An Intelligence Community Technical Specification

Intelligence Community Abstract Data Definition Version 2 (IC.ADD.V2)

9 August 2011

Table of Contents

Executive Summary iv
Chapter 1 - Introduction 1
1.1 - Purpose 1
1.2 - Scope 1
1.3 - Implementation 1
1.4 - Normative and Informative Components 1
1.5 - Typographic conventions 1
1.6 - Data Encoding Specifications 2
Chapter 2 - Information Resource Description Data Elements 3
Chapter 3 - Information Security Marking Data Elements 7
3.1 - Data Elements 7
3.2 - Data Element Refinements 8
Chapter 4 - Publication Data Elements 11
4.1 - Data Elements – Publication Types 11
4.2 - Data Elements – Section Types 11
4.3 - Data Elements – Narrative Types 12
Chapter 5 - Source Reference Citation Data Elements 14
5.1 - Data Elements 14
5.2 - Data Element Refinements 15
Chapter 6 - Knowledge Organization System Data Elements 18
6.1 - Data Elements 18
6.2 - Data Element Refinements – KOS 19
6.3 - Data Element Refinements – KOS Metadata 20
6.4 - Data Element Refinements – Class/Property/Term Metadata 21
Chapter 7 - Knowledge Assertion Data Elements 23
7.1 - Data Elements 23
7.2 - Data Element Refinements – KA 23
7.3 - Data Element Refinements – KA Metadata 24
Appendix A - Change History 27
A.1 - V2 Change Summary 27
Appendix B - Acronyms 29
Appendix C - Bibliography 31
Appendix D - Points of Contact 34
Appendix E - IC CIO Approval Memo 35

List of Tables

Table 1 - Information Resource Description Data Elements 3
Table 2 - Information Security Marking Data Elements 7
Table 3 - Information Security Marking Data Elements 8
Table 4 - Publications Data Elements – Publication Types 11
Table 5 - Publications Data Elements – Section Types 11
Table 6 - Publications Data Elements – Narrative Types 12
Table 7 - Source Reference Citation Data Elements 14
Table 8 - Source Reference Citation Data Element Refinements 15
Table 9 - Knowledge Organization System Data Elements 18
Table 10 - Data Element Refinements – KOS 19
Table 11 - Data Element Refinements – KOS Metadata 20
Table 12 - Data Element Refinements – Class/Property/Term Metadata 21
Table 13 - Knowledge Assertion Data Elements 23
Table 14 - Data Element Refinements – Knowledge Assertion 24
Table 15 - Data Element Refinements – Knowledge Assertion Metadata 25
Table 16 - DES Version Identifier History 27
Table 17 - Change Summary 27
Table 18 - Acronyms 29

Executive Summary

ICD 500: *Director of National Intelligence Chief Information Officer* defines the IC Chief Information Officer (IC CIO's) responsibility to establish common 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 Intelligence Community (IC) as established in relevant law, policy, and directives.

This document falls into the category of common IT standards and defines a collection of abstract data elements, which constitute a top-down view of the types of data and metadata that are important to the IC.

Chapter 1 - Introduction

1.1 - Purpose

This document, the *Intelligence Community Abstract Data Definition* (IC.ADD) defines, at an abstract level, the types of data and metadata that are important to the Intelligence Community (IC). Selected or developed physical Data Encoding Specifications established by the IC map to these abstract data elements providing a means to relate or translate different physical data encodings. These abstract data elements are not meant to be implementable within enterprise systems. IC elements should implement the physical Data Encoding Specifications that implement these abstract data elements. This document is simply a living artifact that codifies a collection of agreed-upon abstract data concepts.

1.2 - Scope

This document is applicable to intelligence data produced in the IC. Each group of data elements presented herein provides the relevant scope for that group. These data elements may have relevance outside the scope of intelligence data, but prior to applying outside of this scope, the definitions should be closely scrutinized and differences separately documented.

1.3 - Implementation

The abstract data elements defined herein are grouped into a number of categories based on their purpose. In some cases, definitions reference other data elements in different groupings. Some groups define data elements and a further refinement of those elements.

Each data element includes a name for the data element and a definition intended to convey a common understanding of the element. In cases where the data element was adopted from elsewhere, the definitions were expanded with IC-specific qualifiers, recommended uses, and encoding schemes where applicable. Additionally, a number of the element definitions suggest a controlled vocabulary for the respective data element values.

Additional data elements and groupings will be added over time to address the expanding list of data elements of common concern to the IC.

1.4 - Normative and Informative Components

This document is normative in its entirety, unless otherwise indicated.

1.5 - Typographic conventions

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 - Data Encoding Specifications

The abstract data elements defined herein are expanded, refined, modeled, and implemented as physical tagging structures found in Data Encoding Specifications (DESs). For example, the Date data element may be expanded and implemented as tagging elements called **DatePublished**, **DatePosted**, and **DateInfoCutoff**.

DESs are unique to specific file formats (e.g., XML, HTML, and Microsoft Word) and/or processing systems. DESs define data encoding-specific tagging elements (i.e., markup), element structures, element relationships, cardinality requirements, and permissible values for populating the elements (e.g., string, date, or a controlled vocabulary).

DESs are represented by a series of documentation and digital artifacts. These artifacts include taxonomies, controlled vocabularies, conceptual data models, data element dictionaries, validation and constraint rules, transformations and mappings, schemas, and developer's guidance.

Requirements unique to specific mission and business interests can be accommodated by adding data elements or prescribing business rules consistent with IC policy guidance for information standards governance.

Chapter 2 - Information Resource Description Data Elements

Scope: The set of data elements defined in this chapter is built upon the International Organization for Standardization (ISO) release (ISO 15836) of the Dublin Core Metadata Element Set (DC MES) and may be considered a profile of the DC MES. The DC MES was extended (or profiled) to address the unique requirements of the IC's national security mission. The Dublin Core Metadata Initiative's (DCMI) goals are important to the IC since they support increased visibility, easier discovery, and enhanced understanding of intelligence information resources across mission domains.

