Intelligence Community Technical Specification

XML Data Encoding Specifications for Intelligence Community Identifier

Version 2021-NOV

December 1, 2022

This document has been approved for Public Release by the Office of the Director of National Intelligence. See Distribution Notice for details.

Distribution Notice:

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

Table of Contents

List of Figures

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Intelligence Community Identifier* (IC-ID.XML) defines detailed implementation guidance for textual identifiers to be used with a variety of text-based encodings and defines how to incorporate those identifiers into Extensible Markup Language (XML) structures.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML[4]) 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 Data Encoding Specification (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

Information sharing within the national intelligence enterprise will increasingly rely on unique identifiers in shared intelligence. A structured, verifiable representation of unique identifiers to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions being performed by human beings today.

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* [6]
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* [7]
  - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [8]
- DoD Issuances:
  - Department of Defense Instruction Number 8320.03, *Unique Identification (UID) Standards for Supporting the DoD Information Enterprise* [2]

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 Namepaces

Prefix	URI
icid	urn:us:gov:ic:id

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.

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
Intelligence Community Specification Framework (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
Augmented Backus-Naur Form (ABNF), *Augmented BNF for Syntax Specifications: ABNF* [1] defined by Internet Standard 68 also known as Request for Comments (RFC) 5234.	The text specification uses ABNF to define the format of the IC Identifier text string. Conformance to the structure defined with ABNF is normative, whereas use of ABNF to encode them is informative.
Schematron[12]	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. The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. Note: The Schematron rules in this specification use Transformations (XSLT) 2.0[14] query binding.
XSLT 2.0[14] implementation of Schematron[12] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the *behavior* of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

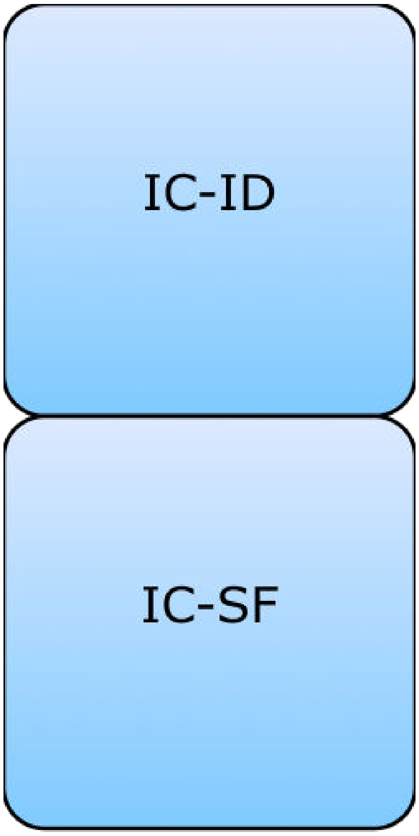

Figure 1 : Related Specifications

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.

