

# **Intelligence Community Metadata Standards for Information Assurance**

## **Information Security Marking**

### **Implementation Guide**



### **Intelligence Community Metadata Working Group**

**Release 2.0  
30 April 2004**

## Preface

This Implementation Guide is part of the documentation set for the Intelligence Community (IC) Metadata Standard for Information Security Marking (ISM). The other part of the set is a Data Element Dictionary ([Appendix B](#), reference [3](#)).

This guide serves to instruct managers and developers on the processes and methods required to adhere to this standard in the collaborative and collateral shared spaces defined by the IC System for Information Sharing (ICSIS), and on implementing and extending this standard to meet organization-specific needs.

IC ISM is an implementation of the World Wide Web Consortium's specification of the Extensible Markup Language (XML) (reference [5](#)). It consists of a set of XML attributes that may be used to associate security-related metadata with XML elements in documents, web-service transactions, or data streams. It is distributed as both an XML entity set and W3C XML Schema (WXS) so that the XML attributes defined in the standard can be incorporated into any XML document type definition (DTD) or schema. Made available along with the IC ISM entity set and WXS are controlled vocabularies of terms that are used as the sources for the values of the IC ISM attributes.

The first section of this implementation guide is an introduction that addresses applicability and the target audience. The second section is a description of the XML components that constitute the IC ISM entity set and WXS. The third section explains how to include the IC ISM entities or attribute groups in XML DTDs or schemas accordingly, and how to extend the entity set and WXS to support local requirements. In section 4 are illustrations of graphical user interfaces as the preferred method of specifying values for the IC ISM attributes. Section 5 explains how to use the attributes to create portion marks, security banners and classification/declassification blocks. Section 6 explains the controlled vocabularies from which the values for the IC ISM attributes are drawn. Section 7 describes each IC ISM attribute in detail, including permissible values, usage examples and notes.

IC ISM is a product of the IC Metadata Working Group (MWG), an activity of the IC Chief Information Officer (CIO) with oversight by the IC CIO Executive Council. The development work that resulted in IC ISM was performed by a panel under the IC MWG.

Comments and suggestions pertaining to this implementation guide should be sent by email to the IC MWG Secretariat listed in [Appendix A](#).

## Table of Contents

<a href="#">Preface .....</a>	<a href="#">i</a>
<a href="#">Table of Contents.....</a>	<a href="#">ii</a>
<a href="#">List of Figures.....</a>	<a href="#">iv</a>
<a href="#">1 Introduction .....</a>	<a href="#">1</a>
<a href="#">1.1 What This Publication Is All About.....</a>	<a href="#">1</a>
<a href="#">1.2 Applicability.....</a>	<a href="#">1</a>
<a href="#">1.3 The Target Audience.....</a>	<a href="#">1</a>
<a href="#">1.4 Where to Submit Questions and Comments.....</a>	<a href="#">1</a>
<a href="#">2 IC ISM Components.....</a>	<a href="#">2</a>
<a href="#">2.1 The Attributes .....</a>	<a href="#">2</a>
<a href="#">2.2 How the Attributes are Packaged .....</a>	<a href="#">2</a>
<a href="#">2.3 The Controlled Vocabularies .....</a>	<a href="#">5</a>
<a href="#">2.4 Specifying Attribute Values.....</a>	<a href="#">7</a>
<a href="#">2.5 Attributes with Dependent or Conditional Relationships.....</a>	<a href="#">8</a>
<a href="#">2.6 Attributes with Specific Rules.....</a>	<a href="#">9</a>
<a href="#">3 Guidelines for Interoperability .....</a>	<a href="#">10</a>
<a href="#">3.1 Integrating the IC ISM Entity Set .....</a>	<a href="#">10</a>
<a href="#">3.2 Integrating the IC ISM W3C XML Schema .....</a>	<a href="#">10</a>
<a href="#">3.3 Namespaces.....</a>	<a href="#">11</a>
<a href="#">3.4 XML Registry .....</a>	<a href="#">12</a>
<a href="#">3.5 Customizing the IC ISM DTD Entity Set or WXS for Internal Use .....</a>	<a href="#">12</a>
<a href="#">3.6 Creating Stylesheets .....</a>	<a href="#">14</a>
<a href="#">4 Data Input Techniques.....</a>	<a href="#">16</a>
<a href="#">4.1 Graphical User Interfaces.....</a>	<a href="#">16</a>
<a href="#">4.2 Manual Data Input .....</a>	<a href="#">20</a>
<a href="#">5 Operations on the Security Attributes.....</a>	<a href="#">21</a>
<a href="#">5.1 Creating Portion Marks .....</a>	<a href="#">21</a>
<a href="#">5.2 Security Rollup .....</a>	<a href="#">21</a>
<a href="#">5.3 Performing Domain Filtering.....</a>	<a href="#">22</a>
<a href="#">6 Using the Controlled Vocabularies.....</a>	<a href="#">23</a>
<a href="#">6.1 Replacing, Extending and Sharing.....</a>	<a href="#">23</a>
<a href="#">6.2 Controlled Vocabulary Listings .....</a>	<a href="#">24</a>
<a href="#">7 Attribute Value Specifications.....</a>	<a href="#">25</a>
<a href="#">7.1 classification.....</a>	<a href="#">25</a>

## Information Security Marking

## Implementation Guide

<a href="#">7.2</a>	<a href="#">classificationReason</a>	<a href="#">27</a>
<a href="#">7.3</a>	<a href="#">classifiedBy</a>	<a href="#">27</a>
<a href="#">7.4</a>	<a href="#">dateOfExemptedSource</a>	<a href="#">28</a>
<a href="#">7.5</a>	<a href="#">declassDate</a>	<a href="#">28</a>
<a href="#">7.6</a>	<a href="#">declassEvent</a>	<a href="#">29</a>
<a href="#">7.7</a>	<a href="#">declassException</a>	<a href="#">29</a>
<a href="#">7.8</a>	<a href="#">declassManualReview</a>	<a href="#">31</a>
<a href="#">7.9</a>	<a href="#">derivedFrom</a>	<a href="#">32</a>
<a href="#">7.10</a>	<a href="#">disseminationControls</a>	<a href="#">33</a>
<a href="#">7.11</a>	<a href="#">FGISourceOpen</a>	<a href="#">36</a>
<a href="#">7.12</a>	<a href="#">FGISourceProtected</a>	<a href="#">37</a>
<a href="#">7.13</a>	<a href="#">nonICmarkings</a>	<a href="#">38</a>
<a href="#">7.14</a>	<a href="#">ownerProducer</a>	<a href="#">39</a>
<a href="#">7.15</a>	<a href="#">releasableTo</a>	<a href="#">41</a>
<a href="#">7.16</a>	<a href="#">SARIdentifier</a>	<a href="#">42</a>
<a href="#">7.17</a>	<a href="#">SCIcontrols</a>	<a href="#">43</a>
<a href="#">7.18</a>	<a href="#">typeOfExemptedSource</a>	<a href="#">45</a>
<a href="#">Appendix A - Points of Contact</a>		<a href="#">A-1</a>
<a href="#">Appendix B - References</a>		<a href="#">B-1</a>
<a href="#">Appendix C - Change History</a>		<a href="#">C-1</a>
<a href="#">Appendix D - Sample Domain Value Document</a>		<a href="#">D-1</a>

**List of Figures**

<a href="#">Figure 1. Entity “%SecurityAttributes” .....</a>	<a href="#">3</a>
<a href="#">Figure 2. Attribute Group “SecurityAttributesGroup” .....</a>	<a href="#">4</a>
<a href="#">Figure 3. Entity “%SecurityAttributesOption” .....</a>	<a href="#">5</a>
<a href="#">Figure 4. Attribute Group “SecurityAttributesOptionGroup” .....</a>	<a href="#">5</a>
<a href="#">Figure 5. Security GUI with US Security Marking Options Displayed .....</a>	<a href="#">17</a>
<a href="#">Figure 6. GUI for Selection of Declassification .....</a>	<a href="#">18</a>

## 1 Introduction

### 1.1 What This Publication Is All About

This implementation guide explains how to use the Intelligence Community Information Security Marking (IC ISM) standard to apply classification and controls tokens to Extensible Markup Language (XML) documents and data streams. The IC ISM standard consists of a vocabulary of agreed-upon XML attributes that were developed by a panel of the IC Metadata Working Group (IC MWG) to support the Controlled Access Program Coordination Office (CAPCO) guidelines for security markings (reference [2](#)). This guide will help organizations tag XML data in such a way that CAPCO-compliant security markings can be generated using standardized transformations and formatting.

This guide should be used in conjunction with the IC ISM Data Element Dictionary (DED), version 2.0 (reference [3](#)). The DED contains definitions of all of the IC ISM attributes.

### 1.2 Applicability

This guide applies to intelligence documents or serialized data streams created in XML format for interchange within the Community via the IC System for Information Sharing (ICSIS) community, organizational, and collateral shared spaces. The intent is to provide a common set of classification and controls XML attributes, for use throughout the Community, that may be associated with any XML data elements and used for categorization and selection as well as formatting of portion marks, security banners and classification/declassification blocks.

IC ISM is *not* intended to address business rules associated with using security metadata, and is therefore not a replacement for CAPCO requirements or the understanding of those requirements. Users of IC ISM may develop specific (but separate) programming interfaces to implement their required business rules for populating and using the IC ISM attributes.

The IC MWG developed IC ISM as part of the IC CIO Executive Council commitment to inter-organization interoperability. IC ISM is based on a number of data modeling activities that have occurred in the IC over the last few years.

### 1.3 The Target Audience

This implementation guide is intended for use by developers and IT support personnel—not analysts and other users. The guide provides implementation details that should be transparent to authors, editors and reviewers.

Users of this guide are expected to have at least basic knowledge of XML. The guide has been written with the assumption that readers understand XML syntax (angle brackets, names, name tokens, unique identifiers, elements, attributes, *et al.*), XML namespaces, and—to a very limited degree—XML document type definitions (DTDs) and W3C XML Schemas (WXS). The references for these W3C specifications can be found in [Appendix B](#).

### 1.4 Where to Submit Questions and Comments

Points of contact for this implementation guide, the IC MSP models, and the IC MWG are listed in [Appendix A](#).

## 2 IC ISM Components

IC ISM defines 18 XML global attributes and a set of controlled vocabularies from which the values of certain attributes may be selected.

### 2.1 The Attributes

The global attributes defined by IC ISM are to be used to associate CAPCO-defined classification and control marking abbreviation components with XML elements in documents or data streams. The names of the 18 attributes are:

1. **classification**
2. **ownerProducer**
3. **SCIcontrols**
4. **SARIdentifier**
5. **FGIsorceOpen**
6. **FGIsorceProtected**
7. **disseminationControls**
8. **releasableTo**
9. **nonICmarkings**
10. **classifiedBy**
11. **classificationReason**
12. **derivedFrom**
13. **declassDate**
14. **declassException**
15. **declassEvent**
16. **typeOfExemptedSource**
17. **dateOfExemptedSource**
18. **declassManualReview**

The attribute names follow the naming guidelines promulgated by the Federal XML Developer's Guide. Lower camel case is used except when an acronym is part of the name. Acronyms are all upper case.

The formal ISO 11179-style definitions of the attributes may be found in the IC ISM DED.

### 2.2 How the Attributes are Packaged

The IC ISM attributes are provided as an XML entity set for DTDs, which is available from the IC XML Registry as an XML schema document with the name "IC\_ISM\_Entities." The entity set may be downloaded from the IC MWG web sites as well. The file name for the entity set is "IC-ISM-v2.ent."

The IC ISM attributes are also provided as a W3C XML schema (WXS), which is available from the IC XML Registry as an XML schema document with the name "IC\_ISM\_WXS". The WXS may be downloaded from the IC MWG web sites as well. The file name is "IC-ISM-v2.xsd".

The DTD entity set consists of two XML parameter entity declarations that declare entities named:

- %SecurityAttributes
- %SecurityAttributesOption

The entity text of these entities contains the definitions of the 18 IC ISM attributes. References to these entities may be inserted into an XML attribute definition list in order to include the names, declared values, and default values of the IC ISM attributes into the attribute definition list of any XML element.

The WXS version consists of declarations for two attribute groups and the 18 IC ISM global attributes. The attribute groups, which are equivalent to the DTD parameter entities, are named:

- SecurityAttributesGroup
- SecurityAttributesOptionGroup

References to these attribute groups may be inserted into a complex type definition in order to include the names, declared values, and default values of the IC ISM attributes into the attribute list of any XML element.