These abstract data elements reflect extensive collaborative efforts within the IC and other US Government organizations, such as the Department of Defense and the Department of Justice. These data elements serve as a foundation for supporting data interoperability as they codify the agreeable data concepts to be implemented in IC Data Encoding Specifications and exchanged within intelligence processing systems.

Data elements labeled with the DCMI designation "(DCMI)" adopt the Dublin Core element definitions, unchanged from the ISO standard. IC-specific expansions of the DCMI definitions are labeled **IC Expansion**. In the context of this section, the term resource in the DCMI definitions pertains to an intelligence or intelligence-related information resource (e.g., document, image, or message).

Table 1 - Information Resource Description Data Elements

Data Element	Definition
Contributor (DCMI)	An entity responsible for making contributions to the resource. Examples of Contributor include a person, an organization, or a service. Typically, the name of a Contributor should be used to indicate the entity.
Coverage (DCMI)	The spatial, temporal [or virtual] topic of the resource, the spatial [or virtual] applicability of the resource, or the jurisdiction under which the resource is relevant. A spatial topic may be a named place or a location specified by its geographic coordinates. A temporal period may be a named period, date, or date range. A jurisdiction may be a named administrative entity or a geographic place to which the resource applies. Recommended best practice is to use a controlled vocabulary such as the Thesaurus of Geographic Names (TGN) Where appropriate, named places or time periods can be used in preference to numeric identifiers such as sets of coordinates or date ranges.
Creator (DCMI)	An entity primarily responsible for making the resource. Examples of Creator include a person, an organization, or a service. Typically, the name of a creator should be used to indicate the entity.
Date (DCMI)	A point or period of time associated with an event in the lifecycle of the resource.

Data Element	Definition
	Date may be used to express temporal information at any level of granularity. Recommended best practice is to use an encoding scheme, such as the World Wide Web Consortium Date Time Format (W3CDTF) profile of ISO 8601. **IC Expansion:** Typically, date will be associated with the creation or availability of the resource.
Description (DCMI)	An account of the resource. Description may include but is not limited to an abstract, a table of contents, a graphical representation, or a free-text account of the resource.
Format (DCMI)	The file format, physical medium, or dimensions of the resource. Examples of dimensions include size and duration. Recommended best practice is to use a controlled vocabulary such as the list of Internet Media Types (MIME). **IC Expansion:** Format may be used to identify the software, hardware, or other equipment needed to display or operate the resource.
Identifier (DCMI)	An unambiguous reference to the resource within a given context. Recommended best practice is to identify the resource by means of a string conforming to a formal identification system. **IC Expansion:** Formal identification systems include but are not limited to the Uniform Resource Identifier (URI) (including the Uniform Resource Locator (URL)), the Digital Object Identifier (DOI), and the International Standard Book Number (ISBN).
Language (DCMI)	A language of the resource. Recommended best practice is to use a controlled vocabulary such as RFC 3066, Tags for the Identification of Languages, which specifies use of ISO 639-2, Codes for the Representation of Names of Languages, three character language code, with an optional appended ISO 3166-1, Codes for the representation of names of countries and their subdivisions, two character country code. For example: “eng-US” or “eng-UK.”
Publisher (DCMI)	An entity responsible for making the resource available. Examples of a Publisher include a person, an organization, or a service. Typically, the name of a publisher should be used to indicate the entity.
Records Management Information	Required information primarily supporting federal record keeping requirements.

Data Element	Definition
Relation (DCMI)	A related resource. Recommended best practice is to identify the referenced resource by means of a label or number conforming to a formal identification system.
Resource Security Mark	The overall security classification and security handling instructions carried by the resource. Resource Security Mark applies to the resource-level classification, SCI controls, dissemination controls, non-IC markings, and other security provisions prescribed by Executive Order 13526, as amended, the Information Security Oversight Office (ISOO) Directive 1 of the National Archives and Records Administration, and the Intelligence Community marking registry maintained by the Controlled Access Program Coordination Office (CAPCO). These values are prominently presented, in the case of intelligence publications, at the top and bottom of every page and in other specified locations. Chapter 3 - Information Security Marking Data Elements for refinements of this data element.
Rights (DCMI)	Information about rights held in and over the resource. **IC Expansion:** Typically, Rights will contain a rights management statement for the resource, or reference a service providing such information. Rights information often encompasses Intellectual Property Rights (IPR), copyright, and various property rights. If Rights is absent, no assumptions may be made about any rights held in or over the resource.
Source (DCMI)	The resource from which the described resource is derived. The described resource may be derived from the related resource in whole or in part. Recommended best practice is to identify the related resource by means of a string conforming to a formal identification system.
Subject (DCMI)	A topic of the resource. Typically, the topic will be represented using keywords, key phrases, or classification codes. Recommended best practice is to use a controlled vocabulary. To describe the spatial or temporal topic of the resource, use the Coverage element. **IC Expansion:** The virtual topic of the resource should also be described using the Coverage element.
Title (DCMI)	A name given to the resource. Typically, a Title will be a name by which the resource is formally known.

Data Element	Definition
Type (DCMI)	The nature or genre of the content of the resource. **IC Expansion:** The Type includes terms describing general categories, functions, genres, or aggregation levels for content. Examples of a Type include publication forms (e.g., reports or articles) and intelligence disciplines (e.g., SIGINT, MASINT, HUMINT). Recommended best practice is to use a controlled vocabulary. To describe the file format, physical medium, or dimensions of the resource, use the Format element.

Chapter 3 - Information Security Marking Data Elements

Scope: These data elements support Executive Order (EO) 13526, *Classified National Security Information* which “prescribes a uniform system for classifying, safeguarding, and declassifying national security information”, across national security disciplines, networks, services, and data.

