



# **Intelligence Community Technical Specification**

---

## **XML Data Encoding Specification for Document and Media Exploitation**

**Version 2021-NOV**

December 1, 2022

Distribution Notice:

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

# Table of Contents

Chapter 1 - Introduction .....	1
1.1 - Purpose .....	1
1.2 - Scope .....	1
1.3 - Enterprise Need .....	1
1.4 - Conventions .....	2
1.4.1 - XML Namespaces .....	3
1.5 - Dependencies .....	3
1.5.1 - Specification Dependencies .....	3
1.5.2 - Inverse Dependencies .....	6
Chapter 2 - Development Guidance .....	7
2.1 - Relationship to Abstract Data Definition and other encodings .....	7
2.2 - Additional Guidance .....	7
2.2.1 - DOMEX Usage .....	7
2.2.2 - DOMEX XML Schema Namespaces .....	10
2.2.2.1 - <b>domex</b> Namespace Elements .....	10
2.2.2.2 - <b>Identity</b> Namespace Elements .....	12
2.2.2.3 - <b>cr</b> Namespace Elements .....	12
2.2.3 - DOMEX Assertion and Trusted Data Objects .....	12
2.2.4 - Handling Assertions .....	12
2.2.5 - Use of IRM (Formerly DDMS) Resource .....	12
2.2.6 - Specification of Dates .....	14
2.2.7 - Specification of Locations .....	14
Chapter 3 - Constraints .....	16
3.1 - Data Validation Constraint Rules .....	16
3.1.1 - Inherited Constraints .....	16
3.1.2 - Value Enumeration Constraints .....	16
3.1.3 - Additional Constraints .....	16
3.1.3.1 - DES Constraints .....	16
3.1.4 - Constraint Rules .....	16
3.2 - Data Rendering Constraint Rules .....	17
3.2.1 - Purpose .....	17
3.2.2 - Rendering Constraint Rules .....	17
Appendix A - Feature Summary .....	18
A.1 - DOMEX Feature Comparison .....	18
Appendix B - Change History .....	19
B.1 - V2021-NOV Change Summary .....	19
B.2 - V2015-AUG Change Summary .....	21
B.3 - V2 Change Summary .....	23
Appendix C - List of Abbreviations .....	26
Appendix D - Bibliography .....	28
Appendix E - Points of Contact .....	31
Appendix F - IC CIO Approval Memo .....	32

## List of Figures

Figure 1 - Related Specifications .....	6
Figure 2 - TDF with Assertions .....	8
Figure 3 - TDO Format Overview .....	9
Figure 4 - TDC Format Overview .....	10
Figure 5 - DOMEX:Acquisition Example .....	11

## List of Tables

Table 1 - XML Namespaces .....	3
Table 2 - Dependencies .....	4
Table 3 - irm:ICResourceMetadataPackage .....	13
Table 4 - Constraint Rules .....	17
Table 5 - Feature Summary Legend .....	18
Table 6 - DOMEX Feature Comparison .....	18
Table 7 - DES Version Identifier History .....	19
Table 8 - Data Encoding Specification V2021-NOV Change Summary .....	19
Table 9 - Data Encoding Specification V2015-AUG Change Summary .....	22
Table 10 - Data Encoding Specification V2 Change Summary .....	23

## Chapter 1 - Introduction

### 1.1 - Purpose

This *XML Data Encoding Specification for Document and Media Exploitation* (DOMEX.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode Document and Media Exploitation 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 DOMEX 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<sup>[3]</sup>) 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 applies to the Document and Media Exploitation (DOMEX) Community. The DOMEX Community is comprised of IC, Department of Defense (DoD), Department of Homeland Security (DHS), and Department of Justice (DOJ) components conducting or providing support to the conduct of DOMEX operations, activities, and functions. This specification defines the metadata standards for the uniform exchange of DOMEX. DOMEX metadata includes elements from the DOMEX taxonomy (collections, media sources/images, and content/files); communications tracking knowledge; and all identifying information extracted from within the data (names, locations, times, activities, relationships, etc.).

### 1.3 - Enterprise Need

Broad information sharing within the national intelligence enterprise is facilitated by the creation and identification of variants of information resources to serve different audiences. The creation of variants at lower classifications or in different formats allows for wider distribution of essential intelligence, protects classified information, protects information sources and methods, and provides a mechanism to connect variants thus diminishing one possible source of circular intelligence reporting.

In the aftermath of 9/11 the National Media Exploitation Center (NMEC) was chartered by the Director, Central Intelligence Agency (CIA) to become the nation's foremost proponent and focus for the exploitation and sharing of the massive captured and seized document and electronic media troves associated with the Global War on Terrorism. From a conceptual plan of action in late 2002, the NMEC partnership consisting of the CIA, Defense Intelligence Agency (DIA), DHS, Federal Bureau of Investigation (FBI), National Security Agency (NSA), and the Defense Cyber Crime Center (DC3) began in earnest in the summer of 2003 to consolidate and build upon the many disparate community DOMEX efforts. In July of 2007 Intelligence Community Directive (ICD) 302, *Document and Media Exploitation* <sup>[5]</sup> established NMEC as the IC's "service of common concern" for national DOMEX. In this capacity NMEC is chartered to help guide the broad community of interest in the development of domain-wide policy, doctrine, and sharing strategies for DOMEX.

