Intelligence Community Technical Specification

XML Data Encoding Specification for Document and Media Exploitation

Version 2015-AUG

August 13, 2015

Table of Contents

List of Figures

List of Tables

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 DOMEX 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

This specification applies to the DOMEX Community. The DOMEX Community is comprised of Intelligence Community (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 - Background

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [9] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common Information Technology (IT) standards, protocols, and interfaces, to establish uniform information security standards, and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* [12] the extensive and consistent use of Extensible Markup Language (XML) within data encoding

specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

An encoding specification defines how to implement the abstract data elements in the IC Abstract Data Definition (ADD) in a particular physical encoding (e.g., data or file format). For example:

- Encoding specifications for textual markup formats, such as XML and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.
- Encoding specifications for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.
- Encoding specifications for application-specific formats, such as Microsoft Word, define document properties, styles, fields, cardinalities, processing requirements, and use.

1.4 - 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, DIA,, DHS, FBI, 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[8] 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 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 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's (NGIC) 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.

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[5]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[9]
- 300 Series:
  - Intelligence Community Directive (ICD) 302, Document and Media Exploitation[8]
- DoD Issuances:
  - Department of Defense Directive Number 3300.03, DoD Document and Media Exploitation (DOMEX) [4]

1.5 - Audience and Applicability

DESs are primarily intended to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described.

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance ,* [11] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

1.6 - Conventions

Certain technical and presentation conventions were used in the creation of this document to ensure readability and understanding.

1.6.1 - Language

The keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this technical specification are to be interpreted as described in the IETF RFC 2119.[13] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.6.2 - Typography

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

1.6.3 - Terminology

For an implementation to conform to this specification, it MUST adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

1.6.4 - 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
ddms	urn:us:mil:ces:metadata:ddms:5
domex	urn:us:mil:ces:metadata:domex
ism	urn:us:gov:ic:ism
cr	urn:CellexReport
Identity	urn:us:mil:ces:metadata:domex_identity

1.7 - 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 IC CIO specifications related to this specification. The graphic depicts direct and transitive 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 specifications listed in Table 2 will be shown in Figure 1; however not all specifications listed in Figure 1 may appear in Table 2. Figure 1 is to aid users in gaining a general understanding of all transitive dependencies.

Table 2 - Dependencies

Name	Dependency Description
XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V1+)[7]	DOMEX elements are used in conjunction with TDF collections as structured assertions that indicate how objects in a trusted data collection are related. The dependence of DOMEX on TDF is normative. Starting with TDF V1, the version of TDF and related specifications imported is no longer normative, so any TDF version 1 or above may be used with DOMEX v1.
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V12+) [15]	Depends on Information Security Markings (ISM). Starting with ISM v9, the version of ISM imported is no longer normative.
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V7)[17]	Depends on Need To Know (NTK) markings. Starting with NTK v7, the version of NTK Imported is no longer normative, so any NTK Version 7 or above may be used.
XML Data Encoding Specification for Enterprise Data Header (IC-EDH XML.V1+)[6]	Depends on Enterprise Data Header (EDH) specification. Starting with EDH v1, the version of EDH imported is no longer normative, so any EDH version 1 or above may be used.
XML Data Encoding Specification for Access Rights and Handling (ARH.XML.V1+)[2]	Depends on Access Rights and Handling (ARH) markings. Starting with ARH v1, the version of ARH imported is no longer normative, so any ARH version 1 or above may be used.
Department of Defense Discovery Metadata Specification (DDMS V5)[3]	Depends on DoD Discovery Metadata Specification (DDMS). The dependence on DDMS is normative.

Name	Dependency Description
Information Resource Metadata (IRM.XML.V11+)[14]	Depends on Information Resource Metadata (IRM). The dependence on IRM is normative.
Schematron[19]	Schematron — ISO/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 XSLT 2.0[26] query binding.
XSLT 2.0[26] implementation of Schematron[19] 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 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.
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the DOMEX CVEs is normative.

