

	<b>MISB Standard 0102.8</b>
<b>Standard</b>  <b>Security Metadata Universal and Local Sets for Digital Motion Imagery</b>	<b>20 May 2010</b>

## 1. Scope

This Standard describes the use of security metadata in MPEG-2 digital motion imagery applications. For applications involving national security it is mandatory that each part of a motion imagery file be marked correctly and consistently with security classification and other security administration information. The approved practices in this Standard *shall* be applied to all motion imagery implementations using MPEG-2 Transport Streams or files and *shall* be used to link security metadata to essence (video, audio, or data) and/or other metadata.

This Standard defines only the format of embedding security metadata in MPEG-2 transport streams or files. (The Standard only addresses the MPEG-2 transport mechanism and is independent of the compression used for the video essence.) The methods used to gather security information, create streams or files and insert security metadata into these transports are the responsibility of application system developers in concert with appropriate Security officials. Similarly, the proper display of security information on screens, computer displays, printed output, *etc.* is the responsibility of system application developers. Originators and application users are responsible for the proper handling and ultimately for the use and disposition of classified information. This Standard is not a Security manual or instruction on when or how to use security markings or caveats. Use of this Standard does not ensure that motion imagery systems can or will be accredited by Security officials.

This Standard was, previous to version 0102.5, a Recommended Practice (RP). Earlier versions of this Standard are still referred to as RP 0102.x in this document.

## 2. References

### 2.1. Normative References

*Note: The documents specified in § 2.1.1, 2.1.2, and 2.1.3 are subject to being superseded by ODNI ICD's.*

The following documents are necessary references for understanding and following the instructions in this Standard:

- 2.1.1. Director of Central Intelligence, Community Management Staff, Controlled Access Program Coordination Office (CAPCO), *Intelligence Community Classification and Control Markings Implementation Manual*, 10 Sep 1999, amended 12 Oct 2000.
- 2.1.2. *CAPCO Authorized Classification and Control Markings Register*.

## UNCLASSIFIED

- 2.1.3. Director of Central Intelligence Directive (DCID) 6/3, *Security Requirements for Interconnected Information Systems*, 24 May 2000.
- 2.1.4. SMPTE 335M-2001, *Metadata Dictionary Structure*.
- 2.1.5. SMPTE 336M-2007, *Data Encoding Protocol Using Key-Length-Value*.
- 2.1.6. SMPTE 330M-2003, *Unique Material Identifier (UMID)*.
- 2.1.7. SMPTE RP210-2001, *Metadata Dictionary*. Updated at <http://www.smptra.org>
- 2.1.8. ISO/IEC 13818-1:2000 *Information Technology – Generic coding of moving pictures and associated audio information: Systems* (commonly called MPEG-2 Systems).
- 2.1.9. ISO 3166-1, *Codes for the representation of names of countries and their subdivisions: Country Codes*, 1 October 1997 and updated by the ISO 3166 Management Authority (MA) at: <http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/index.html> and <http://www.iso.org/iso/en/prods-services/iso3166ma/03updates-on-iso-3166/index.html>.
- 2.1.10. Federal Information Processing Standards (FIPS) Publication 10-4, *Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions*, National Institute of Standards and Technology, April 1995 (through Change Notice 10, 23 March 2006) Change Notices are issued by NGA at [http://earth-info.nga.mil/gns/html/fips\\_files.html](http://earth-info.nga.mil/gns/html/fips_files.html).  
**NOTE: Per Federal Register 73/170 (p. 51276), dated September 2, 2008, FIPS 10-4 is deprecated and may no longer be used to assign country codes to data created after 31 December 2012. Support for FIPS 10-4 will be retained in this Standard for legacy data.**
- 2.1.11. MISB Standard 0107, “*Bit and Byte Order for Metadata in Motion Imagery Files and Streams*,” 11 October 2001
- 2.1.12. MISB Standard (EG) 0601.2, “*UAV Datalink Local Data Set*,” 18 September 2008.
- 2.1.13. STANAG 1059 Ed 8.