ICD 302<sup>[5]</sup> formally defines DOMEX as the processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under the U.S. Government's

physical control and are not publicly available. This definition excludes: handling of documents and media during the collection, initial review, and inventory process; and documents and media withheld from the IC DOMEX dissemination system in accordance with Director of National Intelligence (DNI)-sanctioned agreements and policies to protect sources and methods.

DOMEX includes any information storage media and the means by which it was created (e.g., written, mechanical, chemical electronic, optical, or magnetic form). A document is any recorded information regardless of its physical form or characteristics, including, but not limited to, all written material, whether handwritten, printed, engraved, or photographic matter, which may contain information relative to adversary forces or individuals and groups under investigation for criminal acts. Media is any chemically, mechanically, electronically, or digitally recorded media such as computer files, hard drives, thumb drives, micro-drives, media cards, CD-ROMS, MP3 players, floppy disks, tape recordings, video, sound or voice recordings, DVDs, movie and photographic film, cellular phones, Global Positioning System devices, and typewriter and printer ribbons.

Today, the growing demand for DOMEX across the spectrum of military, Law Enforcement, and Intelligence Community activities is a reflection of the inherent value of captured media and the growing reliance on this intelligence for theater combat and stabilization operations as well as homeland security activities.

NMEC continues to evolve the art and science of DOMEX and derivative intelligence sharing. By working closely with the U.S. Army National Ground Intelligence Center (NGIC)'s National Harmony, the nation's designated database for foreign exploitable materials, NMEC ensures language-based intelligence products are available to consumers throughout the IC. By working with its partnered agencies, NMEC is building high volume data links for the widest possible audience. NMEC is rapidly expanding the number of mission functions participating directly in the exploitation of collected materials while continuing to develop and incorporate new tools and systems to expand mission specific data to the widest possible community of interest.

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

- 300 Series:
  - ICD 302, *Document and Media Exploitation* [\[5\]](#)
- 500 Series:
  - ICD 500, *Director Of National Intelligence Chief Information Officer* [\[6\]](#)
  - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [\[8\]](#)
- DoD Issuances:
  - Department of Defense Directive Number 3300.03, *DoD Document and Media Exploitation (DOMEX)* [\[1\]](#)

## 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 XML Qualified Name used in any example in this document should be interpreted using the information below.

**Table 1 - XML Namespaces**

Prefix	URI
irm	urn:us:gov:ic:irm
domex	urn:us:mil:ces:metadata:domex
ism	urn:us:gov:ic:ism
cr	urn:CellerReport
Identity	urn:us:mil:ces:metadata:domex_identity

## 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<sup>[3]</sup>.

### 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.

In the related specifications figure, [Figure 1](#), SOME-TDF is not an actual specification but a placeholder in the diagram that represents the fact that this specification depends on some TDF specification in its usage as an assertion in a Trusted Data Object (TDO).

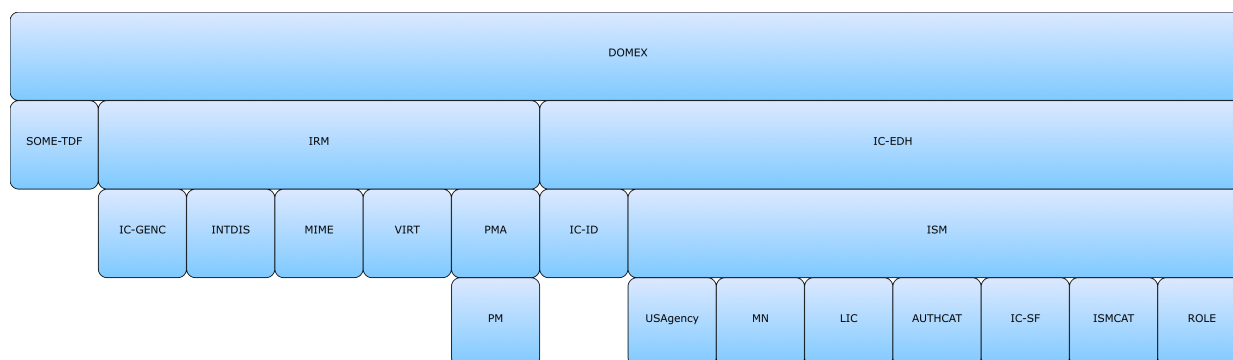


**Table 2 - Dependencies**

Name	Dependency Description
<i>XML Data Encoding Specification for Trusted Data Format</i> (IC-TDF.XML.V2021-NOV+ <sup>[4]</sup> )	This specification depends on the LATEST technically sound, approved version of IC-TDF.XML <sup>[4]</sup> . The dependence of DOMEX.XML on IC-TDF.XML is normative. The minimum version is based on a technical dependency, specifically a correction to a rule that can affect DOMEX: CR-2017-207, TDF Validation Missing RevRecall ISM Consistency Checks.
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ <sup>[10]</sup> )	This specification depends on the LATEST technically sound, approved version of ISM.XML <sup>[10]</sup> . The minimum version was based on compliance with the authoritative source, which is ICD-710 <sup>[7]</sup> . 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 Enterprise Data Header</i> (IC-EDH XML.V2019-MAR+ <sup>[2]</sup> )	This specification does not depend on a specific version of IC-EDH.XML <sup>[2]</sup> ; versions later than version 2019-MAR MAY be used. The dependence of DOMEX.XML on IC-EDH.XML is normative. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.
<i>XML Data Encoding Specification for Information Resource Metadata</i> (IRM.XML.V2021-NOV+ <sup>[9]</sup> )	This specification depends on the LATEST technically sound, approved version of IRM.XML <sup>[9]</sup> . The dependence of DOMEX.XML on IRM.XML is normative. The minimum version is based on a technical dependency, specifically CR-2019-173. This CR modifies the representation of foreign partner organizations in IRM.XML <sup>[9]</sup> to conform to a general change across IC Technical Specifications.
<i>CVE Encoding Specification for US Agency</i> (USAgency.CES.V2017-MARr2018-FEB+ <sup>[14]</sup> )	The specification does not depend on a specific version of USAgency.CES <sup>[14]</sup> ; versions later than version 2017-MARr2018-FEB MAY be used. The minimum version was based on the earliest non-retired version; Enterprise Standards Baseline (ESB) 21-2.0 was used for determining the version.