These data elements serve as a critical bridge between the security marking requirements defined by the National Archives and Records Administration (NARA), Information Security Oversight Office (ISOO) and the IC security markings register maintained by the Office of the Director of National Intelligence (ODNI), Controlled Access Program Coordination Office (CAPCO), and information technology solutions that implement structured security marking metadata.

These data elements were developed to enable important advances designed to simultaneously improve and simplify the marking and handling of information at both the information product and portion-levels across the full range of security classifications. Upon this foundation:

- User interfaces for information security marking will be developed.
- Automated formatting of CAPCO-compliant portion marks, security banners, and classification/declassification blocks will be designed and built.
- Cross-domain security capabilities will be developed and deployed.

3.1 - Data Elements

The data elements defined in this section consist of: the overall security marking of an information product, the classification/declassification instructions of a product, and the portion markings within that product. These three data elements are further refined in the following section.

Table 2 - Information Security Marking Data Elements

Data Element	Definition
Notice	A statement about an information resource designed to inform those accessing the resource. The statement may provide information about handling or protecting the resource, additional information about interpreting the content, use of the resource, etc.
Portion Security Mark	The security classification carried by an individual portion or block of narrative or media, such as a title, paragraph, table, list, media, or caption. When displayed, these values are prominently presented at the beginning of the respective portion, are enclosed in parentheses, and utilize the same separators as the overall classification markings of the information resource. When encoded, they are typically associated with a portion structure (see Chapter 4 - Publication Data Elements).

Data Element	Definition
Resource Classification Declassification Mark	Classification information and declassification instructions associated with a classified resource based on either an original or derivative classification decision(s). When displayed, these values are prominently presented with specific labels and formatting on the first page of a document. When encoded, they are typically associated with an upper-level document structure or information resource metadata description (see Chapter 2 - Information Resource Description Data Elements).
Resource Security Mark	The overall security classification and security handling instructions carried by the resource. When displayed, these values are prominently presented, in the case of intelligence publications, at the top and bottom of every page and in other specified locations. When encoded, they are typically associated with an upper-level document structure or information resource metadata description (see Chapter 2 - Information Resource Description Data Elements).

3.2 - Data Element Refinements

The following data elements refine each of the data elements defined in Table 2: Information Security Marking Data Elements.

Table 3 - Information Security Marking Data Elements

Data Element Refinement	Definition
Applicable Ruleset	The rule sets that a document asserts compliance with.
Atomic Energy Act (AEA) Information Markings	One or more indicators identifying information controlled under the Atomic Energy Act.
Classification	A single indicator of the highest level of classification applicable to an information resource or portion within the domain of classified national security information. The Classification element is always used in conjunction with the Owner Producer element. Taken together, the two elements specify the classification category and the type of classification (US, non-US, or Joint).
Classification Reason	One or more reason indicators or explanatory text describing the basis for an original classification decision.
Classified By	The identity, by name or personal identifier, and position title of the original classification authority for a resource.
Compilation Reason	The reason that a portion or resource is marked with a higher and/ or more restrictive mark than its components would indicate. For example this would document why 3 Unclassified bullet items form

Data Element Refinement	Definition
	a Secret List. Without this reason being noted the above-described document would be considered to be mismarked and over-classified.
Declassification Date	A specific year, month, and day upon which the information shall be automatically declassified if not properly exempted from automatic declassification.
Declassification Event	A description of an event upon which the information shall be automatically declassified if not properly exempted from automatic declassification.
Declassification Exemption	A single indicator describing an exemption to the nominal 25-year point for automatic declassification. This element may be used in conjunction with the Declassification Date or Declassification Event.
Derivatively Classified By	The identity, by name or personal identifier, of the derivative classification authority.
Derived From	A citation of the authoritative source(s) or reference to “Multiple Sources” of the classification markings used in a classified resource.
Display Only To	One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be displayed based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element.
Dissemination Controls	One or more indicators identifying the expansion or limitation on the distribution of information.
FGI Source Open	One or more indicators identifying information, which qualifies as foreign government information, for which the source(s) of the information is not concealed.
FGI Source Protected	A single indicator that information qualifies as foreign government information for which the source(s) of the information must be concealed. Within protected internal organizational spaces this element may be used to maintain a record of the one or more indicators identifying information which qualifies as foreign government information for which the source(s) of the information must be concealed. Measures must be taken prior to dissemination of the information to conceal the source(s) of the foreign government information.
Non-Intelligence Community Markings	One or more indicators of the expansion or limitation on the distribution of an information resource or portion within the domain of information originating from non-intelligence components.
Non-US Controls	One or more indicators of the expansion or limitation on the distribution of an information resource or portion within the domain of information originating from non-US components.

Data Element Refinement	Definition
Owner Producer	One or more indicators identifying the national government or international organization that have purview over the classification marking of an information resource or portion therein. This element is always used in conjunction with the Classification element. Taken together, the two elements specify the classification category and the type of classification (US, non-US, or Joint). Within protected internal organizational spaces this element may include one or more indicators identifying information which qualifies as foreign government information, for which the source(s) of the information must be concealed. Measures must be taken prior to dissemination of the information to conceal the source(s) of the foreign government information.
Point of Contact	An indicator identifying the entity contains a name and/or contact method for a specific point-of-contact requirement in a document.
Releasable To	One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be released based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element.
SCI Controls	One or more indicators identifying sensitive compartmented information control system(s).
Special-Access-Required Program Identifier	One or more indicators identifying the defense or intelligence programs for which special access is required.

Chapter 4 - Publication Data Elements

Scope: These data elements describe components commonly found in textual or mixed-media information products, most appropriately characterized as *publications*. Intelligence publications consist of various types of sections and narrative objects packaged together into different types of publications. Many of these data elements are tightly woven together with other sets of data elements described elsewhere in this document, such as information resource metadata and information security markings.

These data elements were developed to provide the foundation for the exchange and reuse of intelligence publications regardless of where and how they were originally produced. These data elements are designed to support a wide range of advanced information services that will help find, organize, analyze, and manage commonly encoded intelligence information.

