



Intelligence Community Technical Specification

REST Service Encoding Specification for Security Markings

Version 2

14 January 2013

Distribution Notice:

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

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.2.1 - Conditions	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	3
1.6 - Conventions	3
1.7 - Dependencies	4
1.8 - Conformance	4
Chapter 2 - Development Guidance	6
2.1 - Problem Statement	6
2.2 - Use Cases	7
2.2.1 - Request/Response Exchange	7
2.3 - Definitions	8
2.4 - Solution – Security Markings in the HTTP Header	9
2.4.1 - Assumptions	9
2.4.2 - Summary	9
2.4.2.1 - IC-SecurityMarkings Field	10
2.4.2.2 - IC-SecurityMarkings XML	11
2.4.3 - Status Codes	13
Appendix A - Controlled Vocabulary Enumerations	15
Appendix B - Change History	16
B.1 - V2 Change Summary	16
Appendix C - Acronyms	17
Appendix D - Bibliography	20
Appendix E - Points of Contact	22
Appendix F - IC CIO Approval Memo	23

List of Figures

Figure 1 - Multi-Tier Exchange – End User to Service	6
Figure 2 - Simple Request/Response Exchange	7
Figure 3 - Multi-Tier Exchange – End User to Service	7
Figure 4 - Single-Tier Exchange – Service to Service	8
Figure 5 - Example Format	11
Figure 6 - Example Encoding	11
Figure 7 - High Level Structure of Security Metadata	11

List of Tables

Table 1 - Request/Response Conditions Traceability	1
Table 2 - Attribute Multiplicity Description	3
Table 3 - Dependencies	4
Table 4 - Definitions	8
Table 5 - Specification Assumptions	9
Table 6 - IC-SecurityMarkings HTTP Headers	10
Table 7 - IC-SecurityMarkings HTTP Header Description	10
Table 8 - SecurityMarkings Element Description	12
Table 9 - HTTP Status Codes	13
Table 10 - Identifier History	16
Table 11 - Data Encoding Specification V2 Change Summary	16
Table 12 - Acronyms	17

Chapter 1 - Introduction

1.1 - Purpose

This document defines the syntax, protocol and conventions for applying security metadata or notices to a request or a response message conveyed using the Hypertext Transfer Protocol (HTTP).

Adding security metadata and notices to messages provides the capability to route and filter messages based on classification and other security markings. By processing security metadata such as portion markings and tearlines, access control points have the ability to filter data based on the formal authorization credentials of authenticated users.

This specification provides guidance for the implementation of applying such metadata to messages using HTTP or REpresentational State Transfer (REST)-based services.

1.2 - Scope

This technical specification applies to web services using HTTP within the Intelligence Community (IC), including REST-based services. This specification may have relevance outside the intelligence domain; however, prior to applying outside of this defined scope, the information contained herein should be closely scrutinized and differences separately documented and assessed for applicability.

1.2.1 - Conditions

[Table 1](#) lists the common request/response conditions addressed as part of this specification. These conditions are not meant to be viewed as requirements levied on a program, but rather if a program is required to meet the condition, then the program **MUST** implement this specification to address those requirements.

Table 1 - Request/Response Conditions Traceability

Condition
The data transmitted in each exchange (end-to-end, or point-to-point) needs classification metadata tags in accordance with Controlled Access Program Coordination Office (CAPCO) guidance.
The data transmitted in each exchange (end-to-end, or point-to-point) needs 'need-to-know' metadata tags.
The data transmitted in each exchange (end-to-end, or point-to-point) needs appropriate notice metadata tags.
A response needs a status code indicating (1) the success or failure of processing the request, or (2) information about additional circumstances that occurred during the processing about which the response recipient should be aware.

1.3 - Background

The IC Chief Information Officer (IC CIO) is leading the IC's enterprise IT transformation towards a flexible, scalable and interoperable architecture to enable use within and across the

IC. Intelligence Community Directive (ICD) 500: *Director of National Intelligence Chief Information Officer* ^[3] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA).
- Lead the IC's identification, development, and management of IC enterprise standards.
- Incorporate technically sound, deconflicted, 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 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.