As illustrated by the following figure, a reference to entity "%SecurityAttributes" will create an attribute definition list in a DTD in which **classification** and **ownerProducer** are REQUIRED and the other attributes are IMPLIED (*i.e.*, optional).

```
<!ENTITY % SecurityAttributes
    "classification (U | C | S | TS | R
                        NU | NR | NC | NS | NS-S | NS-A |
                        CTS | CTS-B | CTS-BALK |
                        CTSA | NSAT | NCA)
    ownerProducer NMTOKENS #REQUIRED
    SCIcontrols NMTOKENS #IMPLIED
    SARIdentifier NMTOKENS #IMPLIED
    FGIsorceOpen NMTOKENS #IMPLIED
    FGIsorceProtected NMTOKENS #IMPLIED
    disseminationControls NMTOKENS #IMPLIED
    releasableTo NMTOKENS #IMPLIED
    nonICmarkings NMTOKENS #IMPLIED
    classifiedBy CDATA #IMPLIED
    classificationReason CDATA #IMPLIED
    derivedFrom CDATA #IMPLIED
    declassDate NMTOKEN #IMPLIED
    declassException NMTOKENS #IMPLIED
    declassEvent CDATA #IMPLIED
    typeOfExemptedSource NMTOKENS #IMPLIED
    dateOfExemptedSource NMTOKEN #IMPLIED
    declassManualReview (true | false) #IMPLIED">
```

Figure 1. Entity "%SecurityAttributes"



In the WXS syntax, the same effect is accomplished by placing a reference to attribute group “SecurityAttributesGroup” in the type definition for the applicable element. The definition of “SecurityAttributesGroup” is:

```
<xsd:attributeGroup name="SecurityAttributesGroup">
  <xsd:attribute ref="classification" use="required"/>
  <xsd:attribute ref="ownerProducer" use="required"/>
  <xsd:attribute ref="SCIcontrols" use="optional"/>
  <xsd:attribute ref="SARIdentifier" use="optional"/>
  <xsd:attribute ref="FGISourceOpen" use="optional"/>
  <xsd:attribute ref="FGISourceProtected" use="optional"/>
  <xsd:attribute ref="disseminationControls" use="optional"/>
  <xsd:attribute ref="releasableTo" use="optional"/>
  <xsd:attribute ref="nonICmarkings" use="optional"/>
  <xsd:attribute ref="classifiedBy" use="optional"/>
  <xsd:attribute ref="classificationReason" use="optional"/>
  <xsd:attribute ref="derivedFrom" use="optional"/>
  <xsd:attribute ref="declassDate" use="optional"/>
  <xsd:attribute ref="declassException" use="optional"/>
  <xsd:attribute ref="declassEvent" use="optional"/>
  <xsd:attribute ref="typeOfExemptedSource" use="optional"/>
  <xsd:attribute ref="dateOfExemptedSource" use="optional"/>
  <xsd:attribute ref="declassManualReview" use="optional"/>
</xsd:attributeGroup>
```

**Figure 2. Attribute Group “SecurityAttributesGroup”**

Entity “%SecurityAttributes” and attribute group “SecurityAttributesGroup” are meant to be used with any XML element for which classification metadata is *required*.

The replacement text of entity “%SecurityAttributesOption” (Figure 3) is nearly identical to that of “%SecurityAttributes.” It differs only in that the default values of **classification** and **ownerProducer** are IMPLIED rather than REQUIRED.

```
<!ENTITY % SecurityAttributesOption
    "classification (U | C | S | TS | R
                    NU | NR | NC | NS | NS-S | NS-A |
                    CTS | CTS-B | CTS-BALK |
                    CTSA | NSAT | NCA)
    ownerProducer NMTOKENS #IMPLIED
    SCIcontrols NMTOKENS #IMPLIED
    SARIdentifier NMTOKENS #IMPLIED
    FGISourceOpen NMTOKENS #IMPLIED
    FGISourceProtected NMTOKENS #IMPLIED
    disseminationControls NMTOKENS #IMPLIED
    releasableTo NMTOKENS #IMPLIED
    nonICmarkings NMTOKENS #IMPLIED
    classifiedBy CDATA #IMPLIED
    classificationReason CDATA #IMPLIED
    derivedFrom CDATA #IMPLIED
    declassDate NMTOKEN #IMPLIED
    declassException NMTOKENS #IMPLIED
    declassEvent CDATA #IMPLIED
    typeOfExemptedSource NMTOKENS #IMPLIED
```

dateOfExemptedSource	NMTOKEN	#IMPLIED
declassManualReview	(true   false)	#IMPLIED">

**Figure 3. Entity “%SecurityAttributesOption”**

The corresponding WXS syntax is:

```
<xsd:attributeGroup name="SecurityAttributesOptionGroup">
  <xsd:attribute ref="classification" use="optional"/>
  <xsd:attribute ref="ownerProducer" use="optional"/>
  <xsd:attribute ref="SCIcontrols" use="optional"/>
  <xsd:attribute ref="SARIdentifier" use="optional"/>
  <xsd:attribute ref="FGISourceOpen" use="optional"/>
  <xsd:attribute ref="FGISourceProtected" use="optional"/>
  <xsd:attribute ref="disseminationControls" use="optional"/>
  <xsd:attribute ref="releasableTo" use="optional"/>
  <xsd:attribute ref="nonICmarkings" use="optional"/>
  <xsd:attribute ref="classifiedBy" use="optional"/>
  <xsd:attribute ref="classificationReason" use="optional"/>
  <xsd:attribute ref="derivedFrom" use="optional"/>
  <xsd:attribute ref="declassDate" use="optional"/>
  <xsd:attribute ref="declassException" use="optional"/>
  <xsd:attribute ref="declassEvent" use="optional"/>
  <xsd:attribute ref="typeOfExemptedSource" use="optional"/>
  <xsd:attribute ref="dateOfExemptedSource" use="optional"/>
  <xsd:attribute ref="declassManualReview" use="optional"/>
</xsd:attributeGroup>
```

**Figure 4. Attribute Group “SecurityAttributesOptionGroup”**

Entity “%SecurityAttributesOption” and attribute group “SecurityAttributesOptionGroup” are meant to be used with any XML element for which classification metadata may not *always* be required. Examples might be list items within parent lists or paragraphs, for which the classification and controls are set at the level of the parent element. However, even though the **classification** and **ownerProducer** attributes are declared to be optional, if one is used they both must be used whenever security attributes are specified for an element.

With respect to validation of the attributes as they appear in instance documents, the DTD and the WXS are functionally equivalent—with one important exception: the WXS has an associated XML namespace. For more on this, see [3.3](#), below.

## 2.3 The Controlled Vocabularies

CAPCO is the authority for the development and use of the classification marking system for the Intelligence Community. This system employs a uniform list of security classification and control markings authorized for all dissemination of classified (and unclassified) information, including hard-copy and electronic documents, by components of the IC. The IC MWG has developed a set of controlled vocabularies consisting of valid XML name tokens which are associated with the various general categories of security classification and control markings. The name tokens used in the controlled vocabularies that populate the IC ISM attribute values are based on the authorized portion marking abbreviations specified in the CAPCO Authorized Classification and Control Markings Register (reference [1](#)). In most cases, a name token used in a controlled vocabulary is identical to the actual CAPCO authorized portion marking abbreviation. In those few cases in which a CAPCO abbreviation does not meet the syntax requirements of an XML name token, this standard uses a substitute for the abbreviation. A

controlled vocabulary may be contained either within an enumerated list internal to the declaration of an attribute, or within an external document.

An internal enumerated list is used for attribute **classification**. In DTD syntax this list is called a name token group; in the WXS syntax it is a set of enumerations of type name token. The list is built into the declaration of the attribute as its declared value. The list provides choices to be used for the attribute value. In the DTD syntax, the name token group is:

```
(U | C | S | TS | R | NU | NR | NC | NS | NS-S | NS-A |
CTS | CTS-B | CTS-BALK | CTSA | NSAT | NCA)
```

This list is identical to the US and non-US classification portion marking abbreviations in the CAPCO Register.

In the WXS syntax, the set of enumerations looks like this:

```
<xsd:restriction base="xsd:NMTOKEN">
  <xsd:enumeration value="U"/>
  <xsd:enumeration value="C"/>
  <xsd:enumeration value="S"/>
  <xsd:enumeration value="TS"/>
  <xsd:enumeration value="R"/>
  <xsd:enumeration value="NU"/>
  <xsd:enumeration value="NR"/>
  <xsd:enumeration value="NC"/>
  <xsd:enumeration value="NS"/>
  <xsd:enumeration value="NS-S"/>
  <xsd:enumeration value="NS-A"/>
  <xsd:enumeration value="CTS"/>
  <xsd:enumeration value="CTS-B"/>
  <xsd:enumeration value="CTS-BALK"/>
  <xsd:enumeration value="CTSA"/>
  <xsd:enumeration value="NSAT"/>
  <xsd:enumeration value="NCA"/>
</xsd:restriction>
```

Attribute **declassManualReview** also uses an internal name token group in the DTD syntax. That group is:

```
(true | false)
```

In the WXS syntax, **declassManualReview** is declared to have the built-in data type "boolean" which, by definition, means that the permissible values are "true" and "false."

The IC ISM DTD and WXS do not include enumerated lists for the other attributes. The permissible values for those attributes are more subject to change and, consequently, users are expected to refer to authoritative sources for those lists.

In order to support implementation of IC ISM, however, several controlled vocabularies have been created and registered in the IC XML Registry as "domain value sets." Usage of the domain value sets is described and illustrated in section 6, below. As a sample, one of the domain value sets (for "INTnonICmarkings2004-04-30") is listed in [Appendix D](#). In section 7, where applicable, the domain value set for an attribute is identified.

## 2.4 Specifying Attribute Values

For attributes **classification** and **declassManualReview**, the value must be one of the name tokens in their internal controlled vocabularies. For example, to associate a classification with an XML element named “Figure” that contains confidential information, use a start tag like this:

```
<Figure classification="C" ... >
```

For attributes **classifiedBy**, **classificationReason**, **derivedFrom** and **declassEvent**, the declared values are character data (“CDATA”) in the attribute definition list in the DTD entity set, as shown in Figure 1 and Figure 3. These same attributes are declared to be of built-in data type “string” in the WXS. Therefore, the value for any of these attributes is simply a literal text string which may contain alphanumeric characters, spaces, symbols and other legal XML characters.

However, this is not to say that the format and content of a value can not be further restricted through configuration of authoring software by implementing organizations. In fact, it will at times even be necessary to restrict an attribute value in this way in order to comply with CAPCO guidelines. For example:

```
<Security ... derivedFrom="Multiple Sources"/>
```

Although the declared value of **derivedFrom** is just a text string, that string must be restricted to one of several forms: it may specify the title and date of a classification guide, the title and date of a source document, or the literal string “Multiple Sources.” This can only be enforced through software configuration.

The definitions of attributes **declassDate** and **dateOfExemptedSource** differ in the DTD version from the WXS version. In the DTD version, these attributes are declared to be of type “NMTOKEN.” This means that the value may consist only of the alphanumeric characters and the special characters hyphen (“-”), underscore (“\_”), period (“.”), and colon (“:”). It is intended that the value be an ISO 8601-compliant date, such as “2004-04-30.” Since this date format conforms to the syntax of a name token, a parser can perform at least a rudimentary check that the value is of an appropriate type.

In the WXS version, we take advantage of the built-in data type named “date.” This data type constrains the attribute values to the form “YYYY-MM-DD.”

For each of the other attributes the declared value is “NMTOKENS” (short for “name token list”). This means three things:

1. An attribute value may be a single name token or it may be a space-delimited list of name tokens, where each name token is taken from the associated external controlled vocabulary.
2. Each name token must conform to the syntax of an XML name token: that is it may consist only of the alphanumeric characters and the special characters hyphen (“-”), underscore (“\_”), period (“.”), and colon (“:”).
3. The attribute values are case sensitive: “SI” and “si” are not equivalent.

The reason that these attributes are declared to be of type “NMTOKENS” is that multiple controls may apply to the corresponding information for the category of control marking associated with the attribute.

Take these two examples:

```
<Para classification="TS" ... SCIcontrols="SI"> (a)
```

```
<Para classification="TS" ... SCIcontrols="SI TK"> (b)
```

In example (a) the **SCIcontrols** attribute contains a single value, "SI." In example (b), however, the **SCIcontrols** attribute contains two independent values, "SI" and "TK." The embedded space between the name tokens is only a delimiter. We know this because the declared value of **SCIcontrols** is "NMTOKENS." Note also that, since all of the values in these examples consist of just alphabetic characters, they conform to the syntax of a name token.