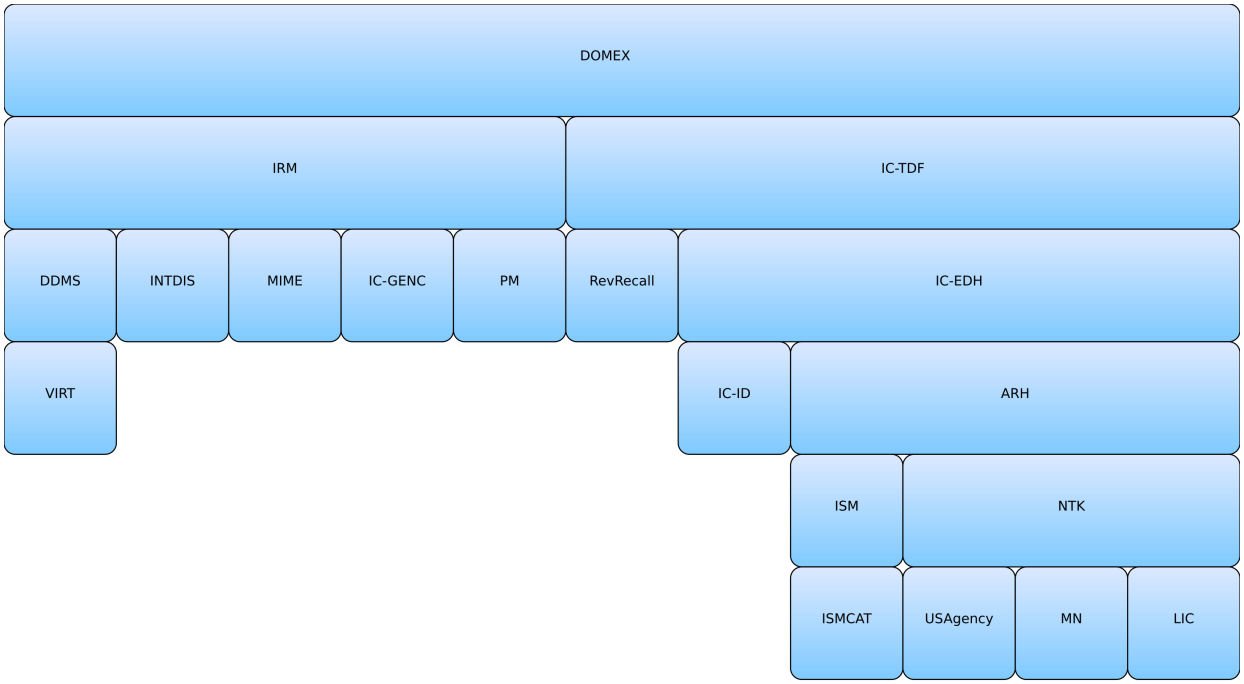

Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions of all transitive dependent specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumerations (CVEs) to validate and operate as intended.

Convenience packages convey all dependencies pre-packaged together and are tested as interoperable. When trying to mix and match versions that have not been pre-packaged together, there may be risk that a particular combination may not be compatible, especially when mixing with versions of specifications that were not available at the time of a specification's release.

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron[19] rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[13] is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.[24] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion**='9' to **@ism:DESVersion**='10' in the xsd:schema statement. The ability to import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications such as ISM CVE updates. The decoupling of dependency versions is not retroactive; see the dependency table for allowed dependency versions.

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

1.9 - Version Policies

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from “The Disposition of Names in an XML Namespace.”[20] This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 “Versioning and XML namespace policy” of “Architecture of the World Wide Web, Volume One.”[22]

In a fashion similar to DocBook there is a “version” attribute (i.e., **@DESVersion**, **@CESVersion**, **@TESVersion**, **@version**) defined in each namespace defined in an IC CIO specification used to capture the version number assigned to each revision of the specification. The **@DESVersion** attribute is the only indicator in an instance document as to what revision of a particular specification the author intended the instance to be valid. Since the namespace does not change, the “version” attribute is required to fully understand the instance document.