4.1 - Data Elements – Publication Types

These data elements represent the most common, general-purpose publication types. These data elements may be refined through the application of the data elements described in Chapter 2 - Information Resource Description Data Elements , which includes overall resource security markings.

Table 4 - Publications Data Elements – Publication Types

Data Element	Definition
Article	Used for news or journalist reporting and for other publications with little or no front or rear matter.
Report	Used for publications with extensive front and rear matter, and body matter that is subdivided into parts, chapters, and/or sections.

4.2 - Data Elements – Section Types

These data elements represent the common organizational structures (e.g., sections) within publications. These data elements may be refined through the application of the data elements described in Chapter 3 - Information Security Marking Data Elements .

Table 5 - Publications Data Elements – Section Types

Data Element* pre-defined section	Definition
Appendix	A collection of supplementary material usually placed after the main body of writing.
Attachments	A section that is appended or attached to a main document, usually a correspondence document.
Bibliography*	A list of the works referenced in the body of a publication or consulted by the author in its production.

Data Element* pre-defined section	Definition
Collect Source	Information about sources from which intelligence is collected
Distribution List*	A series of addresses or routing symbols for distribution of a publication.
Glossary*	A list of often difficult or specialized words with their definitions.
Index*	An alphabetized list of names, places, and/or subjects that facilitates reference to the body of the publication.
Key Findings*	Key conclusions reached after examination or investigation.
Preface*	An introductory section offering information about the source of the request for a report, who wrote the report, the source of the information, how the study was conducted, etc. This element does not specifically address the scope of the report.
Scope*	The extent or range of application, aim or purpose of a report.
Section	Generic subdivision of an article, report, or correspondence.
Section Title	Generic section's primary title.
Sidebar	A short article that is substantially parallel to the text of the main report but not directly a part of it.
Summary*	A comprehensive and usually brief abstract, recapitulation, or compendium of facts, statements, and/or findings.
Table of Contents*	Listing of sections, figures tables or other specially titled content listed by title within the publication and pointer to the content.

4.3 - Data Elements – Narrative Types

These data elements represent the most common narrative (or prose) content of a publication. These data elements may be further refined through the application of the data elements described in Chapter 3 - Information Security Marking Data Elements .

Table 6 - Publications Data Elements – Narrative Types

Data Element	Definition
Assertion	A complex structure used to highlight content and associate special emphasis (via formatting), semantic understanding (via tagging, see Chapter 7 - Knowledge Assertion Data Elements) or ancillary value-added information (via hyperlink).
Equation	A complex structure representing a formula or an expression, such as a mathematical or chemical equation.
Footnote	A note that comments on—or cites a reference for—a designated part of the content, usually presented inline, at the bottom of the page, or at the end of a publication.
List	Series of items representing distinct but related thoughts written together in a meaningful grouping or sequence.

Data Element	Definition
Media Resource	Complex structure including a form of presentable media (e.g., graphic, animation, video) and some form of unique identification (e.g., title) or clarification (e.g., legend).
Note	Comment or explanation further clarifying surrounding content.
Paragraph	A distinct portion of written matter dealing with a particular idea.
Quote	Passage copied verbatim from a book, speech or other source that is properly referenced.
Source Citation	Bibliographic citation specialized to identify information sources necessary to substantiate analysis.
Table	Complex structure including a two-dimensional list organized into a grid containing rows and columns with special presentation characteristics and some form of unique identification (e.g., title).

Chapter 5 - Source Reference Citation Data Elements

Scope: The term source reference citation refers to a bibliographic citation of prior intelligence data used to substantiate analytic judgments. Consistent with Intelligence Community Directive (ICD) 206, *Sourcing Requirements for Disseminated Intelligence Products*, the data elements defined herein are the essential components of a source reference citation necessary to refer to all significant and substantive reporting or other information upon which analytic judgment, assessments, estimates, or confidence levels depend.

These data elements were designed to support the consistent application, display, and use of source reference citations, which will improve discovery, sharing, and the exchange of intelligence between the collection, exploitation, analysis, and dissemination functions of the intelligence process. Source reference citations help:

- Consumers locate and review prior intelligence data upon which analytic judgments are based;
- Collectors and producers systematically analyze how and how often intelligence data is referenced; and
- Consumers identify analytic judgments impacted when prior intelligence data is modified, rescinded, or discredited.

5.1 - Data Elements

These data elements include a cited information resource from which intelligence analysis is based and a reference citation for the cited information resource.

Data elements labeled with the DCMI designation “(DCMI)” adopt the Dublin Core element definitions, unchanged from the ISO standard. IC-specific expansions of the DCMI definitions are labeled **IC Expansion**. In the context of this section, the term *resource* in the DCMI definitions pertains to an intelligence or intelligence-related information resource (e.g., document, image, or message).

Table 7 - Source Reference Citation Data Elements

Data Element	Definition
Bibliographic Resource (DCMI)	A book, article, or other documentary resource. **IC Expansion:** In the context of source reference citations, a bibliographic resource is all significant and substantive reporting or other information upon which analytic judgment, assessments, estimates, or confidence levels depend. An intelligence product may be derived from one or more source references in whole or in part. Recommended best practice is to identify a related information resource by means of a formal identification system.
Bibliographic Citation (DCMI)	A bibliographic reference for the [cited] resource. **IC Expansion:** A special type of bibliographic reference (i.e., a formal identification system) unique to the intelligence discipline that contains

Data Element	Definition
	pertinent information resource metadata and details of the extent of the information being referenced. In accordance with ICD 206, source reference citations are to be listed in a special section at the end of intelligence products.

5.2 - Data Element Refinements

The following data elements refine the Bibliographic Citation data element defined in Table 7: Source Reference Citation Data Elements.

In the context of this section, the term resource in the DCMI definitions pertains to an intelligence or intelligence-related information resource (e.g., document, image, or message).