## 2.2. Informative References

The following documents are useful informative references for understanding and following the instructions in this Standard:

- 2.2.1. MISB RP 0101, *Use of MPEG-2 Systems Streams in Digital Motion Imagery Systems*.
- 2.2.2. *Director of Central Intelligence Directive (DCID)1/7*, 30 Jun 1998
- 2.2.3. DOD Directive (ASD (NII)) “*Data Sharing in a Net-Centric Department of Defense*” Number 8320.2, 2 December 2004.

## UNCLASSIFIED

- 2.2.4. *DOD Net-centric Data Strategy*, 9 May 2003,
- 2.2.5. DOD Discovery Metadata Specification (DDMS), Version 1.0, 29 September 2003.
- 2.2.6. *Executive Order (EO) 12958*, 17 April 1995 Classified National Security Information.
- 2.2.7. *Executive Order 13292*, 25 March 2003, Further Amendment to EO 12958, as amended, *Classified National Security Information*
- 2.2.8. DOD Directive 5200.1 (ASD (C3I)), 13 December 2001, certified current 24 November 2003.
- 2.2.9. DOD Directive 5100.55: *U. S. Security Authority for NATO Affairs reissued. 27 February 2006.*
- 2.2.10. DOD Instruction, Number 5210.52, *Security Classification of Airborne Sensor Imagery and Imaging Systems*, 18 May 1989
- 2.2.11. DOD 5220.22-M (USD(I)) *National Industrial Security Program Operating Manual (NISPOM)*, 28 February 2006
- 2.2.12. Imagery Policy Series, Particular Section 6, "National Airborne Reconnaissance Imagery"
- 2.2.13. STANAG 3678 *Guide to Security Classification of Air Reconnaissance Imagery*, 2005

### 3. Introduction

This Standard defines the content and application of both a Security Metadata Universal Set and Local Set in digital motion imagery. The first section explains the individual elements in KLV Sets that are normative in the SMPTE Metadata Dictionary (SMPTE RP 210) and the MISB Metadata Registry. The construction of both a Security Metadata Universal Set and Local Set from these elements follows SMPTE STD 336M using the KLV metadata encoding protocol. Finally, this Standard defines how the Security Metadata Sets shall be used for tagging essence and other metadata sets in MPEG-2 streams and files.

### 4. Security Metadata Universal and Local Sets for Digital Motion Imagery

The sections of this Standard are applicable only to MPEG-2 transport streams and files.

4.0.1 The practices *shall* be followed to ensure that all parts of an MPEG-2 transport stream or file are tagged correctly with security information for use by applications.

4.0.2 All metadata *shall* be represented using big-endian (most significant byte – MSB - first) encoding.

4.0.3 Bytes *shall* be big-endian bit encoding (most significant bit – msb - first).

## 4.1. Security Metadata Elements

The following Security metadata elements are intended to comprise information needed to comply with CAPCO and other normatively referenced security directives. These normative documents govern when certain fields are mandatory and when fields are optional. Security requirements may dictate that some or all entries are mandatory. In all applications the presence or absence of certain metadata will depend on the context of the application and its unique security requirements. Whenever there is conflict between this Standard and directions of Security officials on the required presence or absence of entries the direction of Security officials takes precedence.

### 4.1.1. Security Classification

This metadata element contains a value representing the entire security classification of the file in accordance with U.S. and NATO classification guidance. Values allowed are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, and UNCLASSIFIED (all caps) followed by a double forward slash “//”. This is a mandatory entry whenever the Security Metadata Sets are used.

### 4.1.2. Classifying Country or Releasing Instructions Country Coding Method

This metadata element identifies the country coding method for the Classifying Country (Par. 4.1.3) and Releasing Instructions (Par. 4.1.6) metadata. The Country Coding Method shall use FIPS 10-4 two-letter or four-letter alphabetic country code; ISO-3166 two-letter, three-letter, or 3-digit numeric; or STANAG 1059 two-letter or three-letter codes.