Name	Dependency Description
<i>CVE Encoding Specification for Media Type</i> (MIME.CES.V2020-OCT+ <sup>[11]</sup> )	The specification does not depend on a specific version of MIME.CES <sup>[11]</sup> ; versions later than version 2020-OCT MAY be used. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ <sup>[3]</sup> )	This specification does not depend on a specific version of IC-SF.XML <sup>[3]</sup> ; 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.
Time Space Position Information (TSPI) 2.0, <i>NGA Standardization Document, Time-Space-Position Information (TSPI)</i> <sup>[13]</sup> .	This specification depends on TSPI Version 2.0 for capturing map and geographical information.
Schematron <sup>[12]</sup>	<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<sup>[15]</sup> query binding.</p>

Name	Dependency Description
<p>XSLT 2.0<sup>[15]</sup> implementation of Schematron<sup>[12]</sup> 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): <a href="http://code.google.com/p/schematron/">http://code.google.com/p/schematron/</a>.</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 <b>MUST</b> 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>



**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<sup>[3]</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 - 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 - 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 DES are encouraged to contact the maintainers of this DES for further guidance when necessary.

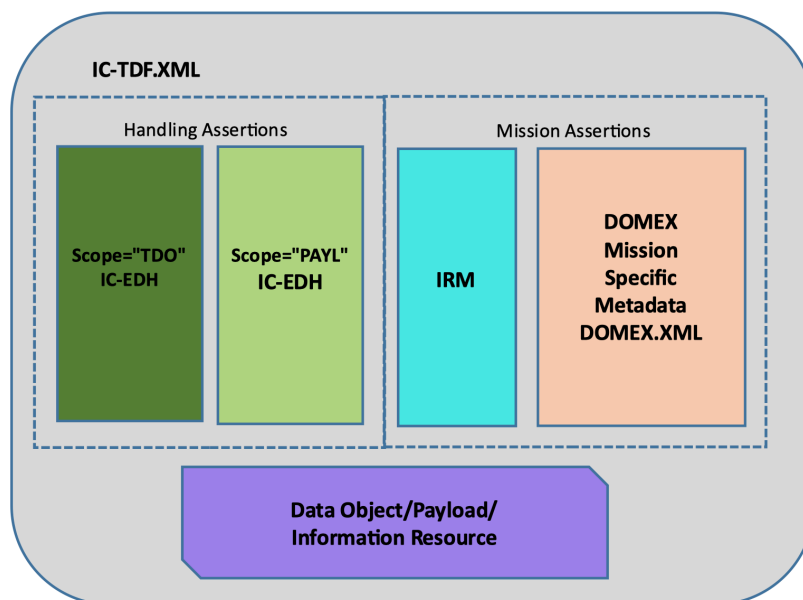
#### 2.2.1 - DOMEX Usage

DOMEX.XML is used in conjunction with TDF objects as structured assertions that contain information required for generating a TDO or Trusted Data Collection (TDC). The *XML Data Encoding Specification for Trusted Data Format* (IC-TDF.XML<sup>[4]</sup>) has a consistent and simple concept of Assertions and Payloads. There are two options for root elements: TDO and TDC. A TDO contains some data (the payload) and some statements about that data (the assertions). In the context of TDF, an 'assertion' is defined as a statement providing handling, discovery, or mission metadata describing a payload, TDO, or TDC depending on the scope of the assertion. Each TDO must contain at least two handling assertions, which provides the minimum information needed to protect the data. Additional discovery and mission assertions may also be provided. A TDC contains a list of TDOs (the payload) and some statements about those TDOs (the assertions). A TDO or TDC conforms to the DOMEX.XML specification when it contains:

- An assertion with a structured statement containing the *XML Data Encoding Specification for Enterprise Data Header* (IC-EDH.XML<sup>[2]</sup>) handling assertions and payloads. Any TDO with a DOMEX assertion, regardless of its root element, **MUST** contain at least two Enterprise Data Header (EDH) handling assertions; **"TDO"** and **"PAYL"**.