As changes to the specification are released, the version number captured in the “version” attribute increments. See Section 1.9.2 - Version Numbering for information on the numbering scheme.

This XML namespace policy only applies to the namespaces defined in this specification, any namespaces that are included by reference should define their own namespace policy.

1.9.2 - Version Numbering

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-MMM). This provides a temporal representation of when the specification was released. When the version number is used in the version attribute, the expression follows the Augmented Backus–Naur Form[1] below:

Version Format when used in the version attribute:

[1] Version : : = Year Month ["-" CustomizationSuffix]
[2] Year : : = 4(DIGIT)
[3] Month : : = 2(DIGIT)
[4] Customization Suffix : : = 1*27(ALPHA / DIGIT / "_")

Version in XML Lexicon

The following vocabulary helps explain the meaning of terms used in the version documentation, and it may further constrain the set of allowable values:

Version	The version number as it might be expressed in a DESVersion, CESVersion or other XML attribute for indicating the version being referenced.
Year	The four digit year from the version of the specification being referenced.
Month	The 2 digit month from the version of the specification being referenced.
CustomizationSuffix	An optional suffix used when customizing a version of a specification. This would be used to indicate that you have extended the specification in some fashion for a particular use case.

Chapter 2 - Development Guidance

2.1 - Relationship to Abstract Data Definition and other encodings

The relationship of the XML structures defined in this encoding specification to the abstract terms defined in the 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 - Document and Media Exploitation DOMEX Usage

DOMEX.XML is used in conjunction with TDF objects as structured assertions that contain information required for generating a Trusted Data Object (TDO) or Trusted Data Collection (TDC). The TDF.XML specification 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 one handling assertion, 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 specification when it contains:

- A structured assertion of scope TDO or TDC with a DOMEX element.
- 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.
- An assertion with a structured statement containing the IRM DES 2014-DEC.

- An assertion of scope payload (PAYL) with a structured statement containing a DDMS resource element.

The DDMS version 5 resource no longer contains all the metadata needed to stand alone. Instead, it generates a DDMS assertion that can be embedded in a TDC or TDO.

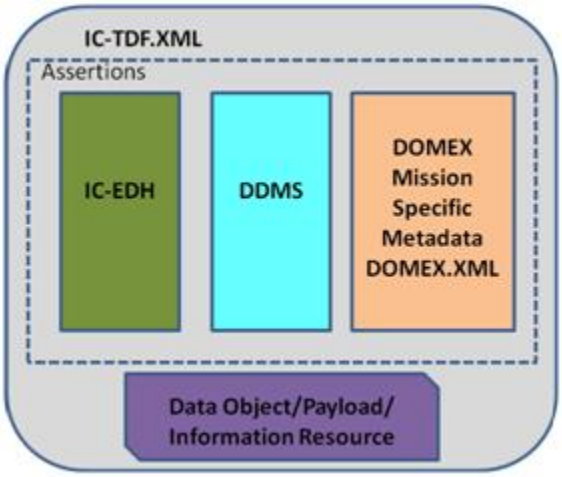

Figure 2 : TDF with Assertions

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 DDMS 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 **ddms:identifier**.

The diagram below shows expected use of IC specifications within a TDO and a DOMEX-specific metadata assertion. The use of the IC-EDH handling assertion and payload are required.