1.4 - Enterprise Need

The IC CIO funds and oversees a number of critical enabling projects, for example the Information Integration (I2) Pilot, Enterprise Search and Integration Services (ES&IS), Next Generation Trident (NGT), Nebula, and in direct support of the IC IT Enterprise. These projects make extensive use of web services and distributed processing, yet each program has yet to establish mechanisms for marking the service request or response with security metadata.

Enterprise needs and requirements for this specification can be found in the following ODNI policies and implementation guidance.

- IC Information Technology Enterprise (IC ITE)
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[2]
- 500 Series:
 - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC^[4]
 - Intelligence Community Policy Guidance (ICPG) 500.2, Attribute-based Authorization and Access Management^[6]
- 700 Series:
 - Intelligence Community Directive (ICD) 710, Classification and Control Markings System^[5]
 - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control^[7]

1.5 - Audience and Applicability

The audience for this document is program managers, systems integrators, system security personnel, and IT professionals wishing to exchange or convey security markings information when using the HTTP protocol.

The applicability of this technical specification is defined in the IC Enterprise Standards Baseline (IC ESB). Additional applicability and guidance may be defined in separate IC policies, as necessary.

IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,^[8] defines the IC ESB and its applicability to IC Elements. 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 defines the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

1.6 - Conventions

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 defined in the Internet Engineering Task Force Request for Change (IETF RFC) 2119 [RFC 2119].^[9] When these words are not capitalized, they are meant in their natural-language sense.

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** – A named entity, variable, element, or attribute name

Throughout this document, references are made to the multiplicity of attributes and parameters. Multiplicity defines the allowed number of occurrences of an attribute value, and also indicates whether the attribute is required or optional.

Table 2 - Attribute Multiplicity Description

Multiplicity	Description
1	Indicates the attribute is REQUIRED and MUST contain only one value.
0:1	Indicates the attribute is OPTIONAL and MAY contain at most one value.
0:*	Indicates the attribute is OPTIONAL and MAY contain any number of values.

Multiplicity	Description
1:*	Indicates the attribute is REQUIRED and MUST contain at least one value.
1:N	Indicates the attribute is REQUIRED, MUST contain at least one value and MAY contain up to N values.
M:N	Indicates the attribute is REQUIRED and MUST contain at least M values and MAY contain up to N values, where N is greater than M.

1.7 - Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in the following table. The documents listed below are referenced in this Data Encoding Specification, and are normative or informative as indicated in the dependencies table.

Table 3 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Access Rights and Handling</i> (ARH.XML.V1+) ^[1]	Depends on Access Rights and Handling (ARH) Specification. Starting with ARH v1, the version of ARH imported is no longer normative, so any ARH version 1 or above may be used.
<i>XML Data Encoding Specification for Information Security Marking</i> (ISM.XML.V9+) ^[11]	Depends on Information Security Markings (ISM). Starting with ISM v9, the version of ISM imported is no longer normative, so any ISM version 9 or above may be used.
<i>XML Data Encoding Specification for Need-To-Know Metadata</i> (NTK.XML.V7+) ^[12]	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.
IETF-RFC 2616, Hypertext Transfer Protocol - HTTP/1.1	Depends on HTTP and REST

1.8 - Conformance

For an implementation to conform to this specification, it MUST adhere to all normative aspects of the specification as identified through use of IETF RFC 2119^[9] keywords. For the purposes of this document, normative and informative are defined as:

1. Normative: prescriptive and necessary to conform to the standard.
2. Informative: serving to instruct or enlighten or inform.

Additional guidance that is either classified or having 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.

Chapter 2 - Development Guidance

This chapter provides the context and underlying assumptions of the problem being addressed and the basis of the solution presented. It begins with a problem statement to define and basic use cases to illustrate the problem, and it defines terms in the context of those use cases. This chapter concludes with specific requirements – behavior and interface – for what is presented as an interoperable solution.

2.1 - Problem Statement

In order for systems to provide access control to content, it is often required to mark message requests and responses with security markings.

[Figure 1](#) illustrates a service chain providing capabilities to a user. In this case, the user accesses a web application via a web browser that serves as the user's agent for the electronic interchange. The application then communicates with a service that in turn communicates with a database. The service can be viewed as a data access or management service that fronts a traditional relational database management system (RDBMS) in a service-enabled environment. In [Figure 1](#), a line between two entities is considered both the request and the response.