Table 8 - Source Reference Citation Data Element Refinements

Data Element Refinement	Definition
Citation Security Mark	Classification marking used for the overall Bibliographic Citation. This is the citation's portion mark as displayed in the bibliography or collection of source references.
Consulted	A date and time when a cited resource was used as a basis for analytic judgment.
Creator (DCMI)	An entity primarily responsible for making the [cited] resource. **IC Expansion:** The Creator can represent an author and/or coauthor and/or point of contact for the cited resource. The entity must be from or associated with the originating organization defined by the Publisher. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.
Date of Information	A date, time range, or time period representing the relative currency of the specific information cited.
Identifier (DCMI)	An unambiguous reference to the [cited] resource within a given context. **IC Expansion:** Recommended best practice is to identify a related information resource by means of a formal identification system. Examples might include a report serial number, document name or number, image frame identification code, or an organization internal identification or tracking number.
Issued (DCMI)	Date of formal issuance (e.g., publication) of the [cited] resource.
Link	A hyperlink to the cited resource. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.

Data Element Refinement	Definition
Publisher (DCMI)	An entity responsible for making the [cited] resource available. **IC Expansion:** An IC element, national government, international organization, or open-source owner(s) and/or producer(s) of a cited resource. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.
Segment Referenced	An identifier or description of the extent of the cited resource. Typically includes a form of label (e.g., a section or paragraph number, image feature, page number or range, video frame or range, etc.), possibly the classification of the extent, and possibly a link into the cited resource. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.
Sourced Content	A word, phrase, sentence, or other contiguous text string for which attribution is being cited. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.
Source Descriptor	An explanation of factors contained in the cited resource or publicly available information that the producing organization assesses may affect the quality or reliability of the information in the specific cited resource. Factors may include, but are not necessarily limited to, completeness, precision or technical quality, context, or age/currency of the information. In the case of human sources, this explanation may include information that describes the level of access, past reporting record, or potential biases (e.g., political, personal, professional, or religious affiliations). If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.
Source Security Mark	Overall classification marking of the cited resource. As the resource could originate from the US or another country, the Source Security Mark should represent an appropriate US marking or an original non-US marking. The originating country of the classification marking should also be recorded.

Data Element Refinement	Definition
Title (DCMI)	A primary title of the [cited] resource. **IC Expansion:** There may be multiple titles associated with a given cited resource, especially if the resource is published as part of a larger compilation of materials. Titles associated with a publication, journal, series, or edition may be necessary to uniquely indentify the cited resource. Recommended best practice is to provide the cited resource's title, possibly an alternative title if one exists, and to provide additional titles of the larger compilations when necessary. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.
Type (DCMI)	The nature or genre of the content of the [cited] resource. **IC Expansion:** The Type includes terms describing general categories, functions, genres, or aggregation levels for content. Examples of Type include publication form (e.g., book, periodical, report, or article), online publication (e.g., Internet site, web page, blog, or wiki), or intelligence discipline (e.g., SIGINT, MASINT, HUMINT). Recommended best practice is to use a controlled vocabulary. If applicable, data associated with this concept should be classification marked and appropriate rules for displaying the marking or for influencing the value or display of the Citation Security Mark should be followed.

Chapter 6 - Knowledge Organization System Data Elements

Scope: A *Knowledge Organization System* (KOS) is a scheme for organizing information and promoting knowledge management. When KOSs are consistently developed and applied, they improve the discovery, sharing, and exchange of intelligence information between the collection, exploitation, analysis, and dissemination functions of the intelligence process.

Specifically, KOSs enable syntactic and semantic data interoperability in the form of a common, computer-processable understanding of intelligence information. Syntactic and semantic data interoperability are mission-critical capabilities necessary for intelligence information integration, analysis, correlation, and discovery.

These data elements and the corresponding definitions and constraints were developed to be the fundamental building blocks for consistent development and application of IC enterprise KOS encoding specifications as well as specific KOS instances.

KOSs are targeted to help organize knowledge about *things*. The KOS data elements are tied to two kinds of things:

- Entity. An *entity* is something with distinct, independent existence in the real world, either concrete or abstract. The term *entity* may be used for the thing in the real world, or alternatively it may be used for a representation of the thing in some information system. Entities represented in information systems are sometimes called *knowledge objects*, *semantic knowledge objects*, *semantic objects*, or simply *objects*.
- Event. An *event* is something that happens or happened in the real world at a specific time and place, an occurrence. The term *event* may be used for the occurrence in the real world, or alternatively it may be used for a representation of the occurrence in some information system.

6.1 - Data Elements

These data elements include a Knowledge Organization System and metadata about that Knowledge Organization System.

Table 9 - Knowledge Organization System Data Elements

Data Element	Definition
Knowledge Organization System	A scheme used for organizing information and promoting knowledge management. Two categories of Knowledge Organization System that are applicable to the IC are *controlled vocabularies* and *ontologies*. Knowledge Organization Systems may be used for specifying the meaning of Knowledge Assertions (see Chapter 7 - Knowledge Assertion Data Elements).
Knowledge Organization	Information that provides data about a Knowledge Organization System, but is not the content of the Knowledge Organization System.

Data Element	Definition
System Metadata	

6.2 - Data Element Refinements – KOS

The following data elements refine the Knowledge Organization System data element defined in Table 9: Knowledge Organization System Data Elements.

