



Intelligence Community Technical Specification

XML Data Encoding Specifications for Production Metrics Assertion

Version 2019-MARr2019-SEP

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	1
1.4.1 - XML Namespaces	2
1.5 - Dependencies	2
1.5.1 - Specification Dependencies	2
1.5.2 - Inverse Dependencies	4
Chapter 2 - Development Guidance	6
2.1 - Understanding Production Metrics Assertion	6
2.2 - Production Metrics Assertion Usage	6
Chapter 3 - Constraints	7
3.1 - Data Validation Constraint Rules	7
3.1.1 - Purpose	7
3.1.2 - Value Enumeration Constraints	7
3.1.3 - Additional Constraints	7
3.1.3.1 - DES Constraints	7
3.1.4 - Constraint Rules	7
3.2 - Data Rendering Constraint Rules	8
3.2.1 - Purpose	8
3.2.2 - Rendering Constraint Rules	8
Appendix A - Feature Summary	9
A.1 - PMA Feature Summary	9
Appendix B - Change History	10
B.1 - 2019-MARr2019-SEP Change Summary	10
B.2 - 2019-MAR Change Summary	10
Appendix C - List of Abbreviations	12
Appendix D - Bibliography	13
Appendix E - Points of Contact	15
Appendix F - IC CIO Approval Memo	16

List of Figures

Figure 1 - Related Specifications	4
---	---

List of Tables

Table 1 - XML Namepaces	2
Table 2 - Dependencies	3
Table 3 - Constraint Rules	8
Table 4 - Feature Summary Legend	9
Table 5 - PMA Feature Comparison	9
Table 6 - DES Version Identifier History	10
Table 7 - Data Encoding Specification 2019-MARr2019-SEP Change Summary	10
Table 8 - Data Encoding Specification 2019-MAR Change Summary	11

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Production Metrics Assertion* (PMA.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode PMA data. This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing PMA data assertion concepts using XML within the use of a Trusted Data Format (TDF) Object or Collection.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[1]) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (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 DES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the DES should be closely scrutinized and differences separately documented and assessed for applicability.

1.3 - Enterprise Need

This DES is designed to fulfill a number of requirements in support of the transformational efforts of the IC. These requirements include:

- Capturing one or more Production Metrics where each of them captures the Actor (who), Subject (what), and optional Location (where) to provide intelligence producers the ability to more accurately track funding for DDII intelligence gathering.
- Capturing one or more Production Metrics where each of them captures the Actor (who), Subject (what), and optional Location (where) to enable intelligence producers to mark data in a way that improves DDII's ability to measure collected information.

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*^[3]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC*^[4]
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance*^[6]

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^[1].

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
pma	urn:us:gov:ic:pma
tdf	urn:us:gov:ic:tdf

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^[1].

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.

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All IC CIO specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ ^[7])	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[7] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[5] . Per ICD-710, all security markings MUST be updated within 365 days of a release of the Register and Manual. As of this release, the latest version of ISM.XML is 2021-NOVr2022-NOV which is based on the Register and Manual released in August, 2019.
<i>XML Data Encoding Specification for Trusted Data Format</i> (IC-TDF.XML.V2019-MAR+ ^[2])	PMA.XML elements as well as its dependent specifications are used in conjunction with IC-TDF.XML ^[2] objects as structured assertions or content that compose the necessary material represented by PMA.XML. The dependence of PMA.XML on IC-TDF is normative. This specification does not depend on a specific version of IC-TDF.XML; IC-TDF.XML versions later than version 2019-MAR MAY be used. The minimum version was based on a technical dependency.
<i>CVE Encoding Specification for Production Metrics</i> (PM.CES.2019-MAR+ ^[8])	The specification does not depend on a specific version of PM.CES ^[8] ; versions later than version 2019-MAR MAY be used. The minimum version was based on authoritative source compliance; DDII guidance.
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[1])	This specification does not depend on a specific version of IC-SF.XML ^[1] ; 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
<p>Transformations (XSLT) 2.0^[10] implementation of Schematron^[9] 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>
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumeration (CVE) included in this DES.	Specification uses CVEs to encode controlled vocabularies.