Example of Country Coding Method:           **ISO-3166 Two Letter**

### 4.1.3. Classifying Country

This metadata element contains a value for the classifying country code preceded by a double slash “//.”

Example of classifying country:

//DEU (Example of ISO-3166 code)  
//UK (Example of default FIPS 10-4 code)

### 4.1.4. Sensitive Compartmented Information (SCI) / Special Handling Instructions (SHI)

If the classification of any material in the transport stream or file is Top Secret, Secret, or Confidential and requires special handling, then SCI/SHI digraphs, trigraphs, or compartment names must be added identifying a single or a combination of special handling instructions. A single entry shall be ended with a double forward slash “//”. Multiple digraphs, trigraphs, or compartment names shall be separated by a single forward slash “/” and the last entry shall be ended with a double forward slash “//”. Multiple SCI/SHI digraphs, trigraphs, or

## UNCLASSIFIED

compartment names shall be concatenated in one metadata element free-text entry and shall not be encoded as individual metadata elements in the Sets.

### 4.1.5. Caveats

This metadata element set contains a value representing all pertinent caveats (or codewords) from each category of the appropriate security entity register. Entries in this field may be abbreviated or spelled out as free-text entries. The Caveats field shall also be used to indicate FOR OFFICIAL USE ONLY or may be abbreviated as FOUO.

### 4.1.6. Releasing Instructions

This metadata element contains a list of country codes to indicate the countries to which information in a digital motion imagery file is releasable. Multiple country codes shall be separated by a blank (space – NOT underscore). Multiple country codes shall be concatenated in one Releasing Instructions metadata element entry and shall not be encoded as individual metadata elements in the Sets. The use of blank spaces to separate country codes, instead of semi-colons or other characters, is to comply with security guidelines and to allow parsing of fields by automated security screening systems. The country code of the originating country shall appear first, then the country codes of other countries to which the data are releasable shall appear in alphabetical order, and, finally, the codes of any non-state organizations (such as NATO) to which the data are releasable shall appear in alphabetical order.

### 4.1.7. Classified By

This metadata element identifies the name and type of authority used to classify the file. The metadata element is free text and can contain either the original classification authority name and position or personal identifier, or the title of the document or security classification guide used to classify the material.

### 4.1.8. Derived From

This metadata element contains information about the original source file or document from which the classification was derived. The metadata element is free-text.

### 4.1.9. Classification or Marking System

This metadata element identifies the classification or marking system used in this Security Metadata Set as determined by the appropriate security entity for the country originating the data. The entry shall be a free text field.

Example of Classification or Marking System:        **XYZ Marking System**

## UNCLASSIFIED

### 4.1.10 Classification Reason

This metadata element contains the reason for classification or a citation from a document (see below). The metadata element is free-text.

### 4.1.11 Declassification Date

This metadata element provides either a date when the classified material may be automatically declassified or if it is subject to Manual Review (MR) and is exempt from automatic declassification. The declassification date format shall be YYYYMMDD or the letters “MR” shall be used.

### 4.1.12 Object Country Coding Method

This metadata element identifies the coding method for the Object Country Code (Par. 4.1.12) metadata. The Object Country Coding Method shall use FIPS 10-4 two-letter or four-letter alphabetic country code or a combination of the two; ISO-3166 two-letter, three-letter, or 3-digit numeric or a combination of the three; or STANAG 1059 two-letter, three-letter, or 3-digit numeric codes or a combination of the three. Use of this element in version 6 and later is mandatory. In version 5 and earlier, it was optional; its absence shall indicate that the default FIPS 10-4 two-letter code was used in the Object Country Code element.