Figure 1 : Multi-Tier Exchange – End User to Service

Each actor in this solution may have certain authorization credentials and "need to know." In order to safeguard information in the IC, mechanisms must be in place to provide access control based on the security policies related to the data being transmitted to each point. In order to provide access control to each actor in this service chain,

1. Data must be marked with security markings which inherently describes the access control policy to the data
2. Policy Enforcement Points (PEPs) in the solution must control access to the data based on the *security markings of the data*, the *security policy* inherent in the security markings of the data, and the *authorization credentials of the recipient*.

In this case, each request and response should be marked up with security markings so that PEPs can control access to the data.

In this example, each requestor in the service chain should supply sufficient information to indicate the security markings of each request so that each recipient in the service chain can properly handle and interpret the request, controlling access properly. In the same way, each node in the service chain may need to respond, providing security markings of the response so that the recipient may adequately handle and control access to each response. This

specification provides guidance for the security markup of requests and responses of REST-based web services.

2.2 - Use Cases

This section presents a basic use case and then a chaining of instances of the basic use case in order to illustrate the general problem.

2.2.1 - Request/Response Exchange

A request/response exchange is depicted in [Figure 2](#) . A consumer interacts directly with a provider: provider accepts the request from consumer, does any necessary processing, and returns a response to consumer.

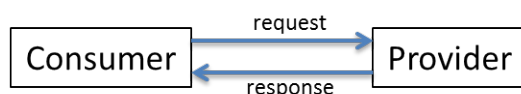


Figure 2 : Simple Request/Response Exchange

Consumer can be a human user interacting through an agent (e.g. browser) or a service acting directly. The provider in this use case may be an application or a service. Examples of the simple request/response exchange are shown below. In each case, there is a need to provide security markings of the request and response so that access control policy may be enforced. Inherent in any request/response interchange involves the enforcement of access control policy based on the *security markings of the data* , the *security policy* inherent in the security markings of the data, and the *authorization credentials of the recipient*. For example, in the multi-tier exchange example, the final service that communicates with a database may respond with data marked up with security markings that the user does not have credentials to view. A policy enforcement point at the web application level would be able to filter the data based on the authorization credentials of the user, stripping out data that the user is not allowed to see, in order to be compliant with access control policy. Although the implementation of access control is beyond the scope of this document, this document aims to provide the capability of security markings to enable such access control.



Figure 3 : Multi-Tier Exchange – End User to Service

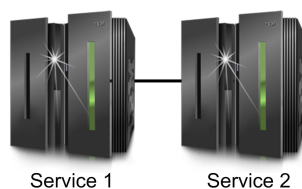


Figure 4 : Single-Tier Exchange – Service to Service

2.3 - Definitions

For the purposes of this specification, the following terms are used throughout the balance of this document to provide clarity and consistency.

Table 4 - Definitions

Term	Definition
Entity	A provider or consumer of a service.
User	An entity that is a human.
Browser	A user-agent that acts as the user in a request/response exchange.
Consumer	An entity capable of making a request to and receiving a response from a service
Service	IT implementation of a provider, but can also be a consumer, where the implementation follows web service standards and design paradigms. As used in this specification, the term web services primarily refers to RESTful implementations but SHOULD be equally applicable for SOAP web services.
Originator	The consumer making the initiating request on behalf of the user in a chained request/response exchange.
Provider	An entity capable of receiving a request, doing appropriate processing, and returning a response. A provider may need to act as a consumer in order to complete its processing.
Requestor	The role of a consumer when making a request to a provider.
Responder	The role of a provider when sending a response to a requestor.
Point-to-Point Transaction	An instance of a simple request/response exchange or a single request/response exchange between a consumer and provider in a chained request/response exchange.

Term	Definition
Service Chain	A sequence in which one service acts as a requestor and engages in a point-to-point exchange with another service, and this pattern of service calling service can be repeated any number of times. As a request (or a consequent request resulting from a previous request) progresses from one service to the next, the service acting as the provider for one request in turn acts as the consumer for the next request. The service chain is the sequence of services that propagates a request and in reverse propagates responses until the originator receives the final response to the initiating request.

2.4 - Solution – Security Markings in the HTTP Header

An HTTP header is defined to support inserting security markings or other related notices in an HTTP request or response. The HTTP payload MAY also be tagged at the implementer's discretion. In addition, this solution allows the reuse of the existing XML processing for document security markings.