Here is another example in which the **releasableTo** attribute value is a space-delimited list of four name tokens:

```
<Para classification="S" ... disseminationControls="REL"
releasableTo="USA AUS CAN GBR">
```

It should be pointed out that the values in the IC ISM controlled vocabularies have been chosen so as to be valid XML name tokens. In the great majority of cases, the authorized portion marking abbreviations in the CAPCO Register already are valid name tokens. However, in a few cases, modified versions of the authorized portion marking abbreviations are used in the controlled vocabularies because the abbreviations, as they appear in the CAPCO Register, do not qualify as valid XML name tokens. For example, for the dissemination control "RESTRICTED DATA-SIGMA 1" marking title, the CAPCO authorized portion marking abbreviation is "RD-SG 1." The space between "SG" and "1" would not be permissible in an XML name token. Therefore, for IC ISM, "RD-SG-1" is used in the corresponding controlled vocabulary. It is up to XSLT stylesheets to transform the name tokens appropriately to generate the correct security markings.

## 2.5 Attributes with Dependent or Conditional Relationships

Numerous, and perhaps sometimes obvious, dependent or conditional relationships do exist between attributes, between attributes with certain values, between individual space-delimited name tokens within an attribute value, or between attributes and elements.

A few examples are:

1. Attributes **classification** and **ownerProducer** must be used together. Both are required in order to specify whether a document is a US document, a non-US document, or a joint document. (See [7.14](#), below.)
2. When (and only when) **typeOfExemptedSource** is used, **dateOfExemptedSource** must also be used.
3. When (and only when) **disseminationControls** contains the "REL" or "EYES" values, **releasableTo** must also be used. (See [7.10](#) and [7.15](#), below.)
4. Individual values within certain multi-valued attributes should be listed in a specific order. For example, the "USA" value (ISO 3166-1 country code trigraph) should always be listed first in the value of the **releasableTo** attribute. (See [7.15](#), below)
5. Many—in fact half—of the IC ISM attributes are meaningful primarily at the product level to provide the values for the classification/declassification block and the declassification parameter of the banners. These should be used as attributes of a portion-level element only when the intent is that the portion will be re-used.

These relationships are rooted in the “business rules” resulting from compliance to CAPCO classification and control marking guidelines, other relevant governances like Executive Order 12958 and ISOO Directive 1, and IC MWG guidelines.

An XML parser program will not, and cannot, enforce these business rules. Nor should XSLT stylesheets be expected to account for incorrect or inappropriate application of attributes or attribute values within XML documents. Business rules like these must be enforced through software configuration as part of the process of applying security marking metadata to XML documents within the digital production authoring environment, or other applications that create XML data streams. One approach by which implementing organizations can enforce business rules is briefly introduced in section [4](#).

## 2.6 Attributes with Specific Rules

The value of the **FGISourceProtected** attribute should be applicable ISO 3166-1 country code trigraphs listed in alphabetical order, followed by applicable registered international organization tetragraphs listed in alphabetical order, identifying the country or countries and/or international organization(s) that furnished information content. As the name of the attribute suggests, the identity of the source(s) of the information is to be protected and should not be disclosed. Therefore, additional measures should be taken so that the value(s) of this attribute should never be displayed or disseminated in the ICSIS shared spaces.

By contrast, when the identity of the country or countries and/or international organization(s) may be disclosed and may appear in portion marks and security banners, the **FGISourceOpen** attribute should be used.

### 3 Guidelines for Interoperability

The IC ISM DTD entity set and WXS are available from both the IC MWG web sites and the IC XML Registry. On the web sites, the entity set is in a file named “IC-ISM-v2.ent” and the WXS is in a file named “IC-ISM-v2.xsd”. In the IC XML Registry, the resource names are “IC\_ISM\_Entities” and “IC\_ISM\_WXS”. They are resources of type “XML Schema Document” in the “INT” registry namespace.

#### 3.1 Integrating the IC ISM Entity Set

The IC ISM DTD entity set may be included by reference in any XML DTD. This requires adding an entity declaration and an entity reference to the DTD. First, declare a parameter entity for the IC ISM entity set file. In the following example, a parameter entity named “IC-Security-Entities” is declared. The replacement text of the entity, “IC-ISM-v2.ent,” is a uniform resource locator (URL) for the entity set file.

```
<!ENTITY % IC-Security-Entities SYSTEM "IC-ISM-v2.ent">
```

Next, place a parameter-entity reference in the DTD at the point at which the IC ISM entity set should be included. The following example shows a parameter-entity reference. When an XML parser encounters this reference, it will retrieve the file “IC-ISM-v2.ent” and read it as if it were part of the parent DTD at the location of the reference.

```
%IC-Security-Entities;
```

Because the IC ISM DTD entity set is itself a set of parameter entity declarations, it should be included near the beginning of a DTD, before any references to the IC ISM entities are used.

Once the IC ISM entity set has been included, the IC ISM parameter entities may be referenced in the attribute definition list of any element. The next example shows the element declaration and attribute definition list declaration for a hypothetical element named “Target”:

```
<!ELEMENT Target          (#PCDATA) >
<!ATTLIST Target
    BNumber      CDATA      #REQUIRED
    Osuffix      CDATA      #IMPLIED
    categoryCode CDATA      #IMPLIED
    %SecurityAttributes;    >
```

The attribute definition list of “Target” includes—in addition to attributes named “BNumber,” “Osuffix” and “categoryCode”—all of the IC ISM attributes.

#### 3.2 Integrating the IC ISM W3C XML Schema

The IC ISM W3C XML Schema may be included by reference in any XML schema. This requires declaring the IC ISM version 2 namespace, and inserting an “import” statement into the schema. First, declare the namespace for the IC ISM WXS file. In the following example, a namespace prefix, “ism,” is declared for the IC ISM XML namespace.

```
<xsd:schema
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:ism="urn:us:gov:ic:ism:v2">
```

Next, insert an “import” statement into the schema at the point at which the IC ISM WXS should be included. The following example shows an “import” statement that tells an XML parser to import schema declarations applicable to the “urn:us:gov:ic:ism:v2” namespace from the URL prescribed by the “schemaLocation” attribute.

```
<xsd:import
  namespace="urn:us:gov:ic:ism:v2"
  schemaLocation="IC-ISM-v2.xsd" />
```

Once the IC ISM WXS has been included, the IC ISM attributes may be referenced in the attribute list of any element. The next example shows the declarations for the example “Target” element in the WXS syntax:

```
<xsd:element name="Target">
  <xsd:complexType>
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="BNumber" type="xsd:string"
          use="required" />
        <xsd:attribute name="Osuffix" type="xsd:string"
          use="optional" />
        <xsd:attribute name="categoryCode"
          type="xsd:string" use="optional" />
        <xsd:attributeGroup
          ref="ism:SecurityAttributesGroup" />
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
</xsd:element>
```

### 3.3 Namespaces

As shown above, the WXS version of IC ISM declares an XML namespace for the schema. The name of that namespace is “urn:us:gov:ic:ism:v2.” The purpose of declaring such a namespace is to facilitate importation of the IC ISM schema into another schema without having to be concerned about conflicts between distinct attribute types that have the same name. For example, the IC ISM attribute **classification** can be used within another schema even when the other schema also declares an attribute named “classification.”

In instance documents, the name of an attribute is considered to include the namespace name. Consequently, the full name of **classification** becomes **urn:us:gov:ic:ism:v2:classification**. In order to avoid unwieldy names, prefixes are used in place of namespace names. In the example of element “Target” in the preceding section, the prefix that was assigned to the IC ISM namespace name was “ism.” In a document that is to be validated against a WXS, the element would be used like this:

```
<Target ism:classification="U"
  ism:ownerProducer="USA"
  BNumber="1234DD5678"
  Osuffix="DD123"
  categoryCode="1234">ammunition plant</Target>
```

Since DTD syntax predated the advent of XML namespaces, DTD parsers do not interpret namespace names or prefixes. Consequently, the current version of the IC ISM DTD entity set



does not make use of namespaces. When DTDs are being used to validate an XML document, the target example would be written like this:

```
<Target classification="U"
        ownerProducer="USA"
        BEnumber="1234DD5678"
        Osuffix="DD123"
        categoryCode="1234">ammunition plant</Target>
```

In DTD usage, it is the responsibility of the organization that develops the parent DTD to be sure that none of the attributes defined for an element conflict with the IC ISM attributes that will be used with that element.

In this document, most of the examples were originally created with DTD implementations in mind. Consequently, the examples do not show namespace prefixes.

### 3.4 XML Registry

XML registries are a vital component in the implementation of shared data exchanges. Developers looking to express information using XML need support in establishing common lexicons and grammars. A registry should be the reference point for obtaining the latest DTDs, schemas, controlled vocabularies, templates and sample documents. Currently, the IC XML Registry (<http://diides.ncr.disa.mil/xmlreg/user/index.cfm>) contains the latest IC ISM components and documentation.

Implementing organizations are encouraged to register any extensions to the IC ISM DTD entity set and schema so that developers may avoid repeating efforts underway at other agencies, reduce overall development efforts, and ensure compatibility.

### 3.5 Customizing the IC ISM DTD Entity Set or WXS for Internal Use

IC ISM has been specifically designed to allow for extensions. Changes to the standard may be necessary to support internal requirements of a specific agency or community of interest. Any extensions or changes made to the standard should be maintained as a separate, organizational representation.

Organizations may extend the IC ISM entity set and schema *for internal use only*. The goal of such extensibility of security metadata is to meet each organization's internal or bilateral requirements, while maintaining a common set of security metadata to allow sharing of information throughout the IC.

#### 3.5.1 Extending or Restricting the Attributes

The extensible nature of XML allows IC ISM to be customized for additional attributes. In this way, agency-specific attributes may be incorporated into a document model. This is best accomplished through the use of locally declared parameter entities in an agency-specific DTD, or locally declared attributes or attribute groups in an agency-specific schema. The agency-specific DTD or schema, sometimes called a driver DTD or driver schema, would define all agency-specific extensions and call in all external modules including the IC ISM Entity Set or IC ISM WXS. This method keeps the IC ISM Entity Set and IC ISM WXS free from internal modification. Later, if the IC ISM Entity Set and IC ISM WXS are revised, the new versions can replace the older versions without impacting local modifications.

In the following example, part (a) illustrates how an organization can declare a local parameter entity that has, as its replacement text, the parameters for two attribute declarations—one named “localMarkings” and the other named “FDO”. Part (b) illustrates how the locally-defined entity can be referenced as part of an element’s attribute definition list to associate the two local attributes, along with the IC ISM security attributes, with an element named “Para”. Part (c) shows the element and attribute definition list declarations with the replacement text substituted for the parameter entity references.

```
<!ENTITY % LocalSecurityAttributes                                (a)
    "localMarkings NMTOKENS #IMPLIED
    FDO             CDATA      #IMPLIED" >
```

```
-----

<!ELEMENT Para          (#PCDATA) >                                (b)
<!ATTLIST Para
    %SecurityAttributes;
    %LocalSecurityAttributes; >
```

```
-----

<!ELEMENT Para          (#PCDATA) >                                (c)
<!ATTLIST Para
    classification      (U | C | S | TS | R
                        NU | NR | NC | NS | NS-S | NS-A |
                        CTS | CTS-B | CTS-BALK |
                        CTSA | NSAT | NCA)
    ownerProducer       NMTOKENS      #REQUIRED
    SCIcontrols         NMTOKENS      #IMPLIED
    SARIdentifier        NMTOKENS      #IMPLIED
    FGIsorceOpen        NMTOKENS      #IMPLIED
    FGIsorceProtected   NMTOKENS      #IMPLIED
    disseminationControls NMTOKENS    #IMPLIED
    releasableTo        NMTOKENS      #IMPLIED
    nonICmarkings       NMTOKENS      #IMPLIED
    classifiedBy         CDATA         #IMPLIED
    classificationReason CDATA         #IMPLIED
    derivedFrom          CDATA         #IMPLIED
    declassDate          NMTOKENS      #IMPLIED
    declassException     NMTOKENS      #IMPLIED
    declassEvent         CDATA         #IMPLIED
    typeOfExemptedSource NMTOKENS      #IMPLIED
    dateOfExemptedSource NMTOKEN      #IMPLIED
    declassManualReview (true | false) #IMPLIED
    localMarkings       NMTOKENS      #IMPLIED
    FDO                 CDATA         #IMPLIED>
```

In the following example, part (a) illustrates how an organization can declare a local attribute group that has, as its replacement text, the attribute references for two attribute declarations—one named “localMarkings” and the other named “FDO”. Part (b) illustrates how the locally-defined attribute group can be referenced as part of an element’s attribute reference list to associate the two local attributes, along with the IC ISM security attributes, with an element named “Para”.

```
<xsd:attributeGroup name="LocalSecurityAttributesGroup">
  <xsd:attribute ref="localMarkings" use="optional"/>
  <xsd:attribute ref="FDO" use="optional"/>
</xsd:attributeGroup>
```

(a)

```
<xsd:element name="Para" type="xsd:string"/>
<xsd:complexType>
  <xsd:attributeGroup ref="ism:SecurityAttributesGroup"/>
  <xsd:attributeGroup ref="ism:LocalSecurityAttributesGroup"/>
</xsd:complexType>
</xsd:element>
```

(b)

### 3.5.2 Extending or Restricting the Controlled Vocabularies

Additional controlled vocabularies or additions and subtractions to the current controlled vocabularies are possible within an agency's controlled space. Changes to the controlled vocabularies do not affect the functionality of the IC ISM entity set. The values used in the controlled vocabularies are recognized by the XML parser as name tokens. The XML parser does not validate the name tokens themselves. Therefore, care must be taken to ensure that any changes to the existing controlled vocabularies are the actual name token values to be stored.

