



Intelligence Community Technical Specification

CVE Encoding Specification for Media Type

Version 2020-OCT

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	5
Chapter 2 - Development Guidance	6
2.1 - Relationship to Abstract Data Definition and other encodings	6
2.2 - List Sources	6
2.3 - Additional Guidance	6
2.3.1 - Usage of the MIME Schema	6
2.3.2 - Usage of the MIME Schematron Library	7
2.3.3 - Deprecated MIME types	7
Chapter 3 - Constraints	8
3.1 - “Living” Constraint Rules	8
3.2 - Data Validation Constraint Rules	8
3.2.1 - Value Enumeration Constraints	8
3.2.2 - Additional Constraints	8
3.2.2.1 - DES Constraints	8
3.2.3 - Constraint Rules	8
3.3 - Data Rendering Constraint Rules	9
3.3.1 - Purpose	9
3.3.2 - Rendering Constraint Rules	9
Appendix A - Feature Summary	10
A.1 - MIME Feature Comparison	10
Appendix B - Change History	11
B.1 - V2020-OCT Change Summary	11
Appendix C - List of Abbreviations	13
Appendix D - Bibliography	14
Appendix E - Points of Contact	16
Appendix F - IC CIO Approval Memo	17

List of Figures

Figure 1 - Related Specifications 4

Figure 2 - Inverse Dependency Specifications 5

List of Tables

Table 1 - XML Namepaces	2
Table 2 - Dependencies	3
Table 3 - Constraint Rules	9
Table 4 - Feature Summary Legend	10
Table 5 - MIME.CES Feature comparison	10
Table 6 - CES Version Identifier History	11
Table 7 - Data Encoding Specification 2020-OCT Change Summary	11

Chapter 1 - Introduction

1.1 - Purpose

This *CVE Encoding Specification for Media Type* (MIME.CES) defines a controlled vocabulary for media types used by the Intelligence Community (IC). This Controlled Vocabulary Enumeration Encoding Specification (CES) provides tokens for both IC-defined media types and general media types defined by the Internet Assigned Numbers Authority (IANA). Though the title refers to media types, this specification retains the abbreviation “MIME” as a generally-known term for media types even though the use is not limited to email and “MIME” is no longer used by IANA; the IANA specification is now known as “Media Type”. This specification applies generally to media types; it is NOT limited to use for mail extensions.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[3]) 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 applies to the use of media types in information produced, stored, or shared within the IC. This CES may be useful outside the scope of intelligence, but potential adopters should independently assess the CES appropriateness for any particular purpose.

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 that defines 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.

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

- 300 Series:
 - Intelligence Community Directive (ICD) 302, *Document and Media Exploitation* ^[4]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[5]
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* ^[6]
 - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[7]

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^[3].

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 Extensible Markup Language (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
mime	urn:us:gov:ic:mime
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^[3].

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>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[3])	This specification does not depend on a specific version of IC-SF.XML ^[3] ; 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.
Schematron ^[10]	<p>Schematron — International Organization for Standardization (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^[11] query binding.</p>

Name	Dependency Description
<p>XSLT 2.0^[11] implementation of Schematron^[10] 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 CVEs included in this CES.	Specification uses CVEs to encode controlled vocabularies. The use of the MIME CVEs is normative.
IANA Website ^[1]	Contains the IANA approved media types which are a significant subset of this CVE.



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 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](#).

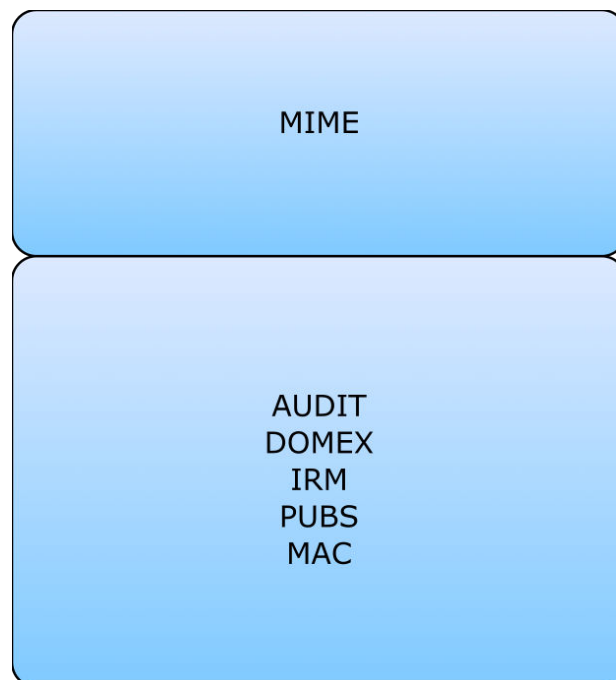


Figure 2 : Inverse Dependency Specifications

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 - List Sources

The media types included in this specification were obtained from:

- IANA website (<http://www.iana.org/assignments/media-types/media-types.xhtml>)
- The current IC-specific media types are defined in the *Community Shared Resources Technical Specification Profiles* data encoding specification
- The legacy media types that existed in *XML Data Encoding Specification for Intelligence Publications* (PUBS.XML^[9]) or *XML Data Encoding Specification for Information Resource Metadata* (IRM.XML^[8]) prior to the creation of MIME.CES are the final source of values.

Each of the above sources are provided as a separate CVE to facilitate review and understanding of the source for each value. The union of all 3 sources is the final CVE that is anticipated to be the one used by most consumers of this specification.