2.4.1 - Assumptions

This section includes a list of assumptions and constraints that **MUST** be met when the exchanges and protocols defined herein are implemented.

Table 5 - Specification Assumptions

Assumption/Constraint
All entities MUST be approved to exchange information by the program's Designated Approval Agent (DAA). This approval may be in the form of an authority to operate (ATO).

2.4.2 - Summary

This specification defines the **IC-SecurityMarkings** field as the means to convey the security markings that describe the messages of a chained request/response exchange:

- Each request **MUST** include the **IC-SecurityMarkings** field as defined below.
- Each requestor **MUST** preserve and augment the **IC-SecurityMarkings** field as specified below.
- Each provider **MUST** accept and process the **IC-SecurityMarkings** field as specified below.

Table 6 - IC-SecurityMarkings HTTP Headers

HTTP Header	Description
IC-SecurityMarkings	Header whose value represents information security markings for classifying, safeguarding, and declassifying national security information, providing a well-defined warning or required notice, or facilitating “need to know” access determinations about a particular resource.

2.4.2.1 - IC-SecurityMarkings Field

The IC-SecurityMarkings field is defined to convey security metadata for the entire HTTP message, including query parameters, headers and the body (e.g., payload).

Each originator MUST create the IC-SecurityMarkings field as part of its request and MUST assign the appropriate security markings (see example in [Figure 7](#)) as the IC-SecurityMarkings value. Each subsequent provider upon assuming the role of requestor MUST update the IC-SecurityMarkings field, as necessary to comply with policy. The provider MUST include the updated IC-SecurityMarkings field when it subsequently acts as a requestor in the chained request/response exchange. Before adding additional markings to the IC-SecurityMarkings field, the provider MUST check that adding such information will not exceed the buffer size. Since many web servers limit the HTTP buffer size to 8192 bytes, the buffer size MUST be limited to 8192 bytes for interoperability purposes. The provider MUST return a fault if the buffer size will be exceeded.

The HTTP body may contain a data payload that also contain security markings. These security markings SHOULD be extracted and processed separately in accordance with the IC ARH.XML, IC ISM.XML and IC NTK.XML technical specifications.

A browser acting as the user MAY provide the IC-SecurityMarkings header in the request. If the browser does not provide the IC-SecurityMarkings header, then the service being called MUST initiate the IC-SecurityMarkings field and SHOULD assume it inherits the security constraints of the network. This service and any other in the service chain MUST update the security markings as specified by relevant policy. Each service is REQUIRED to provide security markings in the IC-SecurityMarkings header field for both the request and response.

Table 7 - IC-SecurityMarkings HTTP Header Description

HTTP Header	Description
Physical Name	IC-SecurityMarkings
Logical Name	SecurityMarkings, Notice, NTK
Description	Security markings for classifying, safeguarding and declassifying the HTTP message.
Multiplicity	1
Allowed Values	Tokenized string of Base64 ² encoded well-formed XML representing the request/response security markings XML structure defined in Section IC-SecurityMarkings XML.

HTTP Header	Description
Backus-Naur Form (BNF) ^a	" IC-SecurityMarkings " ":" <ic-securitymarkings.xml base64 encoded>

^aUsing Augmented BNF notation as specified in RFC 2616^[10].

IC-SecurityMarkings: E(IC-SecurityMarkings.xml)

where any well-formed XML containing the appropriate security marking information can be substituted for IC-SecurityMarkings.xml.

Figure 5 : Example Format

```
IC-SecurityMarkings:
PD94bWwgdMvYc2lvdj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxTZWN1cm10eU1hcm
tpbmdzIHhtbG5zPSJ1cm46dXM6Z2920mljOnJyIiB4bWxuczp4bGluaz0iaHR0cDovL3d3
dy53My5vcmcvMTk5OS94bGluayIgeG1sbnM6aXNtPSJ1cm46dXM6Z2920mlj0mlzbSIgaX
NtOkRFU1ZlcnNpb249IjciIGlzbTpyZXNvdXJjZUUsZW1lbnQ9InRydWUiIGlzbTpjcmVh
dGVEYXRlPSIyMDE5LTA3LTl2IiBpc206Y2xhc3NpZm1jYXRpb249IlUiIGlzbTpv25lcl
Byb2R1Y2VyPSJVU0EiPg0KICAgIDxQb3J0aW9uIGlzbTpbGZc2lmaWNhdGlvdj0iVSig
aXNtOm93bmVyUHJvZHVjZSI9IlVTQSIgeGxpbnM6dHlwZT0ic2ltcGx1IiB4bGluazpocm
VmPSIjeHBvaW50ZXIoLykiLz4NCjwvU2VjdXJpdHlNYXJraW5ncz4=
```