Care must be exercised in order to maintain consistency in stored values. Conversion scripts can be written to correct many inconsistencies, but tighter control and handling of the controlled vocabularies would make more practical sense, and guarantee greater data reliability from the producer and for the consumer.

## 3.6 Creating Stylesheets

One of the guiding principals of XML is that information content within an XML document is independent of any presentation format. To the greatest degree practical, format-oriented markup should be kept out of XML documents. Therefore, in order to be rendered in a useful format, XML documents require accompanying stylesheets. Using the Extensible Stylesheet Language (XSL) (reference [7](#)), developers can convert XML content for display in a web browser, into Portable Document Format (PDF) for hardcopy printing, into other XML hierarchies, into text files such as Rich Text Format (RTF), *etc.*

Each publishing organization will need to create stylesheets for web and print delivery that adhere to the styling guidelines specific to that organization. The "XSL for Transformations" (XSLT) declarative transformation language is the recommended method for creating web pages from XML documents. "XSL for Formatting Objects" (XSLFO) should be used to create PDF output and input for layout and pagination software. Stylesheets for each output type may be created to allow for publishing to various formats to meet the specific requirements of individuals and organizations.

XSLT stylesheets that process the IC ISM attributes to create portion markings, security banners and classification/declassification blocks are available from the IC MWG web sites.

For those who choose to develop their own stylesheets, here are some guidelines:

- Use attributes **classification** and **ownerProducer** together to determine whether to output a US classification parameter, non-US classification parameter, or joint classification parameter.

- Expect the tokens in list-valued attributes to be in the order prescribed by the CAPCO Register. In other words, it should not be necessary to sort the list of values.
- Use the appropriate separators when displaying multiple values from list-valued attributes. The lists for **ownerProducer**, **FGISourceOpen**, and **releasableTo** are all formatted differently, and **releasableTo** is formatted differently when it is used in conjunction with “REL” and in conjunction with “EYES.”
- Transform date values (in **declassDate** and **dateOfExemptedSource**) from the YYYY-MM-DD format to YYYYMMDD for display.
- Transform the tokenized control values that differ from the CAPCO abbreviations to the CAPCO form; for example, transform the **disseminationControls** value “RD-SG-1” to “RD-SG 1” for display.
- If the value list for **disseminationControls** contains “EYES” or “REL,” find the list of country codes and international organization codes in attribute **releasableTo**.
- Output “MR” in the banners if any of the conditions listed in section [7.8.3](#) apply.
- If more than one of the attributes **declassDate**, **declassEvent**, **declassException**, and **typeOfExemptedSource** are present, a stylesheet must determine what to put in the banners and classification/declassification block. If **declassEvent** or **typeOfExemptedSource** is present, or if **declassException** is present and equals “25X1-human,” put “MR” in the banners. If **declassDate** and **declassException** are present and **declassException** is not equal to “25X1-human, put the first 25X token in the banners.

Most of the transformations described by these guidelines are illustrated in section [7](#).

## 4 Data Input Techniques

It is not the intent of the IC MWG that the security attributes be populated manually. The IC security attributes were developed as a set of containers for CAPCO-authorized classification and control markings. Use of the attributes, by themselves, does not guarantee that an appropriate combination of attributes and attribute values has been specified for any given portion or product in order to produce valid portion markings, a valid top and bottom security banner and a valid classification/declassification block. Due to the potentially complex business rules associated with properly marking classified information, the use of a forms-based software interface will provide the best method of creating and storing the security markup.

Business rules, except for basic classification, were not incorporated in IC ISM for several reasons:

- Updates can be incorporated more easily into the model.
- Business rules regarding security metadata are constantly under revision.
- The model can be customized to meet the requirements of each organization.

It will be an organization's responsibility to understand and incorporate the required business practices for security metadata.

### 4.1 Graphical User Interfaces

A security marking GUI should provide a user with all of the valid CAPCO security marking options for the context in which s/he works. Business rules to support relationships of the CAPCO security markings can be incorporated into the GUI. However, most likely the GUI itself—that is, the form—will not provide the logic for validating the overall classification of a product. The use of “roll-up” scripts and human review will ensure the information is properly marked for archiving and distribution.

[Figure 5](#) shows a notional GUI with tabbed pages for the classification and controls options. It is likely that many workable forms-based and other approaches for assisting with the entry of correct classification markings can be devised. This figure serves only to illustrate the idea. It illustrates selection options for US classification and controls.

This particular user interface makes use of XML helper files that contain the requisite controlled vocabularies. The data stored in the helper files is used to populate the dialog's list boxes and check boxes. This method keeps the controlled vocabularies external to the GUI code so that changes to the controlled vocabularies do not necessarily render the code obsolete.

The XML helper files are text files that can be updated easily by an administrator or authorized user in a text editor or XML authoring tool. An organization can easily customize these files to limit or extend the security markings used by that organization.

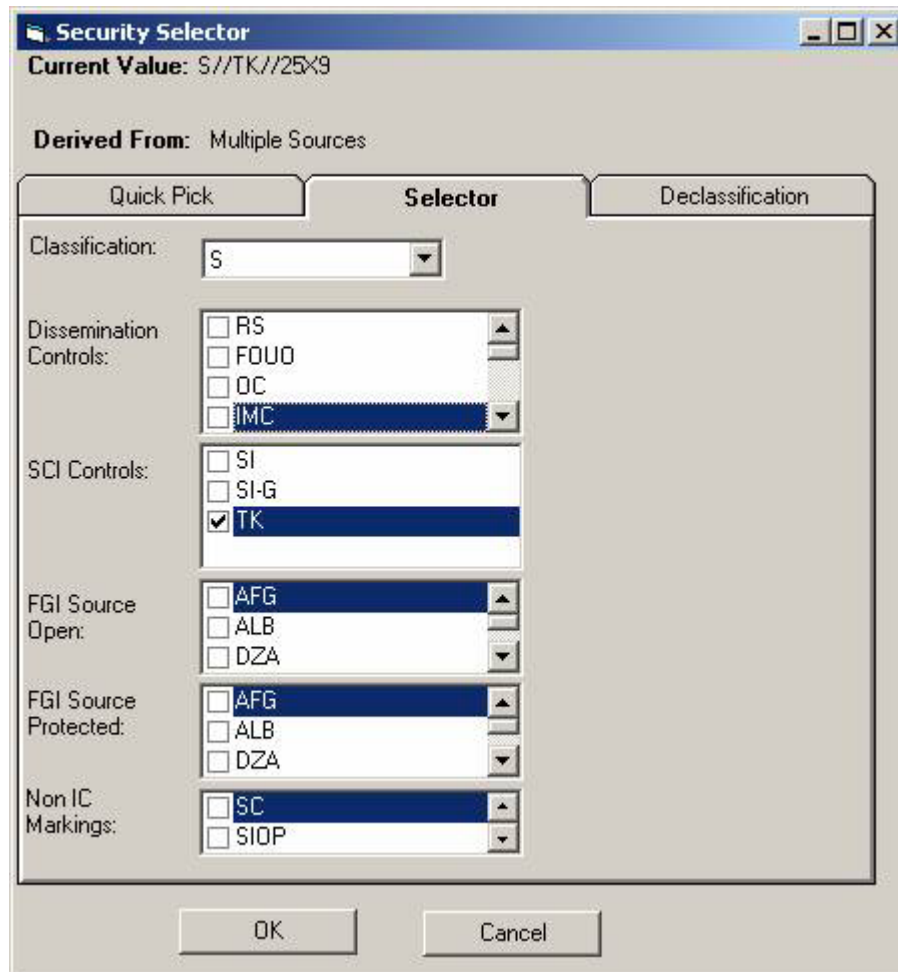
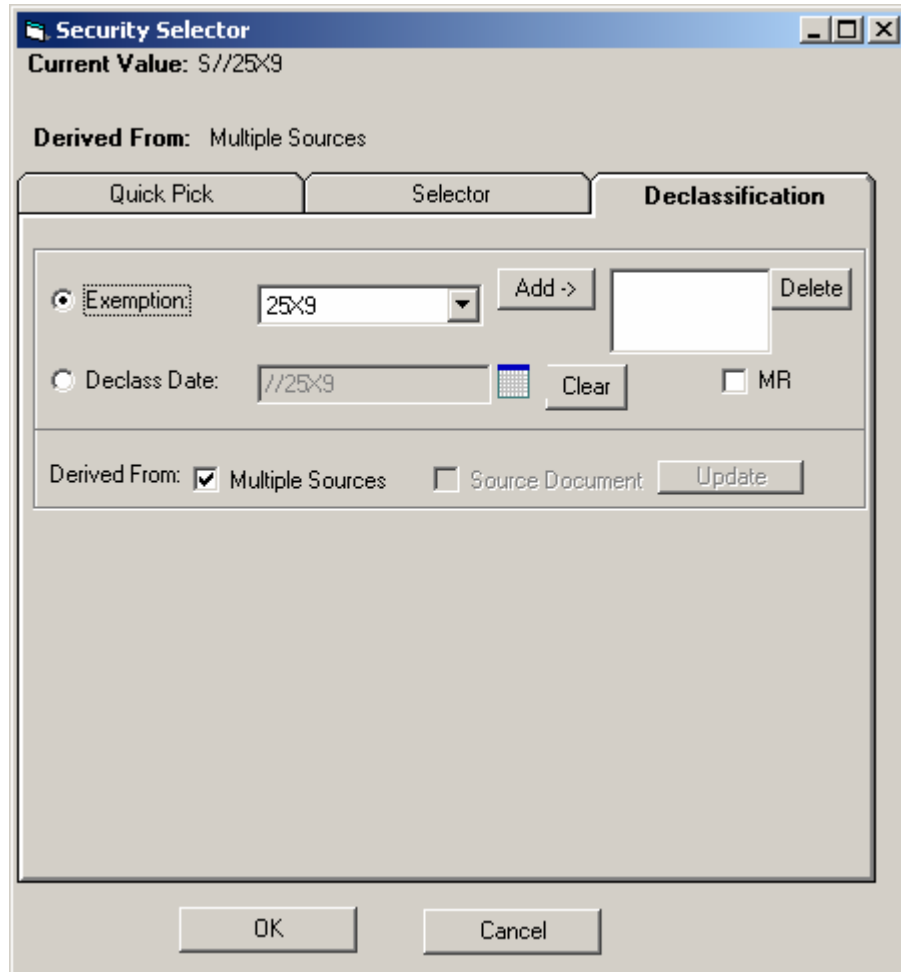


Figure 5. Security GUI with US Security Marking Options Displayed

[Figure 6](#) illustrates a GUI that assists an author with selection of options for the classification/declassification block and the declassification parameter of the banners..



**Figure 6. GUI for Selection of Declassification**

Here is an example of a simple helper file that can be used in conjunction with a GUI. Once again, this is just one potentially useful approach to maintaining the controlled vocabularies in separate files. Some implementers of digital authoring solutions use XML topic maps for the vocabularies. In any case, the helper files are read by the GUI software to populate the various list and check boxes.

