to V2022-NOV .....	8
A.1.2 - Features from V2016-SEP to V2019-MAR .....	8
A.1.3 - Features from V2015-AUG to V2016-SEP .....	9
Appendix B - Change History .....	10
B.1 - 2022-NOV Change Summary .....	10
B.2 - 2022-MAY Change Summary .....	11
B.3 - 2020-OCT Change Summary .....	13
B.4 - 2019-MAR Change Summary .....	13
B.5 - 2017-SEP Change Summary .....	14
B.6 - 2017-MAY Change Summary .....	15
B.7 - 2016-SEP Change Summary .....	16
B.8 - 2015-NOV Change Summary .....	17
Appendix C - List of Abbreviations .....	20
Appendix D - Bibliography .....	21
Appendix E - Points of Contact .....	22
Appendix F - IC CIO Approval Memo .....	23

## List of Figures

Figure 1 - Related Specifications .....	3
Figure 2 - Inverse Dependency Specifications .....	4

## List of Tables

Table 1 - XML Namepaces .....	2
Table 2 - Dependencies .....	3
Table 3 - Constraint Rules .....	7
Table 4 - Feature Summary Legend .....	8
Table 5 - PM Feature Comparison V2019-MAR to V2022-NOV .....	8
Table 6 - PM Feature Comparison V2016-SEP to V2019-MAR .....	8
Table 7 - PM Feature Comparison V2015-AUG to V2016-SEP .....	9
Table 8 - Version Identifier History .....	10
Table 9 - Data Encoding Specification 2022-NOV Change Summary .....	11
Table 10 - Data Encoding Specification 2022-MAY Change Summary .....	12
Table 11 - Data Encoding Specification 2020-OCT Change Summary .....	13
Table 12 - Data Encoding Specification 2019-MAR Change Summary .....	14
Table 13 - Data Encoding Specification 2017-SEP Change Summary .....	15
Table 14 - Data Encoding Specification 2017-MAY Change Summary .....	15
Table 15 - Data Encoding Specification 2016-SEP Change Summary .....	16
Table 16 - Data Encoding Specification 2015-NOV Change Summary .....	18

## Chapter 1 - Introduction

### 1.1 - Purpose

This *CVE Encoding Specification for Production Metrics* (PM.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 PM.CES controlled vocabulary. Production Metrics is a list of metadata values that contain subjects, actors, and locations addressed in Intelligence Community (IC) documents. The Production Metrics subjects, actors, and locations are used to compute metrics on a collection of IC documents. This Controlled Vocabulary Enumeration Encoding Specification (CES) defines the CES elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing data concepts using a variety of formats.

### 1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML<sup>[2]</sup>) 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.

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 the Production Metrics related CVEs including Subjects, Actors, and Locations. While PM values are not directly used for Access Control, the PM values are aggregated into the Mission Need Profile (MN) Issue CVE, and a mapping of PM values to MN Issue values is provided in the *Taxonomy Encoding Specification for Mission-Need Taxonomy* (MNT.XML<sup>[6]</sup>).

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

- 500 Series:
  - Intelligence Community Directive (ICD) 500, *Director Of National Intelligence Chief Information Officer*<sup>[3]</sup>

- ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* [\[4\]](#)
- Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [\[5\]](#)

## 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 [\[2\]](#).

### 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
pm	urn:us:gov:ic:pm
xsd	<a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a>

## 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 [\[2\]](#).

### 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+[2])	This specification does not depend on a specific version of IC-SF.XML[2]; 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.
Value enumerations used for several XML structures are defined in the various CVEs included in this Data Encoding Specification (DES).	Specification uses CVEs to encode controlled vocabularies. The use of the PM CVEs is normative.