Figure 6 : Example Encoding

It is critical to note that the above string does not contain carriage returns or spaces; wrapping is due to the width of the page.

2.4.2.2 - IC-SecurityMarkings XML

The IC-SecurityMarkings XML structure represents the security metadata for a resource (in this case, an HTTP message). The structure contains the Access Rights and Handling (ARH.XML) metadata, Information Security Marking (ISM.XML) metadata, as well as Need-To-Know (NTK.XML) metadata. The high-level structure of the security metadata structure is as follows:

```
<SecurityMarkings xmlns:ism="..." ism:resourceElement="true"
ism:classification="U" ism:DESVersion="...">
  <arh:Security arhDESVersion="..." ism:...>
    <ism:NoticeList>
      <ism:Notice ism:classification="U" ism:...>...</ism:Notice>
      <ism:Notice ism:classification="U" ism:...>...</ism:Notice>
    </ism:NoticeList>
    <ntk:Access>...</ntk:Access>
  </arh:Security>
  <Portion
    ism:classification="U"
    xlink:href="#"xpointer(/)" />
  <Portion
    ism:classification="U"
```

```

        xlink:href="#xpointer(/Request-Line/Request-URI/query)"/>
    <Portion
        ism:classification="U"
        xlink:href="..." />
    ...
</SecurityMarkings>

```

Figure 7 : High Level Structure of Security Metadata

Significant elements are as follows:

Table 8 - SecurityMarkings Element Description

X-Path	Multiplicity	Description
/SecurityMarkings	1	The SecurityMarkings element is the root node of the security marking XML instance. The / SecurityMarkings child elements contain the mandatory and optional security metadata as defined by relevant policy.
/SecurityMarkings/arh:Security	1	The Security element contains any necessary access rights and handling markings for the XML instance. This element also contains ISM security markings as defined by relevant policy.
/SecurityMarkings/arh:Security/@ism:resourceElement	1	REQUIRED attribute whose value MUST be "true."
/SecurityMarkings/arh:Security/ism:NoticeList	0:*	The NoticeList element contains any necessary notices that apply to the entire message. This element contains a list of ISM.XML Notice elements and additional security markings as necessary. A / SecurityMarkings/NoticeList/Notice element MUST include ISM.XML attributes as defined by relevant policy.

X-Path	Multiplicity	Description
/SecurityMarkings/arh:Security/ntk:Access	0:1	The ntk:Access element contains any necessary need-to-know attribute that apply to the entire message. The ntk:Access element is defined by the NTK.XML specification.
/SecurityMarkings/Portion	1:*	The Portion element contains the security metadata for any portion of the message. The element contains ISM.XML attributes for the portion, and a reference to the portion that is being tagged. The xlink:href attribute is used to reference the portion being tagged. Although this element can support multiple Portion elements, it is RECOMMENDED that most implementations make use of the one Portion element representing the entire HTTP message.

2.4.3 - Status Codes

Each response MUST use the standard HTTP status code defined in RFC 2616^[10] to indicate the success or failure of the processing by the responder. To provide further guidance, the following error conditions associated with this specification SHOULD return the following HTTP status codes:

Table 9 - HTTP Status Codes

Condition	HTTP Status Code
A required field is not present.	400 Bad Request
The syntax for a field is not correct.	
Requestor is not able to establish a secure connection.	401 Unauthorizaed
The security marking in the HTTP header cannot be processed (if required).	
The security marking in the HTTP header is higher than the consumer can process in the chained request/response exchange.	403 Forbidden
Processing of the chained request/response exchange cannot be completed.	404 Not Found

Condition	HTTP Status Code
Header size exceeded if modify security markings or notices.	431 Request Header Fields Too Large

Appendix A Controlled Vocabulary Enumerations

This specification leverages those controlled vocabulary enumerations provided in the XML Data Encoding Specification for Access Rights and Handling (ARH.XML)^[1], XML Data Encoding Specification for Information Security Markings (ISM.XML)^[11] and XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)^[12] specifications. Please reference those specifications for information pertaining to controlled vocabularies.