This example of a helper file is an XML document that contains a concatenation of the controlled vocabularies used by the IC ISM attributes.

```
<?xml version="1.0" ?>
<codes>
  <vocab name="nonICmarkings">
    <code>SC</code>
    <code>SIOP</code>
    <code>SINFO</code>
    <code>DS</code>
    <code>XD</code>
    <code>ND</code>
    <code>SBU</code>
    <code>SBU-NF</code>
```

```

</vocab>
<vocab name="disseminationControls">
  <code>RS</code>
  <code>FOUO</code>
  <code>OC</code>
  ...
  <code>DSEN</code>
</vocab>
<vocab name="SCIcontrols">
  <code>SI</code>
  <code>SI-G</code>
  <code>SI-ECI-XXX</code>
  <code>TK</code>
</vocab>
<vocab name="FGISourceOpen">
  <code>AFG</code>
  <code>ALB</code>
  <code>ASM</code>
  <code>DZA</code>
  ...
  <code>SFOR</code>
  <code>UNKNOWN</code>
</vocab>
<vocab name="FGISourceProtected">
  <code>AFG</code>
  <code>ALB</code>
  <code>ASM</code>
  <code>DZA</code>
  ...
  <code>SFOR</code>
</vocab>
<vocab name="nonUScountries">
  <code>AFG</code>
  <code>ALB</code>
  <code>ASM</code>
  <code>DZA</code>
  ...
  <code>ZWE</code>
</vocab>
<vocab name="nonUSclassifications">
  <code>TS</code>
  <code>S</code>
  <code>C</code>
  <code>R</code>
  <code>U</code>
  <code>FGI</code>
  <code>CTS</code>
  <code>CTS-B</code>
  ...
  <code>NCA</code>
</vocab>
</codes>

```



## 4.2 Manual Data Input

Lacking a software application that contains the CAPCO logic and presents a GUI, users may enter security markup into the XML directly using a text editor or an XML-aware authoring application that includes dialogs for setting attribute values. Due to the interrelationships among classification and control markings, users must be well versed in CAPCO and/or organizational guidelines and business rules when entering attributes directly.

Usage examples of the attributes along with associated controlled vocabularies are provided in this IC ISM Implementation Guide. See the IC ISM DED for data element definitions of the IC ISM attributes. The DED will give the user an understanding of each attribute's allowed values and a complete definition.

## 5 Operations on the Security Attributes

Once the IC ISM attributes are populated in an XML document or data stream, the attributes can be used for several key requirements:

1. formatting portion marks, the top and bottom security banner and the classification/declassification block for display, in authoring or editing applications, in web pages, or in print-oriented outputs (such as Portable Document Format files);
2. rolling up the attribute values assigned to child elements in order to determine the classification and controls of the parent element; and
3. filtering documents that have been written for multiple security domains in order to produce domain-specific outputs for dissemination.

### 5.1 Creating Portion Marks

The values of the IC ISM attributes for any given portion-level element will be used to format the corresponding portion mark for display purposes. An XSLT stylesheet may be used to create the portion mark string based on the values of the attributes.

Consider the following example for an element named “Para” in an XML document.

```
<Para classification="S" ownerProducer="USA" SCIcontrols="SI"
disseminationControls="REL" releasableTo="USA CAN GBR">
```

An XSLT stylesheet can be used to create the following portion mark string and place it at the beginning of the paragraph text.

```
(S//SI//REL TO USA, CAN and GBR)
```

### 5.2 Security Rollup

“Security Rollup” can be described as the process of deriving or determining the appropriate set of classification and control marking attributes and their values for a document, data stream or block element, based on all of the classification and control marking attributes and attribute values for subordinate elements found within the document, data stream or block element. The security rollup process is most often associated with determining the set of product-level security attributes which are used to form the security banner (high-water marking) that is displayed at the top and bottom of a document, and to form a document’s classification/declassification block. The security rollup functionality and methodology may be simple or very complex depending on the extent of security markings for which an organization needs to account.

With respect to the process of authoring a document, a security rollup may be repeatedly performed while a document is being authored. Within the authoring tool, the author may call the rollup function manually at any time, and/or a rollup will be performed automatically prior to closing any authoring session and saving the document. From an authoring standpoint, a security rollup can ensure that the document’s high-water marking will be at least at the level necessary based on the classification and control markings of the document’s current content. When a rollup is performed, an author can then verify that a document’s high-water marking is appropriate with respect to the current content, and then either accept the results of the rollup, or modify the results to designate a higher classification level if necessary.

As part of a post-authoring process, security rollup can be included in a filtering process for domain transformation (discussed below). Any automated rollup processes should be followed

by human review and verification to ensure proper markings before dissemination of the documents to the community space.

The name token values in the IC ISM controlled vocabularies duplicate, in almost all cases, the abbreviations used in portion markings authorized by CAPCO. This facilitates the straightforward generation of CAPCO-compliant portion markings with a minimum of transformation effort using attribute values containing name tokens from the controlled vocabularies. However, the generation of CAPCO-compliant security banner markings from the product-level security attributes will require more significant transformation.

### 5.3 Performing Domain Filtering

The IC ISM DTD entity set and WXS enable the process of domain filtering through automated methods. Domain filtering allows a document or portions of a document to be filtered and combined using XSLT stylesheets to form products that can be disseminated to various networking domains based on the classification and/or releasability requirements of the domain. For example, Top Secret portions of a document can be automatically stripped out using an appropriate XSLT stylesheet so that the resulting document can be disseminated to a Secret network. A single XSLT stylesheet can be used to perform all domain-filtering activities. However, it may be more practical and feasible to modularize the filtering process across multiple stylesheets.

## 6 Using the Controlled Vocabularies

As noted above, an XML name token (NMTOKEN) consists of a string of one or more letters, digits, hyphens, underscores, periods, and colons. Most of the IC ISM attributes require a name token or a space-delimited list of name tokens as values. As also noted, there are a relatively small number of instances when CAPCO-authorized abbreviations do not qualify as name tokens and substitutes are used. The name tokens that are the permissible values for the various IC ISM attributes are specified in controlled vocabularies.

For attribute **classification**, the controlled vocabulary is built into the attribute declaration as a name token group in the DTD entity set and as a list of enumerations in the WXS. A validating XML parser will use the name token list or enumeration list to ensure that the value of **classification** is one of the permissible values. The controlled vocabulary for classification is internal to the DTD entity set and WXS because it was the expectation of the IC ISM developers that the permissible values were very stable and would change only infrequently.

For the other attributes with controlled vocabularies the vocabularies are not built into the declarations. They are external domain value sets. They were kept out of the declarations in anticipation that they would change relatively frequently. They are documented in this guide and they exist in digital form in the IC XML Registry. It should be understood that there is no mechanism by which an XML parser can ensure that the name tokens it finds are actually taken from any of the external controlled vocabularies. All the parser can do in this case is verify that an attribute value is in fact a name token or a space-delimited list of name tokens. It is the responsibility of implementing organizations to provide a means for authors and editors to have access to the associated controlled vocabularies when selecting values for the IC ISM attributes, and to restrict the population of attribute values to name tokens contained in those controlled vocabularies.

In some cases the domain value space of an attribute consists of two domain value sets. This is true for those attributes that specify ISO 3166-1 country trigraphs *and/or* CAPCO-defined international organization tetragraphs.

### 6.1 Replacing, Extending and Sharing

Replacing or extending the controlled vocabularies to meet the internal requirements of an organization is rather trivial. Remember, an XML parser does not validate the actual name tokens used. It only checks for unallowable characters in the name tokens.

In order to replace or extend the controlled vocabularies, an organization should first determine which of the current name tokens are relevant for its use, and then define any additional name tokens if necessary. The organization should distribute the list of “new” name tokens to authors and reviewers within the organization (see section [4.2](#)), or integrate the new name tokens into XML helper files for a “Security GUI” as suggested in section [4.1](#). Obviously, because of the probability of manual input errors, checks must be utilized to ensure consistent marking and conformance to the new controlled vocabularies. Similar checks should be utilized if these controlled vocabularies are shared with other organizations.

---

*Caveat:* Any agency-specific name tokens must be removed prior to dissemination of the document’s contents into the IC shared space.

---

## 6.2 Controlled Vocabulary Listings

Each of the following attributes has one or two associated external domain value sets. The contents of the domain value sets are illustrated in Section [7](#).

- **declassException** (Section [7.7](#))
- **disseminationControls** (Section [7.10](#))
- **FGISourceOpen** (Section [7.11](#))
- **FGISourceProtected** (Section [7.12](#))
- **nonICmarkings** (Section [7.13](#))
- **ownerProducer** (Section [7.14](#))
- **releasableTo** (Section [7.15](#))
- **SCIcontrols** (Section [7.17](#))
- **typeOfExemptedSource** (Section [7.18](#))

The domain value sets are maintained as XML instances in the IC XML Registry, the vocabularies are registered as domain value documents, as explained in section [2.2](#). The XML schema for the domain value document type is also available in the Registry.

## 7 Attribute Value Specifications

The following subsections—one for each of the 18 IC ISM attributes—show the permissible values for the attributes and the corresponding formatted marking. Also shown are usage examples. Note that this section shows only unclassified permissible values. Consult the CAPCO Register (reference [1](#)) for the complete sets.

It is important to recognize that this is not an official reference for the CAPCO markings. The CAPCO Register and Implementation Manual (reference [2](#)) are the authoritative sources for most of the abbreviations and markings. International Standard ISO 3166-1 is the authoritative source for country trigraph codes. The authoritative sources for the business rules are the CAPCO Implementation Manual, ISOO Directive 1 (reference [4](#)), and Executive Orders 12958 and 12951.

In the following tables, the values in the “Authorized Abbreviation” and “Marking Title” columns are for displaying the stored values in the top and bottom security banner. Several samples are provided to illustrate how the controlled vocabulary name tokens are incorporated into the XML markup.

### 7.1 classification

This attribute is used at both the product and the element levels to identify the highest level of classification of the information. It is manifested in portion marks and security banners.

#### 7.1.1 Authorized Values

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
TS		TOP SECRET
S		SECRET
C		CONFIDENTIAL
U		UNCLASSIFIED
R		RESTRICTED
CTS		COSMIC TOP SECRET
CTS-B		COSMIC TOP SECRET-BOHEMIA
CTS-BALK		COSMIC TOP SECRET-BALK
NS		NATO SECRET
NS-S		NATO SECRET-SAVATE
NS-A		NATO SECRET-AVICULA
NC		NATO CONFIDENTIAL

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
NR		NATO RESTRICTED
NU		NATO UNCLASSIFIED
CTSA		COSMIC TOP SECRET ATOMAL
NSAT		SECRET ATOMAL
NCA		CONFIDENTIAL ATOMAL

### 7.1.2 Examples

XML Markup	Display Values
<b>classification="C"</b> ownerProducer="USA" disseminationControls="OC REL" releasableTo="USA AUS GBR" declassDate="2007-04-01"	<b>Security Banner</b> <b>CONFIDENTIAL</b> //ORCON,REL TO USA, AUS and GBR//20070401
<b>classification="NS"</b> ownerProducer="NATO" declassDate="2005-08-01"	<b>Security Banner</b> // <b>NATO SECRET</b> //MR
<b>classification="TS"</b> ownerProducer="USA" SCIcontrols="SI" disseminationControls="REL" releasableTo="USA AUS GBR"	<b>Portion Mark</b> <b>TS</b> //SI//REL TO USA, AUS and GBR
<b>classification="CTS-B"</b> ownerProducer="NATO" FGIsorceOpen="NATO"	<b>Portion Mark</b> // <b>CTS-B</b>

### 7.1.3 Notes

1. Attribute **classification** must always be used in conjunction with attribute **ownerProducer**. The two together determine the classification and the type of classification—US, non-US, or joint.
  - When **ownerProducer** equals "USA," the classification is a US classification, and the permissible values are U, C, S and TS.
  - When **ownerProducer** equals "NATO," the classification is a non-US classification and the permissible values are the NATO classifications: CTS, CTS-B, CTS-BALK, NS, NS-S, NS-A, NC, NR, NU, CTSA, NSAT, and NCA.
  - When **ownerProducer** equals a country trigraph or international organization tetragraph other than "USA" or "NATO," the classification is a non-US classification and the permissible values are U, R, C, S and TS.

- When **ownerProducer** equals a multi-valued list of trigraphs and/or tetragraphs, the classification is a joint classification. If “USA” is one of the **ownerProducer** values, the permissible classifications are U, C, S and TS. If “USA” is not one of the **ownerProducer** values, the permissible classifications are U, R, C, S and TS.
2. Although this attribute is technically optional when the %SecurityAttributesOption entity is applied to an element by a DTD or schema, this attribute along with the “ownerProducer” attribute must always be used and an attribute value must be explicitly indicated when security attributes are specify specified for an element.

## 7.2 classificationReason

This attribute is used primarily at the product level to specify the basis for an original classification decision. It is manifested only in the “Reason” line of a document’s Classification/Declassification block.