### 4.1.13 Object Country Code

This metadata element contains a value identifying the country (or countries) that is the object of the video or metadata in the transport stream or file. Multiple country codes shall be separated by a semi-colon “;” (no spaces). Multiple country codes shall be concatenated in one Object Country Code metadata element entry and shall not be encoded as individual metadata elements in the Sets. It is required to populate this field with the Object Country Code of the geographic region lying under the center of the frame. The Object Country Codes of other represented geographic regions may be included in addition to the country code of the geographic region under the center of frame. Note: The use of the semi-colon to separate country codes, instead of blanks or other characters, is to allow processing by current, automated imagery processing and management tools.

### 4.1.14 Comments

This metadata element allows for security related comments and format changes that may be necessary in the future. This field may be used in addition to those required by appropriate security entity and is optional.

## **4.2. Security Metadata Universal Set**

The individual metadata elements that comprise information needed to identify the security classification of MPEG-2 streams and files and other metadata are defined as SMPTE KLV metadata elements in SMPTE RP210-2000 (and updated versions) and the MISB Metadata Registry.

4.2.1 The Security Metadata Universal Set 16-byte Universal Label Key **shall** be:

**06 0E 2B 34 02 01 01 01 02 08 02 00 00 00 00**

4.2.2 Required security and linking information **shall** be contained entirely within a Security Metadata Universal Set that conforms to SMPTE 336M KLV Universal Set encoding rules.

### **4.3. Security Metadata Local Set**

The individual metadata elements that comprise information needed to identify the security classification of MPEG-2 streams and files and other metadata are defined as SMPTE KLV metadata elements in SMPTE RP210-2000 (and updated versions) and the MISB Metadata Registry.

4.3.1 The Security Metadata Local Set 16-byte Universal Label Key **shall** be:

**06 0E 2B 34 02 03 01 01 0E 01 03 03 02 00 00**

4.3.2 Required security and linking information **shall** be contained entirely within a Security Metadata Local Set that conforms to SMPTE 336M KLV Local Set encoding rules.

Comment for version Standard 0102.5: In creating the key for the Security Metadata Local Set in version RP 0102.4, it was necessary to use the DRAFT of SMPTE RP 336M-2007. That draft contained ambiguous information, which led to the incorrect assignment of bytes five and six in the Security Metadata Local Set. The final version of SMPTE RP 336M-2007 removed the ambiguity and it became apparent that the Security Metadata Local Set Key needed to be updated.

### **4.4. Security Metadata Universal and Local Set Application in MPEG-2 Streams**

4.4.0.1 Security Metadata Universal and Local Sets **shall** be associated with the information which they describe by containing a link to some essence or metadata in the transport stream or file.

4.4.0.2 The following metadata elements **shall** be used to associate Security Metadata Sets with essence (video, audio, data) or metadata within MPEG-2 streams or files, which may contain multiple material types.

#### **4.4.1. Metadata Links within MPEG-2 Streams**

Any KLV metadata that conforms to SMPTE 336M (whether individual metadata, sets, or packs) may be linked to MPEG-2 ES within TS or PS formats using the following unique MPEG-2 stream identifiers:

##### **4.4.1.1 Unique Material Identifier (UMID)**

If used, the 32-byte UMID defined by SMPTE 330M **shall** be used to identify the essence to which security metadata is linked.

##### **4.4.1.2 Stream ID**

In MPEG-2 Program Streams the 8-bit stream\_id specifies the type and number of the Elementary Stream. In MPEG-2 Transport Streams the stream\_id may be set by the user to any valid value which correctly describes the Elementary Stream type. (ISO/IEC

## UNCLASSIFIED

13818-1, par 2.4.3.7 and Table 2-18) The stream\_id *shall* be the Value for the Stream ID metadata element.

### 4.4.1.3 Transport Stream ID

When multiple Transport Streams are present in a network environment the 16-bit transport\_stream\_id uniquely identifies a specific Transport Stream from any other Transport Stream to remove any ambiguity. Its value is defined by the originator. (ISO/IEC 13818-1, par 2.4.4.5.) The transport\_stream\_id *shall* be the Value for the Transport Stream ID.