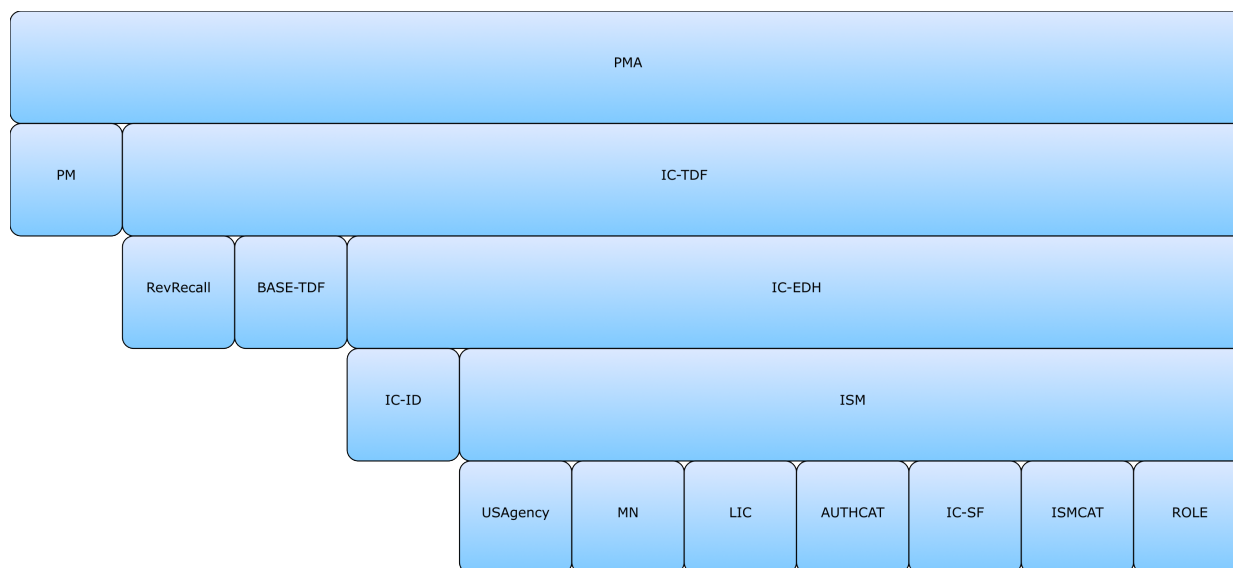


Figure 1 : Related Specifications

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).

This specification is not used by other specifications released by the IC CIO, and therefore does not contain an Inverse Dependency Diagram.

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^[1] 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 - Understanding Production Metrics Assertion

Consistent, structured production metrics assertion information can help track funding for DDII intelligence gathering. A production metrics assertion enables intelligence data producers to mark data in way that allows DDII as a consumer to measure performance.

The encoding of a production metrics assertion is made up of one component:

- A **@pma:ProductionMetricsAssertion** which contains one or more **@pma:ProductionMetric** elements where each of the elements captures the Actor (who), Subject (what), and optional Location (where) of the intelligence information. Information in the **@pma:ProductionMetricsAssertion** enables consumers to measure the performance of intelligence gathering activities.

2.2 - Production Metrics Assertion Usage

PMA.XML is used in conjunction with *XML Data Encoding Specification for Trusted Data Format* (IC-TDF.XML^[2]) objects as structured assertions. A Trusted Data Object (TDO) or a Trusted Data Collection (TDC) conforms to PMA.XML when it contains:

- A structured assertion with an **@pma:ProductionMetricsAssertion** element

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

3.1.1 - Purpose

The PMA.XML schema defines the data elements, attributes, cardinalities and parent-child relationships for which XML instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified in applicable IC policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints. For more information, please see the “Data Validation Constraint Rules” chapter in the IC-SF.XML^[1] framework document.

3.1.2 - Value Enumeration Constraints

Several elements and attributes of the PMA.XML 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 - DES Constraints

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

3.1.4 - Constraint Rules

The detailed constraint rules for the PMA.XML schema can be found in a separate document inside the Documents/PMA directory, in the “PMA_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 “PMA_Rules.pdf” file.

3.2 - Data Rendering Constraint Rules

3.2.1 - Purpose

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

3.2.2 - Rendering Constraint Rules

The following table contains the information for the PMA.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.			

Appendix A Feature Summary

The following tables summarize major features by version for PMA.XML.

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)
Cell Colors represent the same information as the Key value	

A.1. PMA Feature Summary

Table 5 - PMA Feature Comparison

Required date	Feature	V2019-MAR	V2019-MARr2019-SEP
March 8, 2019	Defines the allowable values for Production Metrics Assertion	F	F

Appendix B Change History

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

Table 6 - DES Version Identifier History

Version	Date	Purpose
2019-MAR	March 8, 2019	Initial Release. For details of changes, see Section B.2 - 2019-MAR Change Summary
2019-MARr2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see Section B.1 - 2019-MARr2019-SEP Change Summary

B.1 - 2019-MARr2019-SEP Change Summary

Significant drivers for Revision 2019-MARr2019-SEP include:

- Community Change Requests

[Table 7](#) summarizes the changes made to this technical specification from Version 2019-MAR to Revision 2019-MARr2019-SEP.

Table 7 - Data Encoding Specification 2019-MARr2019-SEP Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Added pm:CESVersion to the PMARootNodeAttributeGroup attribute. (CR-2019-109)	Schema	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Fixed a typo in Section 3.1.2. (CR-2019-051)	Documentation	No impact to systems.
3	Add schematron rule id for rules that use ValidateValidationEnvCVE and ValidateValidationEnvSchema (CR-2019-087)	Schematron	No impact to systems.

B.2 - 2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- Creation of PMA.XML specification.

The following table summarizes the changes in 2019-MAR.

Table 8 - Data Encoding Specification 2019-MAR Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Creation of PMA.XML specification. (CR-2016-034, CR-2018-102)	Documentation Schema Examples Schematron	Data generation and ingestion systems need to be updated to support the latest version of the schema.

Appendix C List of Abbreviations

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

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
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

[1] 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>

[2] IC-TDF.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/hdwc8fn> (case sensitive – hotel delta whiskey charlie 8 foxtrot november)

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

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

[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

[5] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.

Available online Intelink-TS at: <https://go.ic.gov/oSj9K7O> (case sensitive – oscar Sierra juliet 9 Kilo 7 Oscar)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[6] 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>

[7] 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>

[8] PM.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Production Metrics (PM.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/7djZXmA> (case sensitive – 7 delta juliet Zulu Xray mike Alpha)

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

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

[9] 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/>

[10] 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^[6].