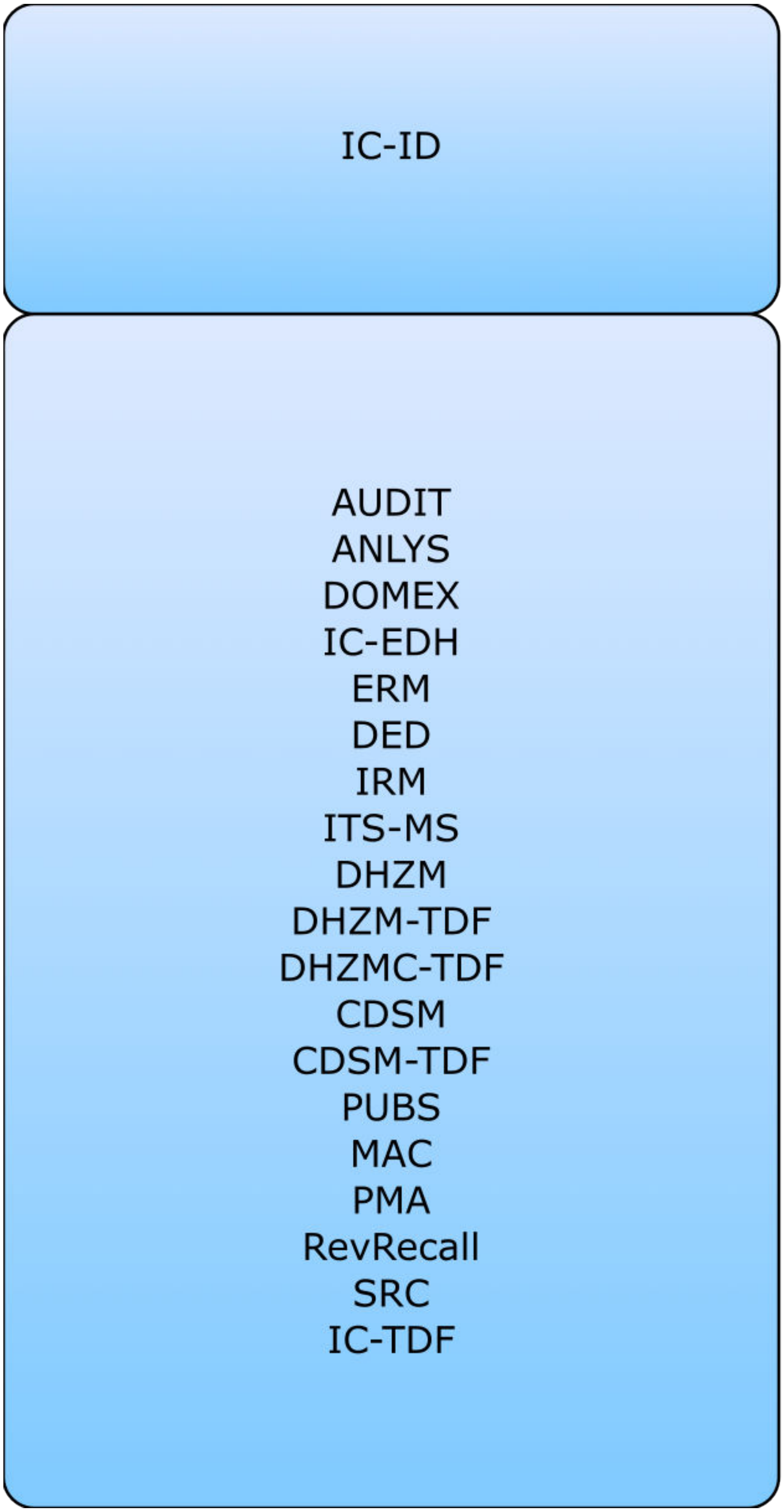

Figure 2 : Inverse Dependency Specifications

1.6 - Conformance

The ABNF rules used to specify the format of an IC-ID are normative, the corresponding textual descriptions are informative. The remainder of this document is normative. Additionally, the use of keywords defined in Internet Engineering Task Force (IETF) RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels* [9] is considered normative within the scope of the sentence.

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

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[4] 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.

Section 2.1 - IC-ID below is the entirety of IC-ID.XML which defines IC Identifiers independently of any particular technology and/or implementation.

2.1 - IC-ID

IC Identifiers as specified in this document are based on the Globally Unique Identifiers for Everything (GUIDE) project of the Central Intelligence Agency (CIA). For background information on GUIDE see http://intellipedia.intelink.ic.gov/wiki/GUIDE. This specification defines the structure and format for globally unique identifiers for all kinds of resources. Registration and resolution of these identifiers to locations (typically with a URL) and retrieval (subject to access controls) is typically handled by a service. While this specification makes numerous references to such a service, this specification is not intended to fully describe, nor is it dependent on such a service. IC Identifiers are typically assigned to resources that are permanent and published, such as intelligence reports and other products. In contrast to common temporal URLs that can change over time and become invalid (i.e., dead links), properly maintained IC Identifiers will always refer to the resource, throughout their lifecycle, no matter where it is stored, or subsequently moved, within the enterprise.

2.1.1 - Deployment & Usage

The following MAY be modified by the Enterprise Standards Baseline (ESB) for example, from a SHOULD to a MUST:

- IC-IDs MUST remain completely UNCLASSIFIED, so they can be used on any network, classified or unclassified.
- IC-IDs MUST NOT encode any information with two exceptions: IC-IDs for **`@ntk:AccessPolicy`** and **`@ntk:ProfileDes`** as part of an Need-To-Know Metadata (NTK) Access Profile.
- IC-IDs MUST NOT encode classified information.
- References to resources (in other web pages, folders, comments, citations, etc.) SHOULD be encoded as IC-IDs.
- IC-IDs SHOULD be routinely assigned to every resource, as early in the resource’s life-cycle as possible.
- All content-creating applications assign IC-IDs to products. Downstream applications check for the existence of an IC-ID, and assign one if not found. Assign IC-IDs to legacy resources as needed.
- IC-IDs MAY be assigned to resources other than documents and digital media, e.g., user identities, non-person entities, and digital policies.

- Commercial data providers to the IC-ID MAY assign IC-IDs to content.
- Creation and assignment of an IC-ID to a resource is independent of registration in an IC-ID Service.
- IC-IDs are the preferred method of identifying and retrieving resources; e.g., IC-IDs SHOULD be returned in search results.