### 7.2.1 Examples

XML Markup	Display Values
<code>classificationReason="1.4(b)"</code>	Classification/Declassification Block Reason: 1.4(b)
<code>classificationReason="1.4(b) 1.4(d)"</code>	Classification/Declassification Block Reason: 1.4(b) 1.4(d)
<code>classificationReason="Foreign Government Information"</code>	Classification/Declassification Block Reason: Foreign Government Information

### 7.2.2 Notes

1. The attribute value may be a citation of one or more of the subparagraphs 1.4(a) through 1.4(h) of EO 12958 Amended, or other explanatory text.
2. When the reason for classification is not apparent from the content of the information, the original classification authority shall provide a more detailed explanation of the reason for classification.

## 7.3 classifiedBy

This attribute is used primarily at the product level to specify the identity, by name or personal identifier, and position title of the original classification authority for a resource. It is manifested only in the “Classified By” line of a document’s Classification/Declassification block.



### 7.3.1 Examples

XML Markup	Display Values
<code>classifiedBy="John Doe, Position Title"</code>	<b>Classification/Declassification Block</b> Classified By: John Doe, Position Title
<code>classifiedBy="ID#, Position Title"</code>	<b>Classification/Declassification Block</b> Classified By: ID#, Position Title

## 7.4 dateOfExemptedSource

This attribute is used primarily at the product level to specify the year, month and day of publication or release of a source document, or the most recent source document, that was itself marked with OADR or X1 through X8. It is manifested only in the "Declassify On" line of a document's Classification/Declassification block.

### 7.4.1 Examples

XML Markup	Display Values
<code>typeOfExemptedSource="OADR"</code> <code>dateOfExemptedSource="1990-10-20"</code>	<b>Classification/Declassification Block</b> Declassify On: Source Marked "OADR", Date of Source: 19901020
<code>typeOfExemptedSource="X1"</code> <code>dateOfExemptedSource="2000-10-20"</code>	<b>Classification/Declassification Block</b> Declassify On: Source Marked "X1", Date of Source: 20001020

### 7.4.2 Notes

1. This attribute should only be used in conjunction with attribute **typeOfExemptedSource**.
2. When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the attribute's value shall reflect the longest duration of any of its sources (*i.e.*, the date of origin of the most recent source).
3. This attribute's value should conform to the YYYY-MM-DD format. It should be transformed to YYYYMMDD for presentation.

## 7.5 declassDate

This attribute is used primarily at the product level to specify a year, month and day for declassification, upon the occurrence of which the information shall be automatically declassified. It is manifested in the declassification date parameter of a document's security banners and in the "Declassify On" line of a document's classification/declassification block.

### 7.5.1 Examples

XML Markup	Display Values
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI" declassDate="2010-01-01"</pre>	<p><b>Security Banner</b></p> <p>TOP SECRET//COMINT//<b>20100101</b></p> <p><b>Classification/Declassification Block</b></p> <p>Declassify On: <b>20100101</b></p>

### 7.5.2 Notes

1. This attribute's value should conform to the YYYY-MM-DD format. It should be transformed to YYYYMMDD for presentation.
2. Inclusion of this attribute's value in the Declassification Date field of a document's security banners may be overridden by programmatic determinations which require the declassification date parameter to be "MR", indicating that "manual review" is required for declassification of the information. However, the declassification date will still be specified in the document's classification/declassification block.

## 7.6 declassEvent

This attribute is used primarily at the product level to specify a description of an event for declassification, upon the occurrence of which the information shall be automatically declassified. It is manifested only in the "Declassify On" line of a document's classification/declassification block.

### 7.6.1 Examples

XML Markup	Display Values
<pre>declassEvent="Return of POTUS from Iraq"</pre>	<p><b>Classification/Declassification Block</b></p> <p>Declassify On: <b>Return of POTUS from Iraq</b></p>

### 7.6.2 Notes

1. When this attribute is used, the Declassification Date field of a document's security banners must be "MR", indicating that "manual review" is required for declassification of the information.

## 7.7 declassException

This attribute is used primarily at the product level to specify one or more exceptions to the nominal 25-year point for automatic declassification. It is manifested in the declassification date field of a document's security banners and in the "Declassify On" line of a document's classification/declassification block.

### 7.7.1 Authorized Values

Value	Description
25X1-human	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(1)
25X1	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(1)
25X2	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(2)
25X3	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(3)
25X4	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(4)
25X5	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(5)
25X6	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(6)
25X7	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(7)
25X8	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(8)
25X9	25-year exemption code for information declassification, EO 12958, Section 3.3 (b)(9)

### 7.7.2 Examples

XML Markup	Display Values
<pre>classification="S" ownerProducer="USA" disseminationControls="REL" releasableTo="USA AUS" declassDate="2040-10-01" declassException="25X4"</pre>	<p><b>Security Banner</b></p> <p>SECRET//REL TO USA and AUS//<b>25X4</b></p> <p><b>Classification/Declassification Block</b></p> <p>Declassify On: <b>25X4</b>, 20401001</p>
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI" derivedFrom="Multiple Sources" declassDate="2040-10-01" declassException="25X1 25X2 25X3"</pre>	<p><b>Security Banner</b></p> <p>TOP SECRET//COMINT//<b>25X1</b></p> <p><b>Classification/Declassification Block</b></p> <p>Declassify On: <b>25X1</b>, <b>25X2</b>, <b>25X3</b>, 20401001</p>

XML Markup	Display Values
<pre> classification="S" ownerProducer="USA" disseminationControls="REL" releasableTo="USA AUS" declassException="25X1-human" </pre>	<p><b>Security Banner</b></p> <p>SECRET//REL TO USA and AUS//<b>MR</b></p> <p><b>Classification/Declassification Block</b></p> <p>Declassify On: <b>25X1-human</b></p>

### 7.7.3 Notes

1. This attribute is named “declassException” and the attribute’s name token values are referred to as “exceptions” in IC ISM documentation in order to avoid confusion with the “typeOfExemptedSource” and “dateOfExemptedSource” attributes and their values. However, the “declassException” attribute’s name token values do correspond to the 25-year declassification exemptions, as they are identified in EO 12958, the CAPCO Implementation Manual, and elsewhere.
2. Other than when the exemption pertains to the identity of a confidential human source, or a human intelligence source, when a 25-year exemption is applied, the “declassDate” or “declassEvent” attribute shall also be updated and the “Declassify On” line in the classification/declassification block shall include the new date or event for declassification.
3. Multiple declassification exceptions may apply to a single document. The attribute’s value may be a space delimited list of name tokens. All of a document’s declassification exceptions will appear in its classification/declassification block. However, only the first (*i.e.*, most restrictive) exception appears in the Declassification Date field of a document’s security banners.
4. When “25X1-human” is specified in the attribute value, the declassification date parameter of a document’s security banners must be “MR”, indicating that “manual review” is required for declassification of the information.

## 7.8 declassManualReview

This attribute is used primarily at the product level as an indication of the need for manual review for declassification of the information, over and above the usual programmatic determinations. It is manifested only in the declassification date parameter of a document’s security banners and is never manifested in the “Declassify On” line of a document’s classification/declassification block.

### 7.8.1 Authorized Values

Value	Description
true	An indication that “manual review” is required
false	An indication that “manual review” is not required

### 7.8.2 Examples

XML Markup	Display Values
<pre>classification="S" ownerProducer="USA" declassDate="2010-10-10" declassManualReview="true"</pre>	<p><b>Security Banner</b></p> <p>SECRET//MR</p>

### 7.8.3 Notes

- The usual programmatic determinations of the need for manual review for declassification are based on the presence of:
  - non-US or jointly owned and/or produced information
  - FGI
  - RD or FRD
  - information subject to the "25X1-human" declassification exception
  - information subject to an event-triggered declassification
  - information derivatively classified from any source document or classification guide that contains the declassification instruction OADR or X1 thru X8
- The declassManualReview attribute should be used *only* to indicate the need for manual review for declassification *over and above* the usual programmatic determinations. XSLT stylesheets should not depend exclusively on the presence of this attribute to determine when "MR" is required in the Declassification Date field of a document's security banners.
- This attribute is included in IC ISM to support use cases presented by two IC agencies. Based on an interpretation from the CAPCO, it should not be required. The situations listed in note 1 should govern the use of "MR."
- Although "false" is currently an authorized value for this attribute, it serves no purpose when it has this value. To signify "false," simply don't use the attribute.

### 7.9 derivedFrom

This attribute is used primarily at the product level as a citation of the authoritative source of the classification markings used in a resource. It is manifested only in the "Derived From" line of a document's classification/declassification block.

### 7.9.1 Examples

XML Markup	Display Values
<code>derivedFrom="Multiple Sources"</code>	<b>Classification/Declassification Block</b> Derived From: <b>Multiple Sources</b>
<code>derivedFrom="Source Document Citation, dated October 20, 2003"</code>	<b>Classification/Declassification Block</b> Derived From: <b>Source Document Citation, dated October 20, 2003</b>
<code>derivedFrom="Classification Guide Citation, dated October 20, 2003"</code>	<b>Classification/Declassification Block</b> Derived From: <b>Classification Guide Citation, dated October 20, 2003</b>

### 7.9.2 Notes

1. If the attribute value does not specify the title and date of a classification guide or the title and date of a source document, it should be explicitly specified to be "Multiple Sources."
2. When classification is derived from multiple sources, IC ISM assumes that the list of sources is maintained elsewhere—normally with a record copy of the document. Users of generic document models, such as the IC Metadata Standard for Publications, may at their discretion insert a list of the classification sources in the body matter or an appendix.

## 7.10 disseminationControls

This attribute is used at both the product and the element levels to identify the expansion or limitation on the distribution of the information. It is manifested in portion marks and security banners.

### 7.10.1 Authorized Values

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
RS	RSEN	RISK SENSITIVE
FOUO	FOUO	FOR OFFICIAL USE ONLY
OC	ORCON	ORIGINATOR CONTROLLED
IMC	IMCON	CONTROLLED IMAGERY
SAMI	SAMI	SOURCES AND METHODS INFORMATION

## Information Security Marking

## Implementation Guide

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
NF	NOFORN	NOT RELEASABLE TO FOREIGN NATIONALS
PR	PROPIN	CAUTION-PROPRIETARY INFORMATION INVOLVED
REL	REL TO	AUTHORIZED FOR RELEASE TO _____
RD	RD	RESTRICTED DATA
RD-CNWDI	RD-CNWDI	RESTRICTED DATA- CRITICAL NUCLEAR WEAPON DESIGN INFORMATION
RD-SG-1 through RD-SG-15	RD-SIGMA 1 through RD-SIGMA 15	RESTRICTED DATA-SIGMA 1 through RESTRICTED DATA-SIGMA 15
FRD	FRD	FORMERLY RESTRICTED DATA
FRD-CNWDI	FRD-CNWDI	FORMERLY RESTRICTED DATA-CRITICAL NUCLEAR WEAPON DESIGN INFORMATION
FRD-SG-1 through FRD-SG-15	FRD-SIGMA 1 through FRD-SIGMA 15	FORMERLY RESTRICTED DATA-SIGMA 1 through FORMERLY RESTRICTED DATA-SIGMA 15
DCNI	DOD UCNI	DOD CONTROLLED NUCLEAR INFORMATION
ECNI	DOE UCNI	DOE CONTROLLED NUCLEAR INFORMATION
EYES		USA/_____ EYES ONLY
LAC		LACONIC
FRONTO		FRONTO
KEYRUT		KEYRUT
SEABOOT		SEABOOT
SETTEE		SETTEE

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
DSEN		DEA SENSITIVE

### 7.10.2 Examples

XML Markup	Display Values
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI TK" disseminationControls="RD-SG-1 RD-SG-8"</pre>	<b>Security Banner</b>  TOP SECRET//COMINT/TALENT KEYHOLE// <b>RD-SIGMA 1-SIGMA 8</b> //MR
<pre>classification="C" ownerProducer="USA" disseminationControls="OC REL" releasableTo="USA AUS GBR" declassDate="2007-04-01"</pre>	<b>Security Banner</b>  CONFIDENTIAL// <b>ORCON,REL TO USA,</b> AUS and GBR//20070401
<pre>classification="C" ownerProducer="USA" disseminationControls="REL" releasableTo="USA AUS GBR"</pre>	<b>Portion Mark</b>  C// <b>REL TO USA, AUS and GBR</b>
<pre>classification="S" ownerProducer="USA" disseminationControls="EYES" releasableTo="USA AUS CAN GBR"</pre>	<b>Portion Mark</b>  S//USA/AUS/CAN/GRB <b>EYES ONLY</b>

### 7.10.3 Notes

- Multiple dissemination controls may apply to a single portion and/or to the document. This attribute's value may be a single XML name token or a space-delimited list of name tokens, which must be ordered as specified in the CAPCO Register.
- The authorized portion mark differs from the stored value for RD-SG-1 through RD-SG-15 and FRD-SG-1 through FRD-SG-15, because the authorized portion mark does not qualify as an XML name token.
- Multiple values for RD-SG-1 through RD-SG-15 and FRD-SG-1 through FRD-SG-15 are stored (in the example below) as follows:  

```
disseminationControls="RD-SG-1 RD-SG-2 RD-SG-3"
```
- However, the Dissemination Controls field of a portion mark using the example above is rendered and displayed as follows:  

```
//RD-SG 1-SG 2-SG 3
```
- When the REL or EYES name token is selected, the "releasableTo" attribute is required also. See "releasableTo" for information regarding usage of its name token values.