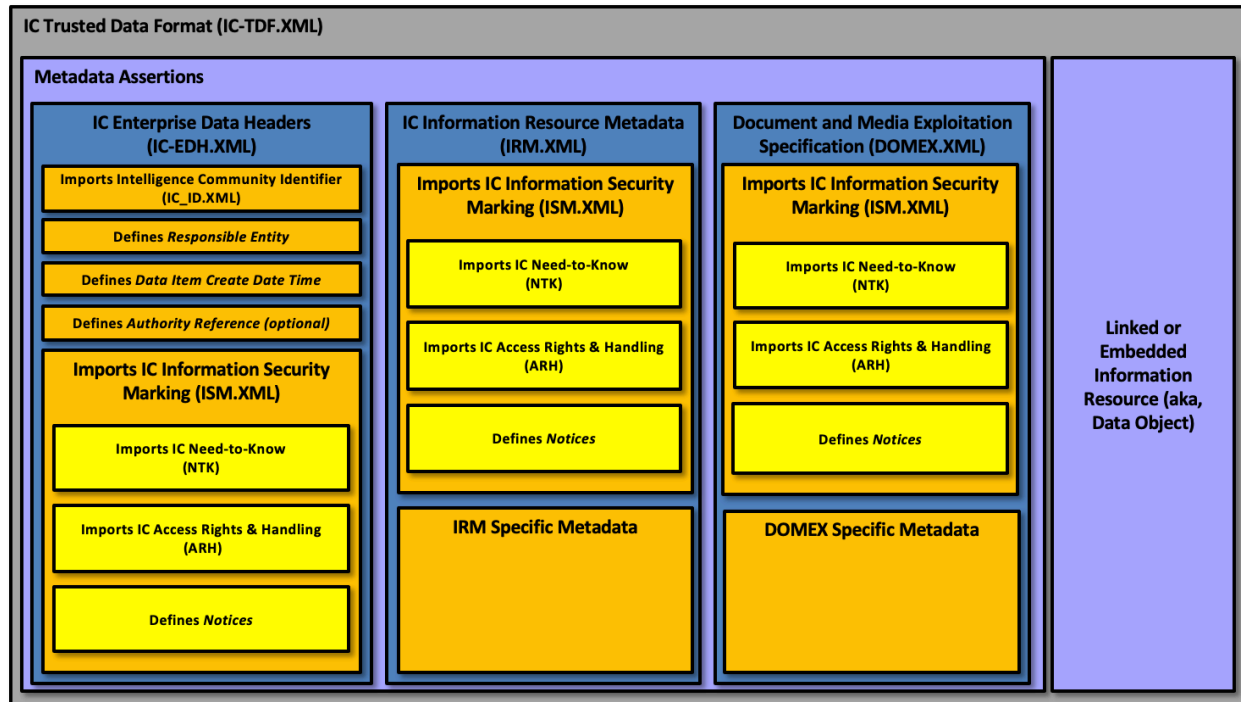
- An assertion with a structured statement containing the *XML Data Encoding Specification for Information Resource Metadata* (IRM.XML<sup>[9]</sup>) resource elements. See [Section 2.2.5 - Use of IRM \(Formerly DDMS\) Resource](#) for more information. Any TDO with a DOMEX assertion, regardless of its root element, **MUST** contain an Information Resource Metadata (IRM) assertion.
- A structured assertion of scope TDO or TDC with a DOMEX root element. DOMEX contains 3 namespaces: domex, Identity, and cr. Each namespace contains one or more root elements. A DOMEX assertion can use any of the namespaces. It is the union of the 3 namespaces that makeup the DOMEX assertion. For more information on DOMEX namespaces, see [Section 2.2.2 - DOMEX XML Schema Namespaces](#).
- A data payload that is a string, a file or other binary data, XML structured content, or reference to the data payload that is not embedded in the TDO but stored in a remote/external location. Linked objects classification does NOT impact the classification of the TDO. Embedded objects classification does impact the classification of the TDO.

As depicted in the diagram below, the TDO will contain the metacard creation and security metadata for the TDO, an EDH with “payload” scope containing the security metadata for the payload, a discovery assertion containing a structured IRM instance, the DOMEX Mission Specific metadata, and a payload, which can be either the URL of the resource or the resource itself. Typically the URL for the resource would be the same as the `@irm:identifier`.



**Figure 2 : TDF with Assertions**

The diagram below shows expected use of IC specifications within a TDO and a DOMEX-specific metadata assertion.



**Figure 3 : TDO Format Overview**

The EDH Assertion identifies the security, access rights and handling, notices, and need to know information for the TDO and the payload. The IRM instance provides information security markings at a portion-marking level.

A TDC consists of a collection of TDOs or TDCs. When used with the DOMEX mission specific metadata assertion, the TDOs and TDCs are in some way related, with relationships encoded in the TDC assertions.

A Cellphone Exploitation (CELLEX) metadata dissemination use case is illustrated below. The TDC corresponds to CELLEX metadata in a foreign language, with child TDOs corresponding to the original foreign language metadata and different types of translations of the metadata. The DOMEX assertion, scoped TDC, will contain the collection details metadata associated with the circumstances of the original mobile device acquisition. The child TDOs will contain metadata about the translated contents of the mobile device. The payload data is the CELLEX metadata consisting of structured XML.

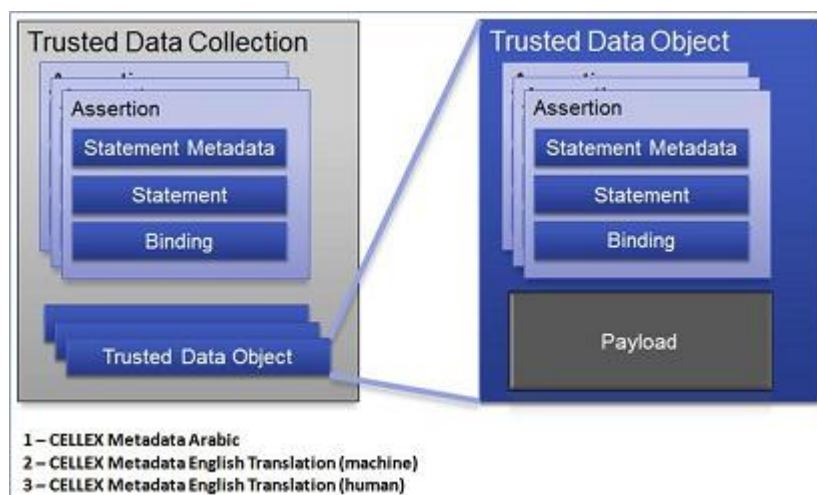


Figure 4 : TDC Format Overview

## 2.2.2 - DOMEX XML Schema Namespaces

The DOMEX.XML schema contains unique namespaces to manage DOMEX metadata in logical blocks; domex, Identity, and cr. A DOMEX assertion may contain elements from all three namespaces depending on the object(s) described.