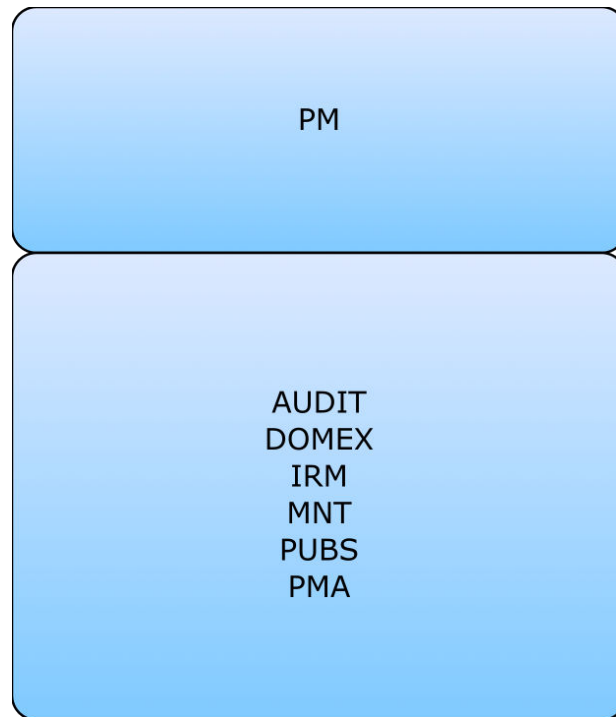
**Figure 1 : Related Specifications**

## 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

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML<sup>[2]</sup> framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

### 2.1 - 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.

There are two ways in which a consumer requiring a PM can use the PM.CES specification: through referencing objects defined in the schema or enforcing the format via running their own Schematron.

#### 2.1.1 - Usage of the PM Schema

The PM.CES schema defines elements (`pm:ProductionMetricsSubject`, `pm:ProductionMetricsActor`, `pm:ProductionMetricsLocation`) and attributes (`@pm:productionMetricsSubject`, `@pm:productionMetricsActor`, `@pm:productionMetricsLocation`) that enforce the allowable values as defined in the specification’s CVE (see [Section 3.1.2 - Value Enumeration Constraints](#) for more details). Consumers of the PM.CES specification should import the PM schema and reference the element or attribute, depending on what is needed. Note: the names for the element and the attribute are similar because the content is the same, i.e., both limit the value to the PM CVE, but the expectation on usage is that the consumer would use one or the other. The difference in capitalization is because they follow the IC naming standards, which requires the first letter for elements to be uppercase and the first letter for attributes to be lower case.

## Chapter 3 - Constraints

### 3.1 - Data Validation Constraint Rules

#### 3.1.1 - Purpose

The PM.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which CES 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.

#### 3.1.2 - Value Enumeration Constraints

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

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

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

#### 3.1.3 - Additional Constraints

##### 3.1.3.1 - CES Constraints

The CES version is specified through attributes on the root element. The schema constrains the values of these attributes. 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.

#### 3.1.4 - Constraint Rules

The detailed constraint rules for the PM.CES schema can be found in a separate document inside the Documents/PM directory, in the "PM\_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 "PM\_Rules.pdf" file.

## 3.2 - Data Rendering Constraint Rules

### 3.2.1 - Purpose

Rendering rules define constraints on the rendering and display of PM.CES documents. The intent is to inform the development of systems capable of rendering or displaying PM.CES data for use by individuals not familiar with the details of the PM.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.

### 3.2.2 - Rendering Constraint Rules

The following table contains the information for the PM.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 this CES.

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. PM Feature Comparison

A.1.1. Features from V2019-MAR to V2022-NOV

Table 5 - PM Feature Comparison V2019-MAR to V2022-NOV

Required date	Feature	V2019-MAR	V2020-OCT	V2022-MAY	V2022-NOV
	Aligns with Subjects mapping from DDII as of 2019-11-01	N	F	F	F
	Aligns with Actors, Subjects, Locations mapping from DDII as of 2022-03-25	N	N	F	F
	Aligns with Subjects mapping from DDII as of 2022-10-27	N	N	N	F

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

Table 6 - PM Feature Comparison V2016-SEP to V2019-MAR

Required date	Feature	V2016-SEP	V2017-MAY	V2017-SEP	V2019-MAR
	PM Coverage CVE Updated and includes: <ul style="list-style-type: none"><li>Enhanced Coverage based on DDII inputs as of 2017-08 to include<ul style="list-style-type: none"><li>New Non-state entities (NSE) and terrorist entities</li><li>Deprecation of existing NSE values</li><li>Modification of existing NSE descriptions</li></ul></li></ul>	N	N	F	F
	Aligns with Subjects mapping from DDII as of 2018-08-07	N	N	N	F
	Support for Production Metric Triples using Actor, Subject, and Location.	N	N	N	F