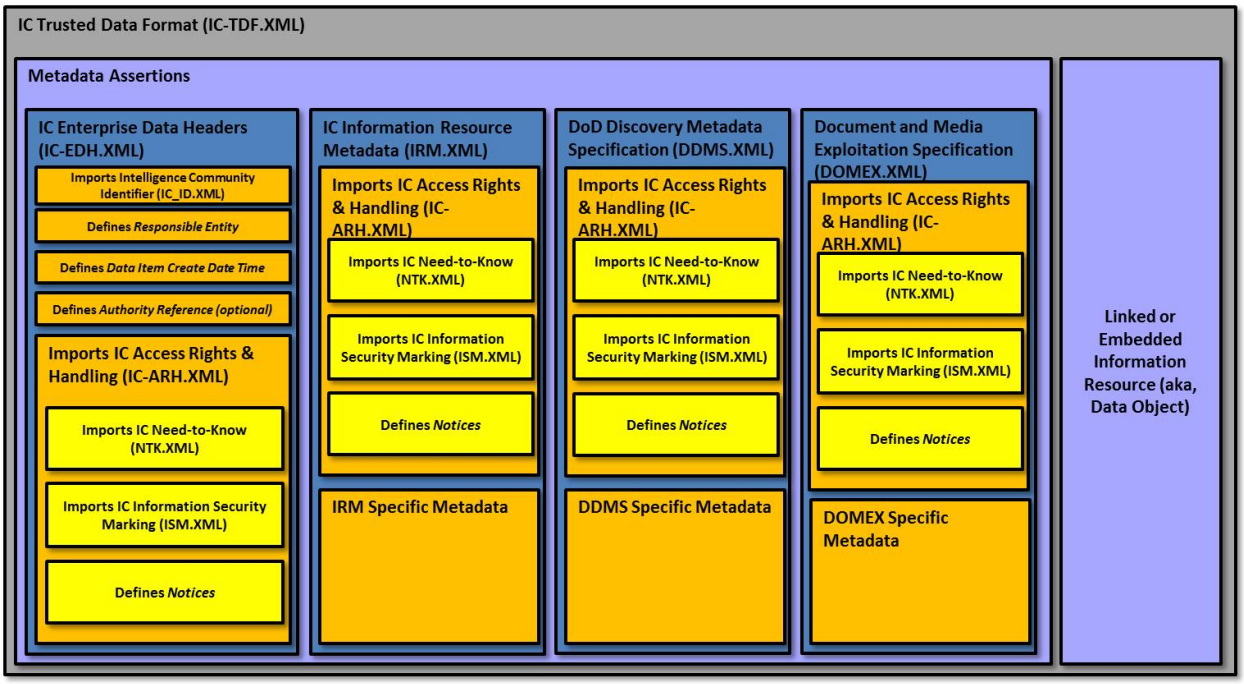

Figure 3 : TDO Format Overview

The EDH Assertion identifies the security, access rights and handling, notices, and need to know information for the TDO and the payload. The DDMS 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.

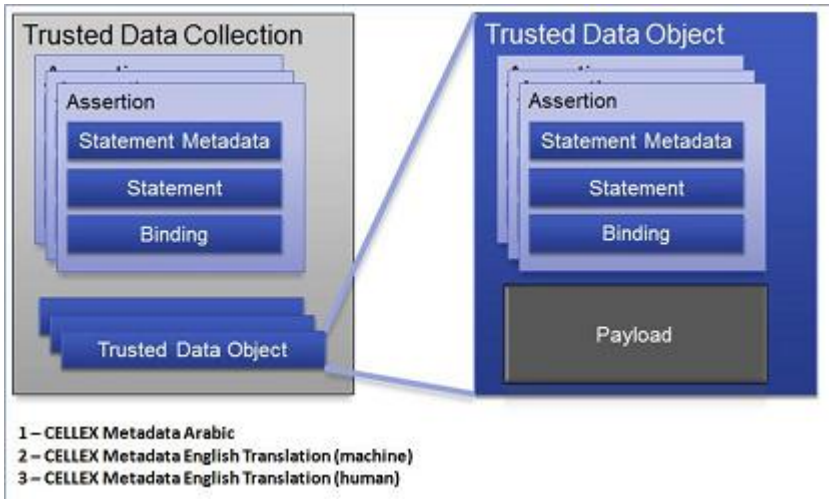

Figure 4 : TDC Format Overview

2.2.2 - Document and Media Exploitation XML Schema Namespaces

The DOMEX.XML schema contains unique namespaces to manage DOMEX metadata in logical blocks. 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*** namespace has multiple root elements: **acquisition, collectionDetails, subjectInformation, identity, equipment, facility, organization,** and **file.**

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.**

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.**

A DOMEX assertion may contain elements from all three namespaces depending on the object(s) described.