For more information on the ESB, please go to the “Enterprise Standards Baseline (ESB) Management” chapter in the IC-SF.XML[4].

2.1.2 - IC-ID Format and Lexicon

While this specification is useful in and of itself, the intended use is for IC-IDs to be incorporated into other specifications. This is the primary reason this specification defines IC-IDs by use of formal language known as ABNF. See http://en.wikipedia.org/wiki/Augmented_Backus-Naur_Form. The following ABNF rules explicitly define the content of an IC Identifier. ABNF is used to provide a formal description independent of any particular technology.

IC-ID Format

[1] IC-ID ::= IC-IDscheme"://" IC-IDprefix "/" IC-IDsuffix
[2] IC-IDscheme ::= "guide"
[3] IC-IDprefix ::= 1*16DIGIT
[4] IC-IDsuffix ::= 1*36(ALPHA / DIGIT / "_" / "-" / ".")

IC-ID Lexicon

The following vocabulary helps explain the meaning of terms used in IC-ID.XML documentation.

Canonical IC-ID

A globally unique identifier, composed of three parts: the IC-ID Scheme, an IC-ID Prefix, and an IC-ID Suffix, e.g., "guide://42/1c3". There MUST NOT be any meaning in an IC-ID with two exceptions: IC-IDs for **`@ntk:AccessPolicy`** and **`@ntk:ProfileDes`** as part of an NTK Access Profile as defined in the “Pre-Defined Access Profiles” section of *XML Data Encoding Specification for Information Security Markings* (ISM.XML[4]). All IC-IDs MUST remain completely UNCLASSIFIED. IC-IDs are immutable; both the Prefix and Suffix can never be changed. There is no theoretical size limit (length) of an IC-ID Prefix or Suffix, but maximum lengths have been established to avoid practical issues with software implementation and to support interoperability needs.

IC-ID Scheme

IC-IDs are intended to be processed using existing Uniform Resource Identifier (URI) processing techniques. To facilitate such we created an unregistered URI scheme of "guide".

IC-ID Prefix

An unsigned integer (base 10), e.g., "42". Prefixes are centrally controlled and assigned to an "owning" agency, program, or project by the IC-ID Prefix Governance process. IC-ID Prefixes from 0 to 999, 9000 to 9999 and 999000 to 999999 are reserved for testing purposes and can be assigned to any project needing them. A prefix is limited to a maximum length of 16 digits and leading zeros are not permitted (see Section 2.1.3.1 - Prefix Governance for details).

IC-ID Suffix

An alphanumeric string, e.g., "1c3". Allowed characters include A-Z, a-z, 0-9, underscore, hyphen, and period. Length is restricted to 36 characters. Suffixes must be unique within a given Prefix. Suffix generation is the responsibility of the client. For IC usage, it is recommended that clients generate Universal Unique Identifier (UUID) Suffixes. IETF-RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*IETF-RFC 4122[10] Type 1 or International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) Rec. X.667, *X.667 : Information technology - Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers* [13] | ISO/IEC 9834-8, *Information technology — Procedures for the operation of object identifier registration authorities — Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers* [11] are suggested. Other techniques may be used. However, some may inadvertently result in randomly generated words which could include offensive language.

2.1.3 - IC-ID Governance

2.1.3.1 - Prefix Governance

- Prefixes are centrally managed by the IC Identifier (IC-ID) project team.
- Prefixes are generally assigned to participating IC agencies in blocks.
- Clients must not begin using IC-ID Prefixes until formally approved and registered by the IC-ID project team.
- Some Prefixes are reserved for special purposes within the IC-ID service:
  - The range 0-999 is reserved for IC-ID internal uses.
  - The range 9000-9999 is reserved for future uses.
  - The range 999000-999999 is reserved for testing uses. This means that "real" data should never be assigned IC-IDs in this range.
- To request a Prefix, send an email to the IC-ID project team. See http://intellipedia.intelink.ic.gov/GUIDE#.28U.29 POCs [http://intellipedia.intelink.ic.gov/GUIDE#.28U.29%20POCs] for contact details.

2.1.3.2 - Suffix Governance

In general, there is no central governance on IC-ID Suffixes, as it is the responsibility of the client to generate the Suffix. Suffixes are generated by the client and MUST be unique within a Prefix.

For more guidance, see the IC-ID Suffix definition in the IC-ID Lexicon.

2.2 - 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.

2.3 - Additional guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations that have no clear, 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 DES are encouraged to contact the maintainers of this DES for further guidance when necessary.