### 2.2.2.1 - *domex* Namespace Elements

The domex namespace includes metadata about a DOMEX collection or single piece of media within a collection that generally answers questions related to the standards of who, what, when, where, why, and how the material was acquired. It also includes metadata about the DOMEX object (file): the original document, derived content, and analytic metadata. Document metadata includes translation metadata and related files. Documents include: documents, videos, images, audio files, and scanned documents (including pocket litter). The **domex** element is used as the root element for a DOMEX assertion. The domex namespace has multiple, alternate root elements: **acquisition**, **collectionDetails**, **subjectInformation**, **equipment**, **facility**, **organization**, **file**, and **mediaDetails**.

#### acquisition

The **acquisition** element is contained in the structured statement of an assertion within a TDO with scope TDO or a TDC with scope TDC. In this context, the instance should be representative of the entire object including all variants. It contains data about a collection or single piece of media within a collection that generally answers core issues related to the standards of who, what, when, where, why, and how the material was collected. Examples of acquisition data are date/time collected, location of collection, collecting organization, legal authority for the collection, processing site, size and type of media, classification, and more. The **@DESVersion** attribute indicates the DOMEX.XML version, and the other elements and attributes represent the acquisition details, collection details, subject information, media details, file details, and analytic metadata for the object. The figure below provides an example.



```

<Assertion tdf:scope="TDO">
  <StatementMetadata>
    <Security xmlns="urn:us:gov:ic:arh"
      ism:classification="U"
      ism:ownerProducer="USA"/>
  </StatementMetadata>
  <StructuredStatement>
    <domex:domex domex:DESVersion="1">
      ...
    </domex:domex>
  </StructuredStatement>
</Assertion>

```

**Figure 5 : DOMEX:Acquisition Example**

collectionDetails	The <b>collectionDetails</b> element is used to specify metadata about documents and/or electronic media acquired during the same capture, seizure, or acquisition event at the same location or attributed to the same individual(s) or group.
subjectInformation	The <b>subjectInformation</b> element is used to specify metadata about the subject of an acquisition. A “subject” could be a person, organization, facility, or piece of equipment that is associated with an acquisition. Multiple subjects of differing types are permitted.
equipment	The <b>equipment</b> element is used to specify metadata about equipment when equipment is the subject of an acquisition. It is also used to specify content and analytic equipment metadata extracted from the file object or added through content management and analysis.
facility	The <b>facility</b> element is used to specify metadata about a facility when a facility is the subject of an acquisition. It is also used to specify content and analytic facility metadata extracted from the file object or added through content management and analysis.
organization	The <b>organization</b> element is used to specify metadata about an organization when an organization is the subject of an acquisition. It is also used to specify content and analytic organization metadata extracted from the file object or added through content management and analysis.
file	The <b>file</b> element is used to specify metadata about an original document, derived content, and analytic metadata. Document metadata includes original file metadata, translation metadata, and related files. Documents include videos, images, audio files, and scanned documents (including pocket litter).



**mediaDetails**

The **mediaDetails** element is used to specify metadata about the media or device source. Media or device metadata includes connection to collection data, item identity within the context of a collection, hardware serial number, model number, and image hash value. Physical media may contain one or more files.

## 2.2.2.2 - Identity Namespace Elements

The Identity namespace contains metadata about the subject of an acquisition when the subject is a person. It may also be used for content and analytic identity metadata extracted from the file object or added through content management and analysis. The root element in the Identity namespace is **identity**.

## 2.2.2.3 - cr Namespace Elements

The cr namespace contains CELLEX metadata extracted from mobile devices using various cellular forensics and exploitation toolkits. The root element in the cr namespace is **cellexReport**.

## 2.2.3 - DOMEX Assertion and Trusted Data Objects

TDOs and TDCs adhere to the IC-TDF.XML<sup>[4]</sup> schema, and the DOMEX metadata is contained in a DOMEX assertion within the TDO or TDC. The DOMEX assertion adheres to the DOMEX.xsd.

## 2.2.4 - Handling Assertions

To facilitate handling and access control decisions, each TDO and TDC MUST contain at least two handling assertions, one with a scope of "**TDO**" and the other with a scope of "**PAYL**" and should be filled out in accordance with the IC-EDH.XML<sup>[2]</sup> specification. A handling assertion is a special type of structured assertion that cannot be encrypted. In general, the handling assertion contains the EDH for the TDO or Payload, providing the attributes needed for policy decisions regarding access control and how the data must be handled.