2.2.3 - *domex* Namespace Elements

The ***domex:*** **acquisition** element is contained in the structured statement of an assertion within a Trusted Data Object (TDO) with scope TDO or a Trusted Data Collection (TDC)) with scope TDC. In this context, the instance should be representative of the entire object including all variants. 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

The **collectionDetails** 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.

The **subjectInformation** 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.

The **facility** 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.

The **organization** 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.

The **equipment** element is used to specify metadata about equipment when a 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.

The **file** 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).

2.2.4 - *Identity* Namespace Elements

The **identity** element is the root element and is used to specify metadata about a person when a person is the subject of an acquisition. It is also used to specify content and analytic identity metadata extracted from the file object or added through content management and analysis.

2.2.5 - *cr* Namespace Elements

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

2.2.6 - Document and Media Exploitation (DOMEX) Assertion and Trusted Data Objects

Trusted Data Objects and Trusted Data Collections adhere to the IC Trusted Data Format XML schema, and the DOMEX metadata is contained in a DOMEX assertion within the TDO or TDC. The DOMEX assertion adheres to the DOMEX.xsd.

2.2.7 - Use of DDMS Resource

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

Table 3 - ddms:resource

ddms:resource	Additional Clarification/Guidance
./title	DDMS does not permit the specification of language for the DDMS title element. Therefore, the translated and descriptive title elements will remain in the DOMEX assertion. Implementers are advised that the DDMS title element must be a human readable name identifying the DOMEX object. The DDMS 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. Examples: domex:acquisition ./title[@type=Translated] or ./title[@type=Descriptive]

ddms:resource	Additional Clarification/Guidance
./identifier	DOMEX identifiers will use the DDMS resource element ddms:identifier with a qualifier and value. Qualifiers may include domexID, collectionId, harmonyNumber, and hashValue. Note: The inclusion of one identifier element is mandatory; there is no upper bound on the number of identifier elements.
./publisher	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.
./acquiredOn	The DDMS element acquiredOn is used for the date the original DOMEX object was obtained, acquired, or collected.
./subjectCoverage/keyword	Keywords about the DOMEX object. Generic or specific terms representing the content of the original DOMEX object.
./geospatialCoverage/boundingGeometry/ tspi:Point	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.
./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

2.2.8 - 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 DDMS construct **Combined Date** that supports a range of date representations.[3] 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 UTC (Coordinated Universal Time), with a special UTC designator (“Z”).

The **documentDate** element uses the DDMS construct ApproximableDate[3] that allows for the date to be specified in terms of approximate start and end dates or in a descriptive way.

2.2.9 - Specification of Locations

Location elements in DOMEX XML including: **collectionLocationCoordinates, gpsCoordinates,** and **location** use the Time-Space-Position Information (TSPI) version 2.0-compliant structures.[21] This permits the DOMEX definition of geospatial concepts to be consistent with DDMS version 5,[3] 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° <= longitude <= +180°; 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 DDMS postalAddress construct.[3]

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body for resolution. Rendering constraint rules define constraints on the display and rendering of documents. While expressed in a similar manner to the data validation constraint rules, 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 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by authoritative guidance. These rules will be expanded and modified as the model matures, tradecraft changes, and as applicable security marking 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.

3.3 - Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the encoding specification artifacts wherever they are located.

3.4 - Constraint Terminology

For the purposes of this document, the following statements apply:

- The term "is specified" indicates that an attribute is applied to an element and the attribute has a non-null value.
- The term "must be specified" indicates that an attribute MUST be applied to an element and the attribute MUST have a non-null value.
- The term "is not specified" indicates that an attribute is not applied to an element, or an attribute is applied to an element and the attribute has a null value.

- The term “must not be specified” indicates that an attribute MUST NOT be applied to an element.

3.5 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning.” An “Error” is more severe and is indicative of a clear violation of a constraint rule, which would be likely to have a significant impact on the quality of a document. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

Each system responsible for processing a document (e.g., create, modify, transform, or exchange) MUST make a mission-appropriate decision about using a document with errors or warnings based on mission needs.