Table 10 - Data Element Refinements – KOS

Data Element Refinement	Definition
Class	A grouping of a number of entities or events (things) regarded as forming a group by reason of common properties, characteristics, qualities, or traits. A Class is specified by a label and a set of properties indicating state and behavior. With the exception of the top-level Classes, each Class is declared to be a child Class of another Class, including classes that are defined in other KOSs. The nature of the parent/child relationship, whether specialization or meronymy, is explicitly stated. The properties of a Class consist of those inherited from the parent Class plus any additional properties that might distinguish it from peer Classes (other Classes with the same parent Class).
Class/Property/ Term Metadata	Information that provides data about a Class, Property, or Term, but is not the content of the Class, Property, or Term.
Property	Some quality that all entities or events that are instances (members) of a Class possess. In a Knowledge Organization System there are two kinds of properties: *attributes* and *relationships*, distinguished by the kind of value the Property may assume. The value of an attribute must be a quantitative or qualitative characteristic type (e.g., a string, a number, a Boolean, a quantity with units, a symbol, or a reference) and can be restricted to a set of allowed values (a *controlled vocabulary*). The value of a relationship must be an instance of another entity or event.
Term	A linguistic form, such as a word, a phrase, an abbreviation, or a definition, used in a specific context. Terms may be related to one another, such as synonyms, antonyms, broader-then, narrower-than, or (non-specific) related-to, as well as ordered according to some stated criterion. Terms may be associated with their recommended usage, such as preferred, alternate, or deprecated.

6.3 - Data Element Refinements – KOS Metadata

The following data elements refine the Knowledge Organization System Metadata data element defined in Table 9: Knowledge Organization System Data Elements.

Data elements labeled with the DCMI designation "(DCMI)" adopt the Dublin Core element definitions, unchanged from the ISO standard. IC-specific expansions of the DCMI definitions are labeled **IC Expansion**. In the context of this section, the term resource in the DCMI definitions pertains to a Knowledge Organization System.

Table 11 - Data Element Refinements – KOS Metadata

Data Element Refinement	Definition
Contributor (DCMI)	An entity [agent] responsible for making contributions to the resource. **IC Expansion:** Entity has a different meaning in context of Knowledge Organization Systems; therefore this DCMI definition refers more appropriately to an *agent*, such as a person, an organization, or a service. Typically, the name of a Contributor should be used to indicate the agent.
Creator (DCMI)	An entity [agent] primarily responsible for making the resource. **IC Expansion:** Entity has a different meaning in context of Knowledge Organization Systems; therefore, this DCMI definition refers more appropriately to an *agent*, such as a person, an organization, or a service. Typically, the name of a Creator should be used to indicate this agent.
Date (DCMI)	A point or period of time associated with an event in the lifecycle of the resource. **IC Expansion:** Date may be used to express temporal information at any level of granularity. Recommended best practice is to use an encoding scheme, such as the W3CDTF profile of ISO 8601. Typically, Date will be associated with the creation or revision of the Knowledge Organization System.
Description (DCMI)	An account of the resource. **IC Expansion:** Description may be a free-text account of the Knowledge Organization System.
Format (DCMI)	The file format, physical medium, or dimensions of the resource. **IC Expansion:** The formal language in which the Knowledge Organization System is encoded, including any version. Recommended best practice is to use a controlled vocabulary for Format.
Identifier (DCMI)	An unambiguous reference to the resource within a given context. **IC Expansion:** Recommended best practice is to identify the resource by means of a string conforming to a formal identification system. The formal

Data Element Refinement	Definition
	identification system for a Knowledge Organization System will typically be a URI (including the URL).
KOS Security Mark	The overall security classification and security handling instructions carried by the Knowledge Organization System.
Publisher (DCMI)	An entity [agent] responsible for making the resource available. **IC Expansion:** Entity has a different meaning in context of Knowledge Organization Systems; therefore, this DCMI definition refers more appropriately to an agent, such as a person, an organization, or a service. Typically, the name of a Publisher should be used to indicate this agent.
Source (DCMI)	The resource from which the described resource is derived. **IC Expansion:** The described Knowledge Organization System may be derived from the Source in whole or in part. Recommended best practice is to identify the Source by means of a string conforming to a formal identification system.
Title (DCMI)	A name given to the resource. **IC Expansion:** Typically, a Title will be a name by which the Knowledge Organization System is known.

6.4 - Data Element Refinements – Class/Property/Term Metadata

The following data elements refine the Class/Property/Term Metadata data element defined in Table 10: Data Element Refinements – KOS.

In the context of this section, the term resource in the DCMI definitions pertains to an instance of a Class, Property, or Term.

Table 12 - Data Element Refinements – Class/Property/Term Metadata

Data Element Refinement	Definition
Class, Property, or Term Security Mark	The overall security classification and security handling instructions carried by the Class, Property, or Term.
Contributor (DCMI)	An entity [agent] responsible for making contributions to the resource. **IC Expansion:** Entity has a different meaning in context of Knowledge Organization Systems; therefore this DCMI definition refers more appropriately to an *agent*, such as a person, an organization, or a service. Typically, the name of a Contributor should be used to indicate the agent.
Creator (DCMI)	An entity [agent] primarily responsible for making the resource.

Data Element Refinement	Definition
	IC Expansion: Entity has a different meaning in context of Knowledge Organization Systems; therefore, this DCMI definition refers more appropriately to an *agent*, such as a person, an organization, or a service. Typically, the name of a Creator should be used to indicate this agent.
Date (DCMI)	A point or period of time associated with an event in the lifecycle of the resource. **IC Expansion:** Date may be used to express temporal information at any level of granularity. Recommended best practice is to use an encoding scheme, such as the W3CDTF profile of ISO 8601. Typically, Date will be associated with the creation or revision of the Class, Property, or Term.
Description (DCMI)	An account of the resource. **IC Expansion:** Description may be a free-text account of the Class, Property, or Term.
Source (DCMI)	The resource from which the described resource is derived. **IC Expansion:** The described Class, Property, or Term may be derived from the related resource in whole or in part. Recommended best practice is to identify the related resource by means of a string conforming to a formal identification system.
Title (DCMI)	A name given to the resource. **IC Expansion:** Typically, a Title will be a name by which the Class, Property, or Term is known.

Chapter 7 - Knowledge Assertion Data Elements

Scope: The term *knowledge assertion* (KA) refers to the human or machine association of structured descriptive information to selected parts of an information resource. Identifying and describing, in a standard and structured way, the meaning inherent in the parts of an information resource will improve intelligence analysis, correlation, fusion, discovery, and overall usability of that information resource.