## 2.2.5 - Use of IRM (Formerly DDMS) Resource

DOMEX.XML uses the IRM.XML<sup>[9]</sup> **ICResourceMetadataPackage** element to capture the "library-card" or discovery and summary content metadata for the DOMEX object. DOMEX discovery metadata is always contained in the IRM assertion and is not duplicated in the DOMEX assertion. The **irm:ICResourceMetadataPackage** is a required assertion in the TDO or TDC that also contains a DOMEX assertion. Additional clarification may be obtained from the IRM.XML<sup>[9]</sup> specification. A crosswalk worksheet also is provided in the IRM.XML<sup>[9]</sup> specification Examples folder. The crosswalk provides additional guidance for populating optional IRM elements with DOMEX elements. Implementers are encouraged to populate the optional IRM elements when possible. There are some cases where multiple DOMEX elements could populate a single IRM resource element depending on the described DOMEX object, for those cases additional guidance is provided in the table below.

**Table 3 - irm:ICResourceMetadataPackage**

<b>irm:ICResourceMetadataPackage</b>	<b>Additional Clarification/Guidance</b>
./title	<p>IRM does not permit the specification of language for the title element. Therefore, the translated and descriptive title elements will remain in the DOMEX assertion. Implementers are advised that the IRM title element must be a human readable name identifying the DOMEX object. The IRM title element should be populated with the English language translation of the title of the DOMEX object or file or the descriptive title. This field must be a human readable name identifying the DOMEX object.</p> <p>Examples:</p> <p>domex:acquisition</p> <p>./title[@type=Translated] or</p> <p>./title[@type=Descriptive]</p>
./identifier	<p>DOMEX identifiers will use the IRM resource element irm:identifier with a qualifier and value. Qualifiers may include domexID, collectionId, harmonyNumber, and hashValue.</p> <p>Note: The inclusion of one identifier element is mandatory; there is no upper bound on the number of identifier elements.</p>
./publisher	<p>Information about the entity responsible for releasing the DOMEX object. It is intended for this to represent the organization or web service releasing the DOMEX object.</p>
./acquiredOn	<p>The IRM element acquiredOn is used for the date the original DOMEX object was obtained, acquired, or collected.</p>
./subjectCoverage/keyword	<p>Keywords about the DOMEX object. Generic or specific terms representing the content of the original DOMEX object.</p>
./geospatialCoverage/boundingGeometry/tspi:Point	<p>The collection location coordinates that represent the location of where the described DOMEX object was collected. It is up to the publisher of the DOMEX object to determine if this optional element is populated.</p>

irm:ICResourceMetadataPackage	Additional Clarification/Guidance
./description	The publisher should determine which descriptive element best represents the object described in the TDO or TDC. The description element may be populated with the domex:acquisition./collectionDescription or ./remark

## 2.2.6 - Specification of Dates

Dates in DOMEX.XML including: **entryDate**, **dateAccessed**, **dateCreated**, **dateModified**, **dateAndTimeOfLastModification**, **dateTimeOriginal**, **translationDate**, **requestDate**, **dateRequired**, **date**, **departureDateTime**, **arrivalDateTime**, **startDate**, **endDate**, **creationDate**, and **lastModifiedDate**, use the IRM construct **Combined Date** that supports a range of date representations. The date SHALL be specified in one of the following formats:

YYYY

YYYY-MM

YYYY-MM-DD

YYYY-MM-DDThhTZD

YYYY-MM-DDThh:mmTZD

YYYY-MM-DDThh:mm:ssTZD

YYYY-MM-DDThh:mm:ss.sTZD

Where:

YYYY 0000 through current year

MM 01 through 12 (month)

DD 01 through 31 (day)

hh 00 through 23 (hour)

mm 00 through 59 (minute)

ss 00 through 59 (second)

.s .0 through 999 (fractional second)

TZD = time zone designator (Z or +hh:mm or -hh:mm)

Times are expressed in Coordinated Universal Time (UTC) (Coordinated Universal Time), with a special UTC designator ("Z").

The **documentDate** element uses the IRM construct **ApproximableDate** that allows for the date to be specified in terms of approximate start and end dates or in a descriptive way.

## 2.2.7 - Specification of Locations

Location elements in DOMEX XML including: **collectionLocationCoordinates**, **gpsCoordinates**, and **location** use the TSPI version 2.0-compliant structures<sup>[13]</sup>. This permits the DOMEX definition of geospatial concepts to be consistent with IRM standards used across the DoD and the international standards community. When encoding geospatial coordinates, the following guidelines should be followed:

- Latitude SHALL be in decimal degrees in the range -90° <= latitude <= +90°.

- North latitudes SHALL be positive, south latitudes shall be negative.
- Longitude SHALL be in decimal degrees in the range  $-180^{\circ} \leq \text{longitude} \leq +180^{\circ}$ ; note that there are two equally acceptable values of longitude for the meridian opposite the prime meridian.
- East longitudes SHALL be positive, west longitudes shall be negative.
- Only the element `tspi:Point` shall be used to encode a geographic point location as either two decimal values in the order of latitude then longitude (no commas) when WGS84E\_2D, or three decimal values in the order latitude then longitude then height above ellipsoid (no commas) when using the WGS84E\_3D CRS.

The **address** element is encoded using the IRM postalAddress construct.

## Chapter 3 - Constraints

### 3.1 - Data Validation Constraint Rules

The DOMEX.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<sup>[3]</sup> framework document.

#### 3.1.1 - Inherited Constraints

In an instance of DOMEX.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](#).

#### 3.1.2 - Value Enumeration Constraints

Several elements and attributes of the DOMEX.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.

#### 3.1.3 - 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 DOMEX.XML schema can be found in a separate document inside the Documents/DOMEX directory, in the “DOMEX\_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 “DOMEX\_Rules.pdf” file.