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.

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

2.3.1 - Usage of the MIME Schema

The MIME.CES schema defines an element (**mime:MIMETYPE**) and an attribute (**@mime:mimetype**) that enforces the allowable values as defined in the specification's CVE (see

[Section 3.2.1 - Value Enumeration Constraints](#) for more details). Consumers of the MIME.CES specification should import the MIME 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 MIME 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 of elements to be uppercase and the first letter of attributes to be lower case.

2.3.2 - Usage of the MIME Schematron Library

The MIME.CES Schematron library contains an abstract rule that enforces the allowable values as defined in the specification's CVE (see [Section 3.2.1 - Value Enumeration Constraints](#) for more details). Consumers of the MIME.CES specification should include the abstract rule and define an implementation for it. This allows for the consumer to define the context that triggers the rule and the value that should be matched against the MIME CVE.

Note that consumers of the MIME.CES Schematron library also need to import the MIME schema within their schema. The importing schema needs to reference the CES version for MIME in order to let systems reviewing the data know what Schematron library to import.

2.3.3 - Deprecated MIME types

The deprecated MIME types are marked with a `@deprecated` attribute. The date noted in the attribute is not the actual date of deprecation but the release date of the specification. The MIME schematron rules provides a warning message based on the existence of the `@deprecated` attribute and does not depend on the release date.

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. 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 MIME.CES schema defines the data elements, attributes, cardinalities and parent-child relationships with 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.

3.2.1 - Value Enumeration Constraints

The purpose of the MIME.CES specification is to define the CVE for allowable media types.

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 - DES Constraints

The Data Encoding Specification (DES) or CES version is specified through attributes on the root element. The schema constrains the values of these attributes. The DES or CES version attribute enables systems probing 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 MIME.CES schema can be found in a separate document inside the Documents/MIME directory, in the “MIME_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 “MIME_Rules.pdf” file as well.

3.3 - Data Rendering Constraint Rules

3.3.1 - Purpose

Rendering rules define constraints on the rendering and display of MIME.CES documents. The intent is to inform the development of systems capable of rendering or displaying MIME.CES data for use by individuals not familiar with the details of the MIME.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 MIME.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 tables summarize major features by version for MIME.CES. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g. The IC Marking System Register and Manual^[2] has an implementation date of one year after issuance).

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. MIME Feature Comparison

Table 5 - MIME.CES Feature comparison

Required date	Feature	V2016-SEP	V2020-OCT
	Defines the allowable values for media types	F	F
	Support for Mime Type video/webm	N	F

Appendix B Change History

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

Table 6 - CES Version Identifier History

Version	Date	Purpose
2016-SEP	September 9, 2016	Initial Release per CR-2015-048
2020-OCT	October 1, 2020	Routine revision to technical specification. For details of changes, see Section B.1 - V2020-OCT Change Summary

B.1 - V2020-OCT Change Summary

Significant drivers for version 2020-OCT include:

- Updates to MIME types.

[Table 7](#) summarizes the changes made to this technical specification from version 2016-SEP to version 2020-OCT.

Table 7 - Data Encoding Specification 2020-OCT Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Update schema guide implementation notes with root node. (CR-2019-111)	Schema	No impact to systems.
2	Updated documentation to use the specification framework. (CR-2019-036)	Documentation	No impact to systems.
3	Remove XML from CES Titles. (CR-2019-047)	Documentation	No impact to systems.
4	Update Schematron rules to have ISM attributes. (CR-2017-310)	Schematron	No impact to systems.
5	Add @id and @role to schematron rules. (CR-2017-227)	Schematron	No impact to existing systems. Additional capabilities.
6	Update Schematron rule to be warnings instead of errors for deprecated MIME types. (CR-2020-017)	Schematron MIME-ID-00001 modified	Systems need to be updated to accommodate this change.
7	Add PDF of Schema Files. (CR-2018-022)	Schema PDFs	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
8	Create RELAX NG forms of CVEs. (CR-2017-181)	CVEs	No impact to systems.
9	Create JSON version of CVEs. (CR-2017-062)	CVEs	No impact to systems.
10	Create CSV version of CVEs. (CR-2017-040, CR-2018-086)	CVEs	No impact to systems.
11	Support change to MIME specification to allow additional values through media type regex. (CR-2019-053)	CVEnumMIMEType Schematron MIME-ID-00002 added	Systems need to be updated to accommodate this change.
12	Add rule to enforce CESVersion. (CR-2017-089, CR-2020-009)	Schematron MIME-ID-00003 added	Systems need to be updated to accommodate this change.

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
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
IANA	Internet Assigned Numbers Authority
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
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

[1] IANA

Internet Assigned Numbers Authority. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.

Media Types (MIME) available online at: <http://www.iana.org/assignments/media-types/media-types.xhtml>

IANA HomePage available online at: <http://www.iana.org>

[2] 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>

[3] 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>

[4] ICD 302

Office of the Director of National Intelligence. *Document and Media Exploitation*. Intelligence Community Directive 302. 6 July 2007.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_302.pdf

[5] 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

[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] 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>

[8] IRM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Resource Metadata (IRM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pOKLbmx> (case sensitive – papa Oscar Kilo Lima bravo mike xray)

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

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

[9] PUBS.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Intelligence Publications (PUBS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/u6bb18P> (case sensitive – uniform 6 bravo bravo 1 8 Papa)

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

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

[10] 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/>

[11] 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].