There are two ways in which a consumer requiring an IC-ID can use the IC-ID.XML specification: through referencing objects defined in the schema or enforcing the format via running Schematron[12].

2.3.1 - Usage of the IC-ID Schema

The IC-ID.XML schema defines an element (**`Identifier`**) and an attribute (**`@identifier`**) that enforces the IC-ID format as defined in Section 2.1.2 - IC-ID Format and Lexicon. Consumers of the IC-ID.XML specification should import the IC-ID 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 contain an IC-ID, 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.

2.3.2 - Usage of the IC-ID Schematron Library

The IC-ID.XML Schematron library contains an abstract rule that enforces the IC-ID format as defined in Section 2.1.2 - IC-ID Format and Lexicon. Consumers of the IC-ID.XML 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 IC-ID format.

Note that consumers of the IC-ID.XML Schematron[12] library also need to import the IC-ID schema within their schema. The importing schema needs to reference the DES Version for IC-ID in order to let systems reviewing the data know what Schematron[12] library to import.

For information on what Schematron[12] is, please see the “Schematron” section in the IC-SF.XML[4] framework document.

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-ID.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[4] framework document.

3.2.1 - Inherited Constraints

In an instance of IC-ID.XML, the use of attributes and elements from supplementary data encoding specifications must be fully conformant with the constraint rules defined in those specifications. For a full list of supplementary specifications, see Section 1.5 - Dependencies.

3.2.2 - Value Enumeration Constraints

Several elements and attributes of the IC-ID.XML model use Controlled Vocabulary Enumeration (CVE)s 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.

3.3 - Additional Constraints

3.3.1 - 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.

3.4 - Constraint Rules

The detailed constraint rules for the IC-ID.XML schema can be found in a separate document inside the Documents/IC-ID directory, in the “IC-ID_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-ID_Rules.pdf” file.

3.5 - Data Rendering Constraint Rules

3.5.1 - Purpose

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

3.5.2 - Rendering Constraint Rules

The following table contains the information for the IC-ID.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 IC-ID.XML. 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 Markings[3] 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. IC-ID Feature Summary

Table 5 - IC-ID Feature comparison

Required date	Feature	V1	V2021-NOV
	Schema Element support	F	F
	Schema Attribute support	F	F
	Schematron support	F	F
	ABNF description of Identifier	F	F
	Removed ISM dependency	N	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
1	April 10, 2013	Initial Release
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 Requests

The following table summarizes the changes made to V1 in developing 2021-NOV.

Table 7 - Data Encoding Specification 2021-NOV Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Remove IC-ID's dependency on ISM for ShortStringType. (CR-2021-030)	Documentation Schema	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Updated documentation to use the specification framework. (CR-2019-030)	Documentation	No impact to systems.
3	Identify the lack of a root node in the Schema Guide. (CR-2019-120)	Schema	No impact to systems.
4	Added schema PDF. (CR-2018-014)	Documentation	No impact to systems.
5	Created schematron rule to check current DESVersion (CR-2017-302, CR-2017-222, CR-2017-081)	Schematron IC-ID-ID-00001 added	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.

Appendix C List of Abbreviations

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

ABNF	Augmented Backus-Naur Form
ADD	Abstract Data Definition
CIA	Central Intelligence Agency
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
ESB	Enterprise Standards Baseline
GUIDE	Globally Unique Identifiers for Everything
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
IC-ID	IC Identifier
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
NTK	Need-To-Know Metadata
RFC	Request for Comments
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universal Unique Identifier

XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

[1] ABNF

Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.
Available online at: http://tools.ietf.org/html/std68
Also known as: http://www.ietf.org/rfc/rfc5234.txt

[2] DoD Instruction 8320.03

Secretary of Defense. *Unique Identification (UID) Standards for Supporting the DoD Information Enterprise*. 8320.03. 31 August 2018.

31 August 2018 edition incorporates Change 2 to the 4 November 2015 edition and reissued as an Instruction.
Available online at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832003p.pdf

[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 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

[7] 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

[8] 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

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

[10] IETF-RFC 4122
Internet Engineering Task Force. *A Universally Unique IDentifier (UUID) URN Namespace*. July 2005.
Available online at: http://tools.ietf.org/html/rfc4122

[11] ISO 9834-8
International Organization for Standardization (ISO). *Information technology — Procedures for the operation of object identifier registration authorities — Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers*. ISO/IEC 9834-8:2014.
Available online at: https://www.iso.org/standard/62795.html

[12] 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/

[13] X.667
International Telecommunication Union. *X.667 : Information technology - Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers*. 14 October 2012.
Available online at: https://www.itu.int/rec/T-REC-X.667-201210-I/en

[14] 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[8].