3.6 - Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are “for official use only.”(FOUO) IDs from 20001 to 30000 are reserved for “Secret” rules and 30001 and above for more classified rules. DOMEX.XML data validation constraint rule IDs are prefixed with “DOMEX-ID-”.

As the constraint rules are managed over time, IDs from deleted rules will not be reused.

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

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.

3.7.2 - Schematron

Schematron[19] is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document MUST meet, 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, and 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.

For better understanding, the Schematron[19] rules for this specification may be executed in *Oxygen®* [18] or with an XSLT 2.0[26]-compliant processor using the XSLT 2.0[26] transforms in the

Schematron implementation from Rick Jelliffe (see XSLT 2.0 implementation of Schematron by Rick Jelliffe in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0[25] and XSLT 2.0[26] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:[16]

> By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this.

Note

For convenience, the specification package provides the XSLT 2.0[26] implementation of Schematron[19] along with a compiled version of the rules.

3.7.3 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content, meaning elements can be empty or null. According to this specification, all required elements (and certain conditional elements) MUST have content, other than white space.[1] Elements, which are allowed to only have text content, MUST have text content specified.

3.7.4 - 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 1.7 - Dependencies.

3.7.5 - Value Enumeration Constraints

Several elements and attributes of the DOMEX.XML model use CVEs 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.

[1] “White space” is defined in XML 1.0[23] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

3.7.6 - Additional Constraints

3.7.6.1 - 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.

3.7.7 - Constraint Rules

The detailed constraint rules for the DOMEX.XML schema can be found in a separate document inside the SchematronGuide 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 SchematronGuide.

3.8 - Data Rendering Constraint Rules

3.8.1 - 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.

3.8.2 - 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.			

Chapter 4 - Conformance Validation

An instance document conforms with this specification if it passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

4.1 - Schema Validation

An instance document MUST comply with the schemas for this specification and this specification's dependencies, and schema validation SHOULD occur prior to other validation steps. If schema validation fails, results from later steps may be indeterminate.

4.2 - Business Rule Validation

An instance document MUST comply with the business rules expressed in this specification. The business rules in this specification are expressed in Schematron, but 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. 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.

Chapter 5 - Generated Guides

5.1 - Schema Guide

The guide was generated with a commercially available product named *oXygen®,* [18] produced by SyncRO Soft.

The guide provides an interactive index to:

- Global Elements and Attributes
- Local Elements and Attributes
- Simple and Complex Types
- Groups and Attribute Groups
- Referenced Schemas

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of the master HTML file *SchemaGuide.html* with supporting graphics.

5.2 - Schematron Guide

The detailed description and reference documentation for the DOMEX.XML Schematron rules can be found in a separate document named *DOMEX_Rules.pdf*, which is located inside the

SchematronGuide directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Appendix A Feature Summary

The following table summarizes major features by version for DOMEX and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

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

DOMEX Feature Comparison				
Required date	**Feature**	**V1**	**V2**	**V2015-AUG**
	DOMEX Agency CVE	N	F	F
	Hash Values	N	N	F
	Legacy File Types	N	N	F
	USB Device Info	N	N	F
	DOMEX Collections Descriptors	N	N	F
	Activity Identification	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	16 August 2013	Initial Release
2	14 March 2014	Routine revision to technical specification. For details of changes, see Section B.2 - V2 Change Summary
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.1 - V2015-AUG Change Summary

B.1 - 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 8 - 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 CVEnumFile-Type.	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.

Change	Artifacts Changed	Compatibility Notes
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.
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.2 - 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 9 - 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.

Change	Artifacts Changed	Compatibility Notes
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.
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 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.