6. When “RD”, “RD-CNWDI”, “RD-SIGMA-1” through “RD-SIGMA-15”, “FRD”, “FDR-CNWDI”, or “FRD-SIGMA-1 through “FRD-SIGMA-15” is specified in the attribute value, the Declassification Date field of a document’s security banners must be “MR”, indicating that “manual review” is required for declassification of the information.

## 7.11 FGIsorceOpen

This attribute is used at both the product and the element levels to identify the known and disclosable originating source (country or registered international organization) or sources (at the product level) of controlled information of non-US origin in a US controlled document, or that the source of information of non-US origin in a US controlled document is unknown. It is manifested in portion marks and security banners.

### 7.11.1 Authorized Values

Stored Value	Description
AFG ALB ... ZMB ZWE	ISO 3166-1 country trigraphs
NATO	North Atlantic Treaty Organization
BWCS	Biological Weapons Convention States
CWCS	Chemical Weapons Convention States
ECTF	European Counter-Terrorism Forces
GCTF	Global Counter-Terrorism Forces
ISAF	International Security Assistance Forces for Afghanistan
KFOR	Stabilization Forces in Kosovo
SFOR	Stabilization Forces in Bosnia
UNKNOWN	Source of Information is unknown

### 7.11.2 Examples

XML Markup	Display Values
<pre>classification="S" ownerProducer="USA" FGIsorceOpen="AUS"</pre>	<b>Security Banner</b> SECRET// <b>FGI</b> AUS//MR
<pre>classification="S" ownerProducer="USA" FGIsorceOpen="AUS NZL NATO"</pre>	<b>Security Banner</b> SECRET// <b>FGI</b> AUS NZL NATO//MR
<pre>classification="C" ownerProducer="USA" FGIsorceOpen="UNKNOWN"</pre>	<b>Security Banner</b> CONFIDENTIAL// <b>FGI</b> //MR
<pre>classification="S" ownerProducer="NZL USA" FGIsorceOpen="DEU"</pre>	<b>Security Banner</b> //JOINT SECRET NZL USA// <b>FGI</b> <b>DEU</b> //MR

XML Markup	Display Values
<pre>classification="S" ownerProducer="DEU" SCIcontrols="SI TK" <b>FGIsourceOpen="DEU"</b> disseminationControls="REL" releasableTo="USA AUS GBR"</pre>	<b>Portion Mark</b> // <b>DEU</b> S//SI/TK//REL TO USA, AUS and GBR
<pre>classification="C" ownerProducer="USA" <b>FGIsourceOpen="UNKNOWN"</b></pre>	<b>Portion Mark</b> // <b>FGI</b> C

### 7.11.3 Notes

1. When the attribute has the value "UNKNOWN", the resulting display is as follows:  
//FGI
2. When this attribute is used at the portion level, its value will always contain only one name token.
3. When this attribute is used at the portion level and its value is not "UNKNOWN," its value will always be identical to the "ownerProducer" attribute value for the portion.
4. When this attribute is used, the declassification date parameter of the document's security banners must be "MR," indicating that "manual review" is required for declassification of the information.

### 7.12 FGIsourceProtected

This attribute is used at both the product and the element levels to identify the known but non-disclosable originating source (country or registered international organization) or sources (at the product level) of controlled information of non-US origin in a US controlled document. The originating source is known and maintained but is not to be displayed on dissemination. It is manifested in portion marks and security banners.

#### 7.12.1 Authorized Values

Stored Value	Description
AFG ALB ... ZMB ZWE	ISO 3166-1 country trigraphs
NATO	North Atlantic Treaty Organization
BWCS	Biological Weapons Convention States
CWCS	Chemical Weapons Convention States
ECTF	European Counter-Terrorism Forces
GCTF	Global Counter-Terrorism Forces
ISAF	International Security Assistance Forces for Afghanistan
KFOR	Stabilization Forces in Kosovo
SFOR	Stabilization Forces in Bosnia

### 7.12.2 Examples

XML Markup	Display Values
<pre>classification="C" ownerProducer="USA" <b>FGISourceProtected="AUS"</b> disseminationControls="OC"</pre>	<b>Security Banner</b> CONFIDENTIAL// <b>FGI</b> //ORCON//MR
<pre>classification="S" ownerProducer="NZL USA" <b>FGISourceProtected="CAN DEU"</b></pre>	<b>Security Banner</b> //JOINT SECRET NZL USA// <b>FGI</b> //MR
<pre>classification="R" ownerProducer="GBR" <b>FGISourceProtected="GBR"</b> disseminationControls="NF"</pre>	<b>Portion Mark</b> // <b>FGI</b> R//NF
<pre>classification="S" ownerProducer="NATO" <b>FGISourceProtected="NATO"</b> disseminationControls="REL" releasableTo="USA AUS JPN"</pre>	<b>Portion Mark</b> // <b>FGI</b> S//REL TO USA, AUS and JPN

### 7.12.3 Notes

1. When this attribute is used at the portion level, its value will always contain only one name token.
2. When this attribute is used, the declassification date parameter of the document's security banners must be "MR," indicating that "manual review" is required for declassification of the information.

## 7.13 nonICmarkings

This attribute is used at both the product and the element levels to identify classified information originating from non-intel components of the US Department of Defense or the US Department of Energy. It is manifested in portion marks and security banners.

### 7.13.1 Authorized Values

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
SC	SPECAT	SPECIAL CATEGORY
SIOP	SIOP-ESI	SINGLE INTEGRATED OPERATIONS PLAN- EXTREMELY SENSITIVE INFORMATION
SINFO		SENSITIVE INFORMATION
DS	LIMDIS	LIMITED DISTRIBUTION

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
XD	EXDIS	EXCLUSIVE DISTRIBUTION
ND	NODIS	NO DISTRIBUTION
SBU	SBU	SENSITIVE BUT UNCLASSIFIED
SBU-NF	SBU-NOFORN	SENSITIVE BUT UNCLASSIFIED NOFORN

### 7.13.2 Examples

XML Markup	Display Values
<pre>classification="S" ownerProducer="USA" nonICmarkings="SC" declassDate="2008-03-15"</pre>	<b>Security Banner</b> SECRET// <b>SPECAT</b> //20080315
<pre>classification="U" ownerProducer="USA" nonICmarkings="SBU-NF"</pre>	<b>Security Banner</b> UNCLASSIFIED// <b>SBU-NOFORN</b>
<pre>classification="S" ownerProducer="USA" nonICmarkings="XD"</pre>	<b>Portion Mark</b> S// <b>XD</b>
<pre>classification="U" ownerProducer="USA" nonICmarkings="SINFO"</pre>	<b>Portion Mark</b> U// <b>SINFO</b>

### 7.14 ownerProducer

This attribute is used at both the product and the element levels to identify the national government or international organization owner(s) and/or producer(s) of the information. The attribute value may be manifested in portion marks or security banners (see note [4](#), below).

#### 7.14.1 Authorized Values

Stored Value	Description
AFG ALB ... ZMB ZWE	ISO 3166-1 country trigraphs
NATO	North Atlantic Treaty Organization
BWCS	Biological Weapons Convention States
CWCS	Chemical Weapons Convention States
ECTF	European Counter-Terrorism Forces
GCTF	Global Counter-Terrorism Forces

Stored Value	Description
ISAF	International Security Assistance Forces for Afghanistan
KFOR	Stabilization Forces in Kosovo
SFOR	Stabilization Forces in Bosnia

### 7.14.2 Examples

XML Markup	Display Values
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI" disseminationControls="REL" releasableTo="USA GBR" declassDate="2015-09-30"</pre>	<b>Security Banner</b>  TOP SECRET//COMINT//REL TO USA and GBR//20150930
<pre>classification="R" ownerProducer="AUS" declassDate="2010-01-01"</pre>	<b>Security Banner</b>  // <b>AUS</b> RESTRICTED//MR
<pre>classification="S" ownerProducer="AUS USA" FGIsourcesOpen="DEU" declassDate="2012-05-01"</pre>	<b>Security Banner</b>  //JOINT SECRET <b>AUS USA</b> //FGI DEU//MR
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI" disseminationControls="OC REL" releasableTo="USA GBR"</pre>	<b>Portion Mark</b>  TS//SI//OC,REL TO USA and GBR
<pre>classification="CTS" ownerProducer="NATO" FGIsourcesOpen="NATO"</pre>	<b>Portion Mark</b>  //CTS
<pre>classification="S" ownerProducer="USA NATO" disseminationControls="NF"</pre>	<b>Portion Mark</b>  //JOINT S <b>USA NATO</b> //NF

### 7.14.3 Notes

1. Attribute **ownerProducer** must be used in conjunction with attribute **classification**. It has no purpose otherwise. This attribute is the primary indication as to whether the corresponding information is "US", "non-US" or "joint." The format of both portion marks and security banners is slightly different for each of these three situations.
2. Although this attribute is technically optional when the %SecurityAttributesOption entity is applied to an element by a DTD or schema, this attribute along with **classification** must always be used and an attribute value must be explicitly indicated when security attributes are specified for an element.

3. When joint ownership applies, list country trigraphs in strict alphabetical order. List international organization tetragraphs in strict alphabetical order. If both trigraphs and tetragraphs apply, list trigraphs first.
4. The attribute value is only directly manifested in portion marks and security banners in two situations. The first is when the attribute value is a space-delimited list of name tokens, indicating that the information is jointly owned and/or produced (*i.e.*, “joint” information). The second is when the value of this attribute is a single name token that is not equal to “USA” (*i.e.*, “non-US” information), *except when the value is equal to NATO*. If the value of this attribute is a single name token and is equal to “USA” or “NATO,” it is not manifested in portion marks or security banners.
5. When this attribute value contains any name token other than “USA,” indicating that it pertains to non-US or jointly owned and/or produced information, the declassification date parameter of a document’s security banners must be “MR,” indicating that “manual review” is required for declassification of the information.

### 7.15 releasableTo

This attribute is used at both the product and the element levels to identify 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. It is manifested in portion marks and security banners.

#### 7.15.1 Authorized Values

Stored Value	Description
AFG ALB ... ZMB ZWE	ISO 3166-1 country trigraphs
NATO	North Atlantic Treaty Organization
BWCS	Biological Weapons Convention States
CWCS	Chemical Weapons Convention States
ECTF	European Counter-Terrorism Forces
GCTF	Global Counter-Terrorism Forces
ISAF	International Security Assistance Forces for Afghanistan
KFOR	Stabilization Forces in Kosovo
SFOR	Stabilization Forces in Bosnia

#### 7.15.2 Examples

XML Markup	Display Values
<pre>classification="S" ownerProducer="USA" SCIcontrols="SI" disseminationControls="OC REL" <b>releasableTo="USA AUS NZL"</b> declassDate="2015-03-01"</pre>	<p><b>Security Banner</b></p> <p>SECRET//COMINT//ORCON,REL TO  <b>USA, AUS and NZL</b>//20150301</p>

XML Markup	Display Values
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI-G" FGIsourceOpen="GBR" disseminationControls="EYES" releasableTo="USA AUS"</pre>	<b>Security Banner</b> TOP SECRET//COMINT-GAMMA//FGI GBR// <b>USA/AUS</b> EYES ONLY//MR
<pre>classification="TS" ownerProducer="USA" SCIcontrols="SI-G TK" disseminationControls="EYES" releasableTo="USA AUS"</pre>	<b>Portion Mark</b> TS//SI-G/TK// <b>USA/AUS</b> EYES ONLY
<pre>classification="C" ownerProducer="USA" FGIsourceOpen="UNKNOWN" disseminationControls="PR REL" releasableTo="USA GBR"</pre>	<b>Portion Mark</b> //FGI C//PR,REL TO <b>USA and GBR</b>

### 7.15.3 Notes

1. When the “releasableTo” attribute is used, the “USA” name token is required. It must be the first name token in the space-delimited list of values. Additional country name tokens are stored in alphabetical order followed by additional registered international organization name tokens in alphabetical order. The following example illustrates this requirement.

```
releasableTo="USA AUS GBR NZL NATO"
```

2. If the “REL” name token is used in attribute **disseminationControls**, the portion mark or security banner using this example is rendered and displayed as follows.

```
//REL TO USA, AUS, GBR, NZL and NATO
```

3. If the “EYES” name token is used in attribute **disseminationControls**, the portion mark or security banner using this example is rendered and displayed as follows.

```
//USA/AUS/GBR/NZL/NATO EYES ONLY
```

4. If a portion level **releasableTo** attribute value is identical to the product level **releasableTo** attribute value, and the portion level and product level **disseminationControls** attribute values both contain either “REL” or “EYES”, then the **releasableTo** value need not be displayed in the portion mark. For example, using the following product level and portion level elements, the portion mark for the “Para” element could be simplified to “(C//REL).”

```
<Security classification="S" ownerProducer="USA"
disseminationControls="REL" releasableTo="USA GBR"
.../>
```

```
<Para classification="C" ownerProducer="USA"
disseminationControls="REL" releasableTo="USA GBR">
```

### 7.16 SARIdentifier

This attribute is used at both the product and the element levels to identify Special Access Required program identifier(s). It is manifested in portion marks and security banners.