A.1.3. Features from V2015-AUG to V2016-SEP

Table 7 - PM Feature Comparison V2015-AUG to V2016-SEP

Required date	Feature	V2015-AUG	V2015-NOV	V2016-SEP
	PM Coverage CVE Added and includes: <ul style="list-style-type: none"><li>Countries sourced from IC-GENC.CES<sup>[1]</sup> instead of ISO-3166</li><li>Enhanced Coverage based on DDII inputs as of 2015-08 to include<ul style="list-style-type: none"><li>New Non-state entities (NSE) and terrorist entities</li><li>Deletion of existing NSE values</li><li>Modification of existing NSE descriptions</li></ul></li></ul>	N	F	F

## Appendix B Change History

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

**Table 8 - Version Identifier History**

Version	Date	Purpose
2015-AUG	August 13, 2015	Initial Release
2015-NOV	November 16, 2015	Routine revision to technical specification. For details of changes, see <a href="#">Section B.8 - 2015-NOV Change Summary</a>
2016-SEP	September, 9, 2016	Routine revision to technical specification. For details of changes, see <a href="#">Section B.7 - 2016-SEP Change Summary</a>
2017-MAY	May 22, 2017	Routine revision to technical specification. For details of changes, see <a href="#">Section B.6 - 2017-MAY Change Summary</a>
2017-SEP	September 29, 2017	Routine revision to technical specification. For details of changes, see <a href="#">Section B.5 - 2017-SEP Change Summary</a>
2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see <a href="#">Section B.4 - 2019-MAR Change Summary</a>
2020-OCT	October 1, 2020	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - 2020-OCT Change Summary</a>
2022-MAY	May 13, 2022	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - 2022-MAY Change Summary</a>
2022-NOV	November 29, 2022	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - 2022-NOV Change Summary</a>

### B.1 - 2022-NOV Change Summary

Significant drivers for Version 2022-NOV include:

- DDII updates to values as of 2022-10-27

The following table summarizes the changes made to 2022-MAY in developing 2022-NOV.

**Table 9 - Data Encoding Specification 2022-NOV Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Updated values based on DDII information for PM CVEs. (CR-2022-040) <ul style="list-style-type: none"><li>• CVEEnumPMSubject</li></ul> Updated Description TERR.	Documentation CVE CVEEnumPMSubject.xml updated	Systems may need to be updated to handle new values.

## **B.2 - 2022-MAY Change Summary**

Significant drivers for Version 2022-MAY include:

- DDII updates to values as of 2022-05-01

The following table summarizes the changes made to 2020-OCT in developing 2022-MAY.



**Table 10 - Data Encoding Specification 2022-MAY Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	<p>Updated values based on DDII information for PM CVEs. (CR-2019-170,CR-2021-019)</p> <ul style="list-style-type: none"> <li>CVEnumPMActor <p>Updated to use GENC country short name instead of full name.</p> <p>See CVEnum-PMNonStateActors description for non-state actor changes.</p> <p>Update NotAvail to 100322 Unidentified Actor</p> <p>Deleted WWW</p> </li> <li>CVEnumPMLocation <p>Updated to use GENC country short name instead of full name.</p> </li> <li>CVEnumPMNonStateActors <p>Added 100002, 100003, 100004 , 100007, 100012, 100014, 100025, 100026, 100039, 100040, and 90 consecutive values from 100233 to 100322.</p> <p>Updated description 100012, 100039, 100060, 100070, 100075, 100076, 100136</p> </li> <li>CVEnumPMSubject <p>Deleted NotAvail.</p> <p>Deprecated ACTM, ENRF, ESEC, HAPR, HREL, HRWC, SRCC.</p> </li> </ul>	<p>Documentation</p> <p>CVE</p> <p>CVEnumPMActor.xml updated</p> <p>CVEnumPMLocation.xml updated</p> <p>CVEnum-PMNonStateActors.xml updated</p> <p>CVEnumPMSubject.xml updated</p>	<p>Systems may need to be updated to handle new values.</p>

#	Change	Artifacts Changed	Compatibility Notes
	Added CHTC, CNRE, POWS(deprecated), STCM, WDPR.  Updated Description CRIM, DEPS, ECON, ENRF, FINT, FMCC, FPLD, HAPR, HLTH, INFR, TFIN, WMDN, WPNS.		