Change	Artifacts Changed	Compatibility Notes
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.
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 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
ARH	Access Rights and Handling
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
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
GENC	Geopolitical Entities, Names, and Codes
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive

ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IRM	Information Resource Metadata
ISM	Information Security Markings
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology
NGIC	National Ground Intelligence Center
NMEC	National Media Exploitation Center
NSA	National Security Agency
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PAYL	Payload
PDF	Portable Document Format
PUBS	Intelligence Publications
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
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

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] ARH.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*.
Available online Intelink-TS at:http://go.ic.gov/Fub6Gnw
Available online Intelink-U at:http://purl.org/IC/Standards/ARH
Available online at:http://purl.org/IC/Standards/public

[3] DDMS V5
Department of Defense. *DoD Discovery Metadata Specification*. 5.
Available online at:http://go.ic.gov/IDsfIgi

[4] DoD Directive 3300.03
Secretary of Defense. *DoD Document and Media Exploitation (DOMEX)*. 3300.03. 11 January 2011.
Available online at:www.dtic.mil/whs/directives/corres/pdf/330003p.pdf

[5] IC ITE INC1 IMPL
Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at:http://go.ic.gov/4X6TOc1

[6] 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:http://go.ic.gov/TQjVx3d
Available online Intelink-U at:http://purl.org/IC/Standards/EDH
Available online at:http://purl.org/IC/Standards/public

[7] IC-TDF.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (TDF.XML)*.
Available online Intelink-TS at:http://go.ic.gov/sonBSai
Available online Intelink-U at:http://purl.org/IC/Standards/TDF
Available online at:http://purl.org/IC/Standards/public

[8] 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

[9] 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:http://go.ic.gov/5Ot5sbK
Available online at:http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[10] ICPG 710.1
Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at:http://go.ic.gov/JztUoEQ

[11] 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: http://go.ic.gov/sLKNq3N
Available online Intelink-U at: http://www.purl.org/ic/standards/policy/ICS500-20

[12] ICS 500-21
Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online Intelink-TS at: http://go.ic.gov/cWyv9nw
Available online Intelink-U at: http://www.purl.org/ic/standards/policy/ICS500-21

[13] 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

[14] IRM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Resource Metadata (IRM.XML)*.
Available online Intelink-TS at:http://go.ic.gov/9g8Osir
Available online Intelink-U at:http://purl.org/IC/Standards/IRM
Available online at:http://purl.org/IC/Standards/public

[15] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.
Available online Intelink-TS at:http://go.ic.gov/3oipfOY
Available online Intelink-U at:http://purl.org/IC/Standards/ISM
Available online at:http://purl.org/IC/Standards/public

[16] Jelliffe
Richard Alan Jelliffe. *FAQ*. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?.
Available online at: http://www.schematron.com

[17] NTK.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.

Available online Intelink-TS at:http://go.ic.gov/YLXsYUX
Available online Intelink-U at:http://purl.org/IC/Standards/NTK
Available online at:http://purl.org/IC/Standards/public

[18] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*.
Available online at: http://www.oxygenxml.com/

[19] 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/

[20] TAG-9-Jan-2006
W3C Technical Architecture Group (TAG). *The Disposition of Names in an XML Namespace*. 9 January 2006.
Available online at:http://www.w3.org/2001/tag/doc/namespaceState.html

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

[22] WEBARCH-15-Dec-2004
W3C. *Architecture of the World Wide Web, Volume One*. 15 December 2004.
Available online at:http://www.w3.org/TR/webarch

[23] XML 1.0
World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0, Second Edition*. W3C, 6 October 2000.
Available online at:http://www.w3.org/TR/2000/REC-xml-20001006

[24] XML Catalogs
The Organization for the Advancement of Structured Information Standards [OASIS]. *XML Catalogs*. Committee Specification 06 Aug 2001.
Available online at:https://www.oasis-open.org/committees/entity/spec-2001-08-06.html

[25] XPath2
World Wide Web Consortium (W3C). *XML Path Language (XPath) 2.0 (Second Edition)*. W3C Recommendation 14 December 2010 (Link errors corrected 3 January 2011).
Available online at:http://www.w3.org/TR/xpath20/

[26] 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 ICtechnical 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: http://purl.org/ic/standards/public

Intelshare: http://purl.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@ugov.gov.

Appendix F IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO 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 OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO 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 IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.[11]