## 3.2 - Data Rendering Constraint Rules

### 3.2.1 - Purpose

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

**Table 4 - 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 DOMEX.XML

Table 5 - 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. DOMEX Feature Comparison

Table 6 - DOMEX Feature Comparison

Required date	Feature	V1	V2	V2015-AUG	V2021-NOV
	DOMEX Agency CVE	N	F	F	F
	Hash Values	N	N	F	F
	Legacy File Types	N	N	F	F
	USB Device Info	N	N	F	F
	DOMEX Collections Descriptors	N	N	F	F
	Activity Identification	N	N	F	F
	Removal of DDMS standard (subsumed onto IRM.XML <sup>[9]</sup> )	N	N	N	F
	Added new domex:domex all-inclusive root element.	N	N	N	F

## Appendix B Change History

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

**Table 7 - DES Version Identifier History**

Version	Date	Purpose
1	August 16, 2013	Initial Release
2	March 14, 2014	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - V2 Change Summary</a>
2015-AUG	August 13, 2015	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - V2015-AUG Change Summary</a>
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V2021-NOV Change Summary</a>

### B.1 - V2021-NOV Change Summary

Significant drivers for version 2021-NOV include:

- Inclusion of new ISM version.\*
- Removal of DDMS standard (subsumed onto IRM).
- Community Change Requests.

[Table 8](#) summarizes the changes made to this technical specification from version 2015-AUG to version 2021-NOV.

**Table 8 - Data Encoding Specification V2021-NOV Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Updated documentation to use the specification framework. (CR-2019-026)	Documentation	No impact to systems.
2	Added Deprecation Field to CVEs. (CR-2018-079)	CVEs	Systems need to be updated to accommodate this change.
3	Added PDF of Schema Files. (CR-2018-010)	Schema	No impact to systems.
4	Created RELAX NG forms of CVEs. (CR-2017-171)	CVEs	No impact to systems.
5	Created JSON version of CVEs. (CR-2017-052)	CVEs	No impact to systems.



#	Change	Artifacts changed	Compatibility Notes
6	Created CSV version of CVEs. (CR-2017-030)	CVEs	No impact to systems.
7	Identified the root node in the Schema Guide. (CR-2019-116)	Documentation	No impact to systems.
8	Updated for removal of DDMS (CR-2019-168)	DOMEX and Identity Schemas	Systems need to be updated to accommodate this change.
9	Issues in DOMEX Rule 00002 - Rule 0002 enforced DDMS assertion presence. Obsolete. Removed. (CR-2017-272)	Schematron DOMEX-ID-00002 deleted	Systems need to be updated to accommodate this change.
10	Update Schematron rules to have ISM attributes (CR-2017-298)	Schematron rules - all	No impact to systems.
11	Any TDO with a DOMEX assertion regardless of its root element is now checked to ensure the TDO also contains an IRM assertion. (Including CellexReport or Identity) (CR-2017-273)	Schematron DOMEX-ID-00004 modified	Systems need to be updated to accommodate this change.
12	Any DOMEX assertion regardless of its root element is now checked to ensure its scope is either TDO or TDC. (Including CellexReport or Identity) (CR-2017-271)	Schematron DOMEX-ID-00009 added	Systems need to be updated to accommodate this change.
13	Added new domex:domex all-inclusive root element and added @DESVersion to all existing root elements. All systems must now supply a DESVersion attribute on the DOMEX assertion root element. All systems may now use the domex:domex root for clearer definition of a DOMEX root. (Including CellexReport or Identity) (CR-2017-269)	DOMEX, CellexReport and Identity Schemas Schematron DOMEX-ID-00008 added	Systems need to be updated to accommodate this change.
14	Add @id and @role to Schematron (CR-2017-219)	Schematron rules - all	Systems need to be updated to accommodate this change.
15	Updated Schematron rules to be warnings instead of errors for matching Version attribute - Converted to environment check. (CR-2017-077)	Schematron DOMEX-ID-00001 modified	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
16	Updated Rule filenames to match pattern (CR-2016-073)	Schematron DOMEX-ID-00001 modified DOMEX-ID-00003 modified DOMEX-ID-00004 modified DOMEX-ID-00005 modified DOMEX-ID-00006 modified DOMEX-ID-00007 modified	No impact to systems although may prevent unnecessary error and/or warning messages from some validators.
17	Updated Dependency table to point to the appropriate law or policy for ISM. (CR-2019-148)	Documentation	No impact to systems.
18	Updated documentation to better explain the 3 DOMEX namespaces and the root nodes within. (CR-2017-270)	Documentation	No impact to systems.
19	Added DESVersion warning enforcement rules (CR-2021-001)	Schematron DOMEX-ID-00010 added DOMEX-ID-00011 added DOMEX-ID-00012 added DOMEX-ID-00013 added DOMEX-ID-00014 added	No impact to systems.
20	Updated rule to handle agency values that now have "USA." prefixed (CR-2019-003)	Schematron DOMEX-ID-00006 modified	No impact to systems although may prevent unnecessary error and/or warning messages from some validators.

\* - Systems using version 2015-AUG or earlier must check and update if necessary for compliance with new ISM standard.

## B.2 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Supporting legacy DOMEX data
- Support for additional hashing algorithms
- Adding USB Device Information
- Adding Activity Element and CVE

The following table summarizes the changes made to V2 in developing V2015-AUG.