### B.3 - 2020-OCT Change Summary

Significant drivers for Version 2020-OCT include:

- DDII updates to values as of 2019-11-01

The following table summarizes the changes made to 2019-MAR in developing 2020-OCT.

**Table 11 - Data Encoding Specification 2020-OCT Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Updated values based on DDII information. Added new tokens FINT, CBWD, WPNS. Deprecated existing tokens ACWP, WMDB, WMDC, WMDM. Updated description DEMG, ENRF, FMCC, FPLD, HAPR, HREL, WMDN (CR-2019-169)	CVE  CVEnumPMSubject.xml updated	Systems may need to be updated to handle new values.
2	Updated 2016-SEP change log to align with public release. (CR-2019-177)	Documentation	No impact to systems.
3	Update schema guide implementation notes with root node. (CR-2019-125)	Schema	No impact to systems.
4	Update description for FPLD in PM Subject CVE. (CR-2020-037)	CVE  CVEnumPMSubject.xml updated	No impact to systems.

### B.4 - 2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- DDII updates to values as of 2018-08-07

The following table summarizes the changes made to 2017-SEP in developing 2019-MAR.

**Table 12 - Data Encoding Specification 2019-MAR Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Created PM Location CVE. (CR-2016-033)	CVE  CVEEnumPMLocation.xml added  Schema	Systems may need to be updated to handle new values.
2	Updated CESVersion attribute to generic regex in the schema and created schematron rule to check current CESVersion (CR-2018-092)	Schema  Schematron  PM-ID-00001 added	Data generation and ingestion systems need to be updated to accommodate the changes.
3	Updated CSV generation to include a column for deprecation date information. (CR-2018-088)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.
4	Added schema PDF. (CR-2018-025)	Documentation	No impact to systems.
5	Updated Production Metrics Subjects CVE with the latest published material from the DD/II website. Added support for Production Metric Triples using Actor, Subject, and Location. (CR-2017-267)	CVE  CVEEnumPMSubject.xml updated  Schema updated	Systems may need to be updated to handle new values.
6	Updated documentation to use the specification framework. (CR-2018-126)	Documentation	No impact to systems.
7	Fix validity of JSON-LD CVEs. (CR-2018-144)	CVE	Data generation and ingestion systems using JSON need to be updated to accommodate the changes.
8	Updated Purpose section to be less XML centric. (CR-2019-004)	Documentation	No impact to systems.

## B.5 - 2017-SEP Change Summary

Significant drivers for Version 2017-SEP include:

- DDII updates to values as of 2017-08-02.

The following table summarizes the changes made to 2016-SEP in developing 2017-SEP.

**Table 13 - Data Encoding Specification 2017-SEP Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Create RelaxNG CVE Fragments for PM. (CR-2017-184)	CVEs	No impact to systems.
2	Create JSON version of CVEs in PM (CR-2017-065)	CVEs	No impact to systems.
3	Create CSV version of CVEs in PM (CR-2017-043)	CVEs	No impact to systems.
4	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-254)	Documentation	No impact to systems.
5	Added Non-State Entities: 100231, 100232  Deprecated: 100192, 100224  Updated 100228: fixed spelling error. Updated 100163: fixed spelling error. Updated 100144: add acronym. Updated 100231: corrected name.  (CR-2017-205),(CR-2017-206)	CVE  CVEnum-PMNonStateActors	Systems may need to be updated to handle new/updated values.
6	Added definitions for Dependencies and Inverse Dependencies. (CR-2017-277)	Documentation	No impact to systems.

## B.6 - 2017-MAY Change Summary

Significant drivers for Version 2017-MAY include:

- DDII updates to values as of 2017-05-18.

The following table summarizes the changes made to 2016-SEP in developing 2017-MAY.