These data elements are the essential components of a knowledge assertion necessary to provide layers of structured metadata ranging from simple identity assertions (e.g., of a person's name) to more complex relationships (e.g., the connection among people, organizations, and events). Knowledge assertions provide a way to express the *deep content* found within intelligence information in a standardized manner.

The definitions in this chapter use some common terms and data elements from Chapter 6 - Knowledge Organization System Data Elements . These include Entity, Event, Class, Property Attribute, and Relationship.

7.1 - Data Elements

These data elements include a Knowledge Assertion and metadata about that Knowledge Assertion.

Table 13 - Knowledge Assertion Data Elements

Data Element	Definition
Knowledge Assertion	A statement that: 1) associates a finite part of a resource with an Attribute of an entity or event (see Resource Segment Attribute Assertion), 2) provides additional Attributes for a referenced entity or event (see Attribute Assertion), or 3) provides Relationships for a referenced entity or event (see Relationship Assertion).
Knowledge Assertion Metadata	Information that provides data about a Knowledge Assertion, but is not the content of the Knowledge Assertion.

7.2 - Data Element Refinements – KA

The following data elements refine the Knowledge Assertion data element defined in Table 13: Knowledge Assertion Data Elements.

Table 14 - Data Element Refinements – Knowledge Assertion

Data Element Refinement	Definition
Attribute Assertion	A statement that a specified quantitative or qualitative characteristic is the value of a specified attribute of some entity or event. The attributes allowed in a Knowledge Assertion are defined in the Knowledge Organization System specified in the Knowledge Assertion Metadata. More than one Attribute Assertion may be made about the same entity or event. An Attribute Assertion is the same conceptually as a Resource Segment Attribute Assertion, except that the attribute's value is not the content of a Resource Segment, but some other quantitative or qualitative characteristic.
Relationship Assertion	A statement that another specified entity or event is the value of a specified relationship of a specified entity or event. The relationships allowed in a Knowledge Assertion are defined in the Knowledge Organization System specified in the Knowledge Assertion Metadata. More than one Relationship Assertion may be made about the same entity or event. An entity or event that is the value of the relationship may also be identified in an external information resource using a unique identifier.
Resource Segment	A specific, possibly non-contiguous, part of an information resource to which an entity or event is associated via a Knowledge Assertion. A Resource Segment could be a specific set of characters in text, a specific area in an image, a specific set of signals, a specific clip in an audio or video, etc.
Resource Segment Attribute Assertion	A statement that a Resource Segment's content is the value of a specified attribute of some entity or event. The attributes allowed in a Knowledge Assertion are defined in the Knowledge Organization System specified in the Knowledge Assertion Metadata. More than one Resource Segment Attribute Assertion may be made about the same entity or event.

7.3 - Data Element Refinements – KA Metadata

The following data elements refine the Knowledge Assertion Metadata data element defined in Table 13: Knowledge Assertion Data Elements.

Data elements labeled with the DCMI designation "(DCMI)" adopt the Dublin Core element definitions, unchanged from the ISO standard. IC-specific expansions of the DCMI definitions

are labeled **IC Expansion**. In the context of this section, the term *resource* in the DCMI definitions pertains to a Knowledge Assertion.

Table 15 - Data Element Refinements – Knowledge Assertion Metadata

Data Element Refinement	Definition
Confidence	A measure, description or assessment of the conviction with which the Knowledge Assertion is made. The normative scale for a measure must be explicit and accessible.
Contributor (DCMI)	An entity [agent] responsible for making contributions to the resource. **IC Expansion:** Entity has a different meaning in context of Knowledge Assertions; therefore this DCMI definition refers more appropriately to an *agent*, such as a person, an organization, or a service. Typically, the name of a Contributor should be used to indicate the agent.
Creator (DCMI)	An entity [agent] primarily responsible for making the resource. **IC Expansion:** Entity has a different meaning in context of Knowledge Assertions; therefore, this DCMI definition refers more appropriately to an *agent*, such as a person, an organization, or a service. Typically, the name of a Creator should be used to indicate this agent.
Date (DCMI)	A point or period of time associated with an event in the lifecycle of the resource. **IC Expansion:** Date may be used to express temporal information at any level of granularity. Recommended best practice is to use an encoding scheme, such as the W3CDTF profile of ISO 8601. Typically, Date will be associated with the creation or revision of the Knowledge Assertion, but can also apply to the dates of applicability of a Knowledge Assertion.
Format (DCMI)	The file format, physical medium, or dimensions of the resource. **IC Expansion:** The formal language in which the Knowledge Assertion is encoded, including any version. Recommended best practice is to use a controlled vocabulary for Format.
Knowledge Assertion Security Mark	The security classification and security handling instructions carried by the Knowledge Assertion.
Knowledge Organization System Reference	The reference to the Knowledge Organization System that specifies the meaning of the Knowledge Assertion. The Knowledge Organization System's Description must include any version information.
Publisher (DCMI)	An agent responsible for making the resource available.

Data Element Refinement	Definition
	IC Expansion: Examples of a Publisher include a person, an organization, or a service. Typically, the name of a Publisher should be used to indicate this agent.
Source (DCMI)	The resource from which the described resource is derived. **IC Expansion:** The described Knowledge Assertion may be derived from the Source in whole or in part. Recommended best practice is to identify the Source by means of a string conforming to a formal identification system.

Appendix A Change History

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

Table 16 - DES Version Identifier History

Version	Date	Purpose
1	24 December 2009	Initial release published as an IC technical data specification. Merged and rescinded ICS 2007-500-3, ICS 2007-500-4, ICS 2008-500-2, and ICS 2008-500-7. Added two new abstract data element sets not previously published for Knowledge Organization Systems and Knowledge Assertions.
2	9 August 2011	Update with definitions approved by prior releases of DESs.