**Table 9 - Data Encoding Specification V2015-AUG Change Summary**

Change	Artifacts Changed	Compatibility Notes
Accommodate additional derived file types that exist in legacy data. Move media information and translation information into the main file model. Modify derived file type to be a generic file type.	Schema Examples	Data generation and ingestion systems need to be updated in order to support the concept of derived files from derived files and derived file types that exist in legacy data.
Rename existing fileType element to fileMimeType. Create new fileType element supported by CVEnumFileType.	Schema CVEnumFileType Examples	Data generation and ingestion systems need to be updated in order to support the file types that exist in legacy data.
Add new elements to the Collection Details container element.	Schema Examples	Data generation and ingestion systems need to be updated in order to fully model legacy data.
Unbounded the element hashValue to allow for multiple hashing algorithm values.	Schema Examples	Data generation and ingestion systems need to be updated to provide for the expression of multiple hash values that may be associated with a DOMEX object.
Add new elements and attributes for USB devices.	Schema Examples	Data generation and ingestion systems need to be updated to support USB device metadata.

Change	Artifacts Changed	Compatibility Notes
Add new elements Activity and SubActivity supported by new CVEnumDOMEXActivity and Schematron rule at the Collection, Media, and File level.	Schema Examples Schematron Unit Test	Data generation and ingestion systems need to be updated to support Activity and SubActivity metadata. When a DOMEX object (Collection, Media, or File) is tagged with an Activity value and optional SubActivity element, the new Schematron rule validates the SubActivity value is valid for the given Activity value.
Updated code descriptions to improve readability.	Schematron	No impact to data generation and ingestion systems.

## B.3 - V2 Change Summary

Significant drivers for Version 2 include:

- Changes resulting from the DOMEX metadata standards pilot effort.

The following table summarizes the changes made to V1 in developing V2.

**Table 10 - Data Encoding Specification V2 Change Summary**

Change	Artifacts Changed	Compatibility Notes
Merge and update Media Type CVEs.	Merged CVEnum-DOMEXFileMediaType and CVEnumDOMEXImageMediaType to create new CVE CVEnum-DOMEXMediaType  Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated to use the new CVE and media type values.
Unbounded the Identity namespace element 'alias' to allow association of multiple aliases with a single identity.	Schema  Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated to allow multiple aliases.

Change	Artifacts Changed	Compatibility Notes
Update Identity namespace elements 'placeofBirth' and 'placeofDeath' to provide better specificity of location.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated to allow for the expanded location element values.
Unbound the DOMEX namespace element facility address to allow for multiple addresses to be associated with a single facility.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
Unbound the DOMEX namespace element file/project to allow multiple project names to be associated with a single collection event.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
In the DOMEX namespace remove required elements on Original file.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
Adopt Geopolitical Entities, Names, and Codes (IC-GENC)	Schema Schematron CVEnumIRMCoverageISO3166-Trigraph removed. Included IC-GENC CVEs. Unit Tests Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated to remove the IRM CVE and use the IC-GENC CVEs.
Made DOMEX namespace complex element deviceImage optional.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
Made CellexReport namespace complex element uploadInfo optional.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.

Change	Artifacts Changed	Compatibility Notes
Create new DOMEX CVE for agencies.	Schema New CVEs added for DOMEX agencies. Schematron Unit Tests Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated to use the new DOMEX agency CVEs.
Add idNumber element to identificationType/license in the Identity namespace to allow a license number to be recorded.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
Update CVEnum-DOMEXLicenseType with new terms Passport and Visa.  Update LicenseType element with destinationCountry.	Schema CVEnumDOMEXLicenseTypeType updated. Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
Remove hash code value from the Department of Defense Discovery Metadata Specification (DDMS) assertion.	Schema Examples	Data generation and ingestion systems participating in the DOMEX metadata pilot effort need to be updated.
Add Crosswalk Worksheet DOMEX V2 to DDMS V5.	Examples	None.

## Appendix C List of Abbreviations

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

ADD	Abstract Data Definition
CELLEX	Cellphone Exploitation
CIA	Central Intelligence Agency
CVE	Controlled Vocabulary Enumeration
DC3	Defense Cyber Crime Center
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOMEX	Document and Media Exploitation
EDH	Enterprise Data Header
ESB	Enterprise Standards Baseline
FBI	Federal Bureau of Investigation
GENC	Geopolitical Entities, Names, and Codes
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IRM	Information Resource Metadata
ISO	International Organization for Standardization

NGIC	National Ground Intelligence Center
NMEC	National Media Exploitation Center
NSA	National Security Agency
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TSPI	Time Space Position Information
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations



## Appendix D Bibliography

[1] DoD Directive 3300.03

Secretary of Defense. *DoD Document and Media Exploitation (DOMEX)*. 3300.03. 11 January 2011.

Available online at: <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/330003p.pdf>

[2] IC-EDH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Data Header (IC-EDH.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/5Pg1r8s> (case sensitive – 5 Papa golf 1 romeo 8 sierra )

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

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

[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] 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>

[5] 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](http://www.dni.gov/files/documents/ICD/ICD_302.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](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)

[7] 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](http://www.dni.gov/files/documents/ICD/ICD_710.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] 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>

[10] 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>

[11] MIME.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Media Type (MIME.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/3UCPH01> (case sensitive – 3 Uniform Charlie Papa Hotel 0 1 )

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

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

[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] TSPI 2.0

National Geospatial Intelligence Agency. *NGA Standardization Document, Time-Space-Position Information (TSPI)*. Version 2.0. 5 April 2012.

[14] USAgency.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/wmyIRCV> (case sensitive – whiskey mike yankee India Romeo Charlie Victor )

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

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

[15] 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 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>[8]</sup>.