Appendix B Change History

The following table summarizes the version identifier history for this technical specification.

Table 10 - Identifier History

Version	Date	Purpose
1	17 July 2012	Initial Release
2	21 January 2013	Routine revision to technical specification. For details of changes, see Section B.1 - V2 Change Summary

B.1 - V2 Change Summary

Significant drivers for Version 2 include:

- ISM V10 Changes
- NTK

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

Table 11 - Data Encoding Specification V2 Change Summary

Change	Artifacts changed	Compatibility Notes
Added schematron rules to ensure that the versions of the imported specs meet the minimum allowed versions.	Schematron RR-SM-ID-00001 Added RR-SM-ID-00002 Added	Data generation and ingestion systems need to be updated enforce the new rules.
Updated to use ARH	Schema	Data generation and ingestion systems need to be updated to use the correct Schema definitions and values

Appendix C 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 12 - Acronyms

Name	Definition
A&A	Access Rights and Handling
ABAC	Attribute Based Access Control
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CMS	Cryptographic Message Syntax
CVE	Controlled Vocabulary Enumeration
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DDMS	Department of Defense Discovery Metadata Specification
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
EDH	Enterprise Data Header
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
GIS	Geospatial Information System
GNS	Geographic Names Server
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I2	Information Integration
IC	Intelligence Community
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
IC EA	IC Enterprise Architecture

Name	Definition
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
IRM	Information Resource Metadata
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWT	JSON Web Token
KA	Knowledge Assertion
KOS	Knowledge Organization System
MAC	Multi Audience Collection
MIME	Multipurpose Internet Mail Extensions
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NGT	Next Generation Trident
NPE	Non-Person Entity
NSI	National Security Information
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PK	Private Key
PKI	Public Key Infrastructure
RDBMS	Relational Database Management System
REST	REpresentational State Transfer

Name	Definition
RFC	Request for Comments
RR-ID	REST Security Encoding Specification for End-to-End Identity Propagation
SAML	Security Assertion Markup Language
SSD	Special Security Directorate
SSL	Secure Sockets Layer
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TGN	Thesaurus of Geographic Names
TLS	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VIRT	Virtual Coverage
W3CDTF	World Wide Web Consortium Date Time Format
WSDL	Web Service Definition Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

Appendix D Bibliography

Bibliography

[1] ARH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*.

Available online IntelLinkU at: <http://purl.org/IC/Standards/ARH>

Available online at: <http://purl.org/IC/Standards/public>

[2] 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 at: <http://go.ic.gov/HvBHBmY>

[3] ICD 500

Director of National Intelligence Chief Information Officer. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[4] ICD 501

Director of National Intelligence Chief Information Officer. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[5] ICD 710

Director of National Intelligence Chief Information Officer. *Classification and Control Markings System*. Intelligence Community Directive 710. 11 September 2009.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[6] ICPG 500.2

Assistant Director of National Intelligence for Policy and Strategy. *Attribute-Based Authorization and Access Management*. Intelligence Community Policy Guidance 500.2. 23 November 2010.

Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[7] ICPG 710.1

Assistant Director of National Intelligence for . *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online at: <http://go.ic.gov/fU3HML>

[8] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[9] IETF-RFC 2119

Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.

Available online at: <http://tools.ietf.org/html/rfc2119>

[10] IETF-RFC 2616

Internet Engineering Task Force. *Hypertext Transfer Protocol -- HTTP/1.1*. June 1999.

Available online at: <http://www.ietf.org/rfc/rfc2616.txt>

[11] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML)*.

Available online IntelLinkU at: <http://purl.org/IC/Standards/ISM>

Available online at: <http://purl.org/IC/Standards/public>

[12] NTK.XML

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

Available online IntelLinkU at: <http://purl.org/IC/Standards/NTK>

Available online at: <http://purl.org/IC/Standards/public>

Appendix E Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at 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 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.^[8]