A.1 - V2 Change Summary

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

Table 17 - Change Summary

Change	Artifacts changed	Compatibility Notes
Removed "Document Organization" listing sections and appendixes from the Executive Summary	ADD	
Remove Background section	ADD	
Changed **Coverage** data element description to removed the "IC Expansion" describing NGA GEOnet as an alternative to TGN.	ADD	
Changed **Language** data element description	ADD	Changed recommended best practice to use RFC 3066 rather than 4646.
Updated references from EO 12958 to EO 13526	ADD	
Added entry for **Records Management Information** data element	ADD	
Removed **Date of Exempted Source** data element	ADD	
Removed **Type of Exempted Source** data element	ADD	
Added **Display Only To** data element	ADD	
Added **Compilation Reason** data element	ADD	

Change	Artifacts changed	Compatibility Notes
Added **Applicable Ruleset** data element	ADD	
Added **Atomic Energy Act (AEA) Information Markings** data element	ADD	
Added **Collect Source** data element	ADD	
Added **Alternate Compensatory Control Measures (ACCM)** data element	ADD	
Added **Non-US Controls** data element	ADD	
Removed **Briefing** data element	ADD	
Removed **Correspondence** data element	ADD	
Removed **Digest** data element	ADD	
Removed **Amplification** data element	ADD	
Removed **Analysis** data element	ADD	
Added **Notice** data element	ADD	

Appendix B Acronyms

This appendix lists all the acronyms referenced in this DES and lists other acronyms that may have been used in other DES. This appendix is a shared resource across multiple documents so in any given DES there are likely acronyms that are not referenced in that particular DES.

Table 18 - Acronyms

Name	Definition
CAPCO	Controlled Access Program Coordination Office
CVE	Controlled Vocabulary Enumeration
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DOI	Digital Object Identifier
DNI	Director National Intelligence
E.O.	Executive Order
GNS	Geographic Names Server
HTML	HyperText Markup Language
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICS	Intelligence Community Standard
ISBN	International Standard Book Number
ISM	Information Security Marking Metadata
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
KA	Knowledge Assertion
KOS	Knowledge Organization System
MIME	Internet Media Types
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NSI	National Security Intelligence
ODNI	Office of the Director of National Intelligence
SSC	Special Security Center
TGN	Thesaurus of Geographic Names
URI	Uniform Resource Identifier

Name	Definition
URL	Uniform Resource Locator
W3CDTF	World Wide Web Consortium Date Time Format
XML	Extensible Markup Language

Appendix C Bibliography

This appendix lists all the sources referenced in this DES and lists other sources that may have been used in other DESs. This appendix is a shared resource across multiple documents so in any given DES there are likely sources that are not referenced in that particular DES.

(CAPCO Implementation Guide)

Community Classification and Control Markings Implementation Manual. Unclassified FOUO version. Volume 4, Edition 2 (Version 4.2). 31 May 2011. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Implementation%20Manual%20v4%202_MAY_31_2011_FOUO_datefixed.pdf.

(CAPCO Register)

Authorized Classification and Control Markings Register. Unclassified FOUO version. Volume 4, Edition 2 (Version 4.2). 31 May 2011. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register_FOUO_v4.2_MAY31_2011.pdf.

(DC MES)

Dublin Core Metadata Element Set. Version 1.1. 02 June 2003. Dublin Core Metadata Initiative. http://dublincore.org/documents/dces/.

(E.O. 12958, as amended)

Executive Order 12958 – Classified National Security Information, as Amended. Federal Register, Vol. 68, No. 60. 25 March 2003. The White House. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html.

(E.O. 12829, as amended)

Executive Order 12829 – National Industrial Security Program, as Amended. Federal Register, Vol. 58, No. 240. 16 December 1993. The White House. http://www.archives.gov/isoo/policy-documents/eo-12829.html.

(E.O. 13526)

Executive Order 13526 – Classified National Security Information. 29 December 2009. The White House. http://www.archives.gov/isoo/pdf/cnsi-eo.pdf.

(ICD 206)

Sourcing Requirements for Disseminated Intelligence Products. Intelligence Community Directive Number 206. 17 October 2007. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_206.pdf.

(ICD 500)

Intelligence Community Directive Number 500. Director of National Intelligence Chief Information Officer. 7 August 2008. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_500.pdf.

(ICD 501)

Intelligence Community Directive Number 501. Director of National Intelligence Chief Information Officer. 21 January 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_501.pdf.

Classification and Control Markings System. Intelligence Community Directive Number 710. 11 September 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_710.pdf.

(ICD 500-27)

Intelligence Community Standard for Collection and Sharing of Audit Data for IC Information Resources by IC Elements Number 500-27. DRAFT. Office of the Director of National Intelligence.

(ISO 639-2)

Codes for the representation of names of languages – Part 2: Alpha-3 code ISO 639-2:1998. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4767.

(ISO 3166-1)

Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. ISO 3166-1:2006. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719.

(ISO 8601)

Data elements and interchange formats – Information interchange – Representation of dates and times. ISO 8601:2004. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40874.

(ISO 15836)

Information and documentation – The Dublin Core metadata element set. ISO 15836:2009. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142.

(ISO 19757-3:2006)

Information technology - Document Schema Definition Language (DSDL) - Part 3: Rule-based validation - Schematron. 19757-3:2006 International Organization for Standardization (ISO). http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

(ISOO Directive 1)

Classified National Security Information (Directive No. 1); Final Rule. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 68, No. 183. 22 September 2003. Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.pdf.

(RFC 3066)

Tags for the Identification of Languages. January 2001. H. Alvestrand. Cisco Systems. http://www.rfc-editor.org/rfc/rfc3066.txt.

Marking Classified National Security Information. Information Security Oversight Office. December 2010. http://www.archives.gov/isoo/training/marking-booklet.pdf

http://www.schematron.com/.

Appendix D 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 DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

Appendix E 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.