**Table 14 - Data Encoding Specification 2017-MAY Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Updated values based on DDII information. (CR-2017-019)	CVE  CVEnumPMCoverage  CVEnum-PMNonStateActors  CVEnumPMSubject	Systems may need to be updated to handle new/updated values.

#	Change	Artifacts Changed	Compatibility Notes
2	Added inverse dependency section along with hard and soft inverse dependency descriptions. (CR-2017-122)	DES	No impact to systems.

## B.7 - 2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- DDII updates to values.

The following table summarizes the changes made to 2015-NOV in developing 2016-SEP.

**Table 15 - Data Encoding Specification 2016-SEP Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Updated (POWS) (HAPR). (CR-2015-108)	CVE CVerenumPMSubject	Systems may need to be updated to handle new/updated values.
2	IC-GENC countries had codespace updates.  Added non-state entities (NSE) 100203, 100204, 100205  Deprecated NSE 100010, 100023, 100035, 100078, 100084, 100098, 100100, 100145, 100147, 100153, 100161, 100190  Replaced 100078 with 100112  Replaced 100084 and 100147 with 100120  Updated 100107  Updated 100150  Updated 100136 (CR-2016-042)	CVE CVerenumPMCoverage CVerenum-PMNonStateActors	Systems may need to be updated to handle new/updated values.

#	Change	Artifacts Changed	Compatibility Notes
3	The schema change logs will no longer be maintained as of the 2016-SEP release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2016-SEP, reference the change history in the CES.	Schema	No impact to systems.
4	Removed schematron. There was only an abstract pattern and the Common Metadata Standards Tiger Team (CMSTT) has decided that abstract patterns should not be referenced across specifications. (CR-2015-020)	Schematron	Systems that used the abstract pattern will have to implement in their own specification.
5	Updated with element and attribute groups.	Schema	No impact to systems.
6	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 - 2015-NOV Change Summary

Significant drivers for Version 2015-NOV include:

- DDII desires for more granular markings.

The following table summarizes the changes made to v2015-AUG in developing 2015-NOV.

**Table 16 - Data Encoding Specification 2015-NOV Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Created PM Coverage CVE.	<p>CVE</p> <p>CVEnum-PMCoverage.xml added.</p> <p>CVEnum-PMNonStateActors.xml added (subset of PM Coverage CVE).</p> <p>Countries based on IC-GENC instead of ISO-3166 used in IRM Coverage CVE</p> <p>156 new Non-state entities (NSE) and terrorist entities added to PM Coverage CVE`</p> <p>Existing NSE 100042 "West Bank and Gaza Strip" removed given "West Bank" and Gaza Strip" existing as countries in IC-GENC so their NSE token is a IC-GENC trigraph where as other NSEs use the 6 digit numeric.</p> <p>Existing NSE 100027 "Narcotics Kingpin Organizations" is being deleted and replaced by the new NSE 100057 "CPOT\Kingpin Organizations"</p> <p>The following existing NSE values have been removed (100002, 100003, 100004, 100007, 100012, 100014, 100015, 100016, 100018, 100025, 100026,</p>	Systems may need to be updated to handle new/updated values.

#	Change	Artifacts Changed	Compatibility Notes
		100037, 100039, 100040)  The following existing NSE values had description updates (100005, 100006, 100008, 100009, 100020, 100028, 100029, 100030, 100031, 100032, 100033, 100034, 100043)	



## Appendix C List of Abbreviations

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

CES	Controlled Vocabulary Enumeration Encoding Specification
CMSTT	Common Metadata Standards Tiger Team
CSV	Comma Separated Value
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICS	Intelligence Community Standard
JSON	JavaScript Object Notation
MN	Mission Need Profile
XML	Extensible Markup Language

## Appendix D Bibliography

### [1] IC-GENC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Geopolitical Entities, Names, and Codes (IC-GENC.CES)*.

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

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

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

### [2] 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/pNFyVg> (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>

### [3] 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](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)

### [4] 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](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)

### [5] 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>

### [6] MNT.XML

Office of the Director of National Intelligence. *Taxonomy Encoding Specification for Mission-Need Taxonomy (MNT.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/e6MOkMT> (case sensitive – echo 6 Mike Oscar kilo Mike Tango )

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

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

## 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](mailto: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<sup>[5]</sup>.