### 7.16.1 Authorized Values

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
program trigraph or digraph		SPECIAL ACCESS REQUIRED-[program identifier]

### 7.16.2 Examples

XML Markup	Display Values
<pre>classification="TS" ownerProducer="USA" SARIdentifier="ABC" declassDate="2010-08-30"</pre>	<b>Security Banner</b> TOP SECRET// <b>SPECIAL ACCESS REQUIRED-ALPHA BRAVO CHARLIE</b> //20100830
<pre>classification="TS" ownerProducer="USA" SARIdentifier="ABC DE" declassDate="2010-08-30"</pre>	<b>Security Banner</b> TOP SECRET// <b>SPECIAL ACCESS REQUIRED-ALPHA BRAVO CHARLIE/DELTA ECHO</b> //20100830
<pre>classification="TS" ownerProducer="USA" SARIdentifier="ABC"</pre>	<b>Portion Mark</b> TS// <b>SAR-ABC</b>
<pre>classification="TS" ownerProducer="USA" SARIdentifier="ABC DE"</pre>	<b>Portion Mark</b> TS// <b>SAR-ABC/DE</b>

### 7.16.3 Notes

1. The SAR program identifiers and program trigraphs and digraphs used in the examples above are for illustration purposes only. The name tokens in the attribute values will be actual program trigraphs and digraphs. An XSLT stylesheet will need to associate the name tokens in the attribute values with the actual SAR program identifiers for display in the document's security banners.

## 7.17 SCIcontrls

This attribute is used at both the product and the element levels to identify classified information concerning or derived from intelligence sources, methods, or analytical processes which is required to be handled within formal control systems established by the DCI (in accordance with DCID 1/19, Section 1.1). It is manifested in portion marks and security banners.

### 7.17.1 Authorized Values

Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
--	----------------------------	---------------



Stored Value (Authorized Portion Marking)	Authorized Abbreviation	Marking Title
SI	SI	COMINT
SI-G	SI-G	COMINT-GAMMA
SI-ECI-XXX	SI-ECI XXX	COMINT-ECI XXX
TK	TK	TALENT KEYHOLE

### 7.17.2 Examples

XML Markup	Display Values
<pre>classification="TS" ownerProducer="USA" <b>SCIcontrols="SI-ECI-ABC SI-ECI-XYZ"</b> disseminationControls="NF" declassDate="2010-08-30"</pre>	<b>Security Banner</b>  TOP SECRET// <b>COMINT-ECI ABC-ECI XYZ</b> //NOFORN//20100830
<pre>classification="TS" ownerProducer="USA" <b>SCIcontrols="SI-G"</b> disseminationControls="REL" releasableTo="USA AUS GBR" declassDate="2010-05-20"</pre>	<b>Security Banner</b>  TOP SECRET// <b>COMINT-GAMMA</b> //REL TO USA, AUS and GBR//20100520
<pre>classification="TS" ownerProducer="USA" <b>SCIcontrols="SI-G"</b> disseminationControls="OC PR REL" releasableTo="USA AUS GBR"</pre>	<b>Portion Mark</b>  TS// <b>SI-G</b> //OC,PR,REL TO USA, AUS and GBR
<pre>classification="S" ownerProducer="USA" <b>SCIcontrols="SI-ECI-ABC"</b></pre>	<b>Portion Mark</b>  S// <b>SI-ECI ABC</b>

### 7.17.3 Notes

1. The name tokens shown above in the controlled vocabulary for SCIcontrols do not include classified values. The classified tokens may be appended to the controlled vocabulary by organizations requiring their use. At a later date a classified registry most likely will maintain these values, but that had not yet been determined at the time of this publication.
2. In the SI-ECI-XXX name token, "XXX" is a placeholder for a three-letter alphabetic ECI designator. The stored values will include the actual ECI designator. For purposes of illustration, the following examples provide guidance in their usage:

SCIcontrols="SI-ECI-ABC"

3. However, the portion mark using the example above is rendered and displayed as follows:

//SI-ECI ABC

4. Multiple values for SI-ECI are stored as follows:

SCIcontrols="SI-ECI-ABC SI-ECI-DEF SI-ECI-GHI"

5. However, the portion marking using this example is rendered and displayed as follows:

//SI-ECI ABC-ECI DEF-ECI GHI

## 7.18 typeOfExemptedSource

This attribute is used primarily at the product level to specify a marking of a source document that causes the current document to be exempted from automatic declassification. It is manifested only in the "Declassify On" line of a document's classification/declassification block.

### 7.18.1 Authorized Values

Value	Description
OADR	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "Originating Agency's Determination Required" or "OADR"
X1	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X1"
X2	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X2"
X3	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X3"
X4	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X4"
X5	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X5"
X6	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X6"
X7	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X7"
X8	Used when a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction "X8"

### 7.18.2 Examples

XML Markup	Display Values
<code>typeOfExemptedSource="OADR"</code> <code>dateOfExemptedSource="1990-10-20"</code>	<b>Classification/Declassification Block</b>  Declassify On: Source Marked "OADR", Date of Source: 19901020
<code>typeOfExemptedSource="X1 X2"</code> <code>dateOfExemptedSource="2000-10-20"</code>	<b>Classification/Declassification Block</b>  Declassify On: Source Marked "X1 X2", Date of Source: 20001020

### 7.18.3 Notes

1. When this attribute is used, attribute **dateOfExemptedSource** must also be used.
2. When this attribute is used, the declassification date parameter of the current document's security banners must be "MR," indicating that "manual review" is required for declassification of the information in the current document.

## Appendix A - Points of Contact

Name	Position	Contact Information
<b><i>Send comments and suggestions about this guide to:</i></b>		
Karen Stevens	Secretariat, IC MWG	+1 (703) 874-8264 stevensk@saic.com (unclassified) stevnsk@cia.ic.gov (IC E-MAIL)
<b><i>Other points of contact are:</i></b>		
Tim West	Chair, IC MWG	+1 (202) 231-2256 timothy.west@dia.mil
Mary Ann Melosh	Support, IC MWG	+1 (703) 676-5826 mary.a.melosh@saic.com
Clive Carpi	Support, IC MWG	+1 (703) 676-4926 clive.c.carpi@saic.com
Jim Greenwood	Support, IC MWG	+1 (703) 676-5038 james.d.greenwood@saic.com

## Appendix B - References

1. Intelligence Community, Community Management Staff, Controlled Access Programs Coordination Office, *Authorized Classification and Control Markings Register*. (See CAPCO home page on Intelink.)
2. Intelligence Community, Community Management Staff, Controlled Access Programs Coordination Office, *Authorized Classification and Control Markings Implementation Manual*. (See CAPCO home page on Intelink.)
3. Intelligence Community, Metadata Working Group, *IC ISM Data Element Dictionary*, Version 2.0, 30 April 2004. Available at "<http://www.imd.ic.gov/ICML/Index.html>" on Intelink; at "<http://www.xml.saic.com/icml/>" on the Internet; and as resource "IC\_ISM\_DED" in the DoD XML Registry.
4. U.S. National Archives and Records Administration, Information Security Oversight Office, *Classified National Security Information Directive No. 1*, October 30, 2003.
5. World Wide Web Consortium, W3C Recommendation, *Extensible Markup Language (XML) 1.1*, 4 April 2004.
6. World Wide Web Consortium, W3C Recommendation, *Namespaces in XML 1.1*, 4 April 2004.
7. World Wide Web Consortium, W3C Recommendation, *Extensible Stylesheet Language (XSL)*, Version 1.0, W3C Recommendation, 15 October 2001.
8. World Wide Web Consortium, W3C Recommendation, *XSL Transformations (XSLT)*, Version 1.0, 16 November 1999.

## Appendix C - Change History

Version	Date	Purpose
1.0	05 July 2002	Initial release
2.0	30 April 2004	<p>Updated to support changes to the CAPCO Register and Implementation Manual.</p> <p>Added "ownerProducer" as a required attribute for entity "SecurityAttributes" and as an optional attribute for entity "SecurityAttributesOption." Purpose is to provide a single method for specification of US, non-US, and joint classifications.</p> <p>Changed the enumerated list for the "classification" attribute to include non-US values.</p> <p>Added optional attribute "SARIdentifier" as a separate container for DoD/DoE special-access-required nicknames, codewords, or trigraph/digraph to support elevation of SAR to the same level as SCI controls.</p> <p>Added optional attributes "classifiedBy" and "classificationReason" to support generation of EO 12958 classification/declassification blocks.</p> <p>Changed the declared value of "derivedFrom" to CDATA to allow the titles and dates of source documents or classification guides to be specified.</p> <p>Replaced the single attribute "declassification" with distinct attributes for date-determined and event-determined declassification and for the 25X declassification exceptions.</p> <p>Added attributes "typeOfExemptedSource" and "dateOfExemptedSource" for use in specifying that one or more sources was marked OADR, X1 through X8.</p> <p>Added attribute "declassManualReview" for use in forcing "MR" to appear in header and footer banners (regardless of whether any caveats in the portions would necessitate manual review).</p> <p>Removed entity "DowngradeAttributes," reflecting the configuration management panel's decision to allow portion mark oriented and banner oriented attributes to be used together on any object.</p>

## Appendix D - Sample Domain Value Document

Each of the controlled vocabularies used with the IC ISM attributes is represented by a domain value document in the XML Registry. This appendix contains the domain value document for the non-IC markings controlled vocabulary. This is the format in which the vocabulary is available from the DoD XML Registry. The information resource name for this file in the XML Registry is "INTnonICmarkings2004-04-30".

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE DomainValueSet SYSTEM
"http://diides.ncr.disa.mil/xmlreg/DTD/registry_domain_values.
dtd">

<DomainValueSet>

<ReferenceSetId/>
<EffectiveDate>2004-04-30</EffectiveDate>
<SecurityClassification>UNCLASSIFIED</SecurityClassification>
<Definition>Information security classification markings for
classified information originating from non-intelligence
components of the US Department of Defense or the US
Department of Energy</Definition>

<Namespace>INT</Namespace>
<InformationResourceName>
INTnonICmarkings2004-04-30
</InformationResourceName>
<InformationResourceVersion>
2004-04-30
</InformationResourceVersion>

<DomainValues>

<DomainValue security_classification="Unclassified">
<KeyValue>SC</KeyValue>
<Description>SPECIAL CATEGORY</Description>
<NonKeyValue>SPECAT</NonKeyValue>
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>SIOP</KeyValue>
<Description>SINGLE INTEGRATED OPERATIONS PLAN-EXTREMELY
SENSITIVE INFORMATION</Description>
<NonKeyValue>SIOP-ESI</NonKeyValue>
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>SINFO</KeyValue>
<Description>SENSITIVE INFORMATION</Description>
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>DS</KeyValue>
<Description>LIMITED DISTRIBUTION</Description>
<NonKeyValue>LIMDIS</NonKeyValue>
```

```
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>XD</KeyValue>
<Description>EXCLUSIVE DISTRIBUTION</Description>
<NonKeyValue>EXDIS</NonKeyValue>
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>ND</KeyValue>
<Description>NO DISTRIBUTION</Description>
<NonKeyValue>NODIS</NonKeyValue>
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>SBU</KeyValue>
<Description>SENSITIVE BUT UNCLASSIFIED</Description>
</DomainValue>

<DomainValue security_classification="Unclassified">
<KeyValue>SBU-NF</KeyValue>
<Description>SENSITIVE BUT UNCLASSIFIED NOFORN</Description>
<NonKeyValue>SBU NOFORN</NonKeyValue>
</DomainValue>

</DomainValues>
</DomainValueSet>
```