### 4.4.1.4 Universal Label Key ID

The 16-byte Universal Label Key for the element, set or pack to which the Security Metadata Set is linked *shall* be the Value of the Universal Label Key ID.

## 4.4.2. Linking Security Metadata to MPEG-2 Streams

To indicate the security classification of individual MPEG-2 streams the appropriate link metadata elements shall be contained within a Security Metadata Sets as follows:

*4.4.2.1 Elementary Streams*– Use of stand-alone ES formats outside of an MPEG-2 TS or PS is discouraged for the reasons cited in the MISB RP 0101, *Use of MPEG-2 Systems Streams in Digital Motion Imagery Systems*. However, each Elementary Stream within a Transport Stream or Program Stream may be associated with a valid Metadata Security Set by containing the one or more UMID or Stream ID metadata elements for the streams to which they apply. If the same Metadata Security Set applies to multiple Elementary Streams then the Metadata Security Set *shall* contain each of the UMIDs or Stream IDs separately in the Set.

*4.4.2.2 Transport Streams* – Each Transport Stream may be associated with a valid Metadata Security Set by containing the UMID or Transport Stream ID metadata element for that Transport Stream. The Security Metadata Sets for the Transport Stream *shall* convey all the security information for the highest classification Elementary Stream or metadata contained in the Transport Stream.

*4.4.2.3 Program Streams* – The UMID *shall* be used for directly linking Security metadata to identified Program Streams in their entirety.

4.4.2.4 The Security Metadata Sets for the Program Stream *shall* convey all the security information for the highest classification Transport Stream, Elementary Stream or metadata contained in the Program Stream.

## 4.4.3. Linking Security Metadata to Other Metadata

4.4.3.1 When only a single metadata element is associated with a Security Metadata Set the Security Metadata Set *shall* contain the Universal Label Key ID the Value of which is the 16-byte Universal Label Key for the single metadata element.

4.4.3.2 When some, but not all metadata elements within a set or pack must be linked to a Security Metadata Set, the Security Metadata Set *shall* contain each individual Universal Label Key ID for the metadata to which it is linked.

## UNCLASSIFIED

4.4.3.3 When all metadata in a set or pack is associated with a Security Metadata Set then the set or pack *shall* contain the Security Metadata Set with a Universal Label Key ID whose value is the Universal Label Key for the set or pack.

4.4.3.4 If all metadata in an Elementary Stream is associated with the same Security Metadata Set then the two *shall* be associated using the method in 4.3.2 above for Elementary Streams.

### 4.4.4. Security Metadata without Links

When no links are used in the Security Metadata Set all the security information *shall* be considered to apply to all the essence and metadata in the MPEG-2 TS or PS.

### 4.4.5. Security Metadata Universal and Local Set Repetition Rate

Security Metadata Sets *shall* be repeated at regular intervals within a stream or file consistent with any changes in classification or planned use by applications. Applications that produce very short motion imagery clips or segments of a few seconds in duration may need to repeat Security Metadata Sets as often as every frame.

### 4.4.6. Unclassified Essence and Metadata

When essence and/or metadata are entirely unclassified the Security Metadata Set *shall* consist of the value "UNCLASSIFIED//" for Security Classification. Other entries in the Set that limit or clarify the classification are optional.

### 4.4.7. Partial Security Metadata Universal and Local Sets

For some operational situations or applications not all metadata elements in Par. 4.1 may be required. It is the responsibility of the originator and his cognizant Security official to ensure that all appropriate security entries are filled in.

### 4.4.8. Absence of Security Metadata Universal or Local Sets in MPEG-2 Streams

*The absence of Security Metadata Sets cannot and shall not be construed as rendering an MPEG-2 stream or metadata Unclassified.* The proper insertion of Security Metadata Sets into MPEG-2 streams and the extraction of Security information is the responsibility of system developers. It is the responsibility of bitstream originators and system developers to incorporate continual checks for Security Metadata Sets in their applications

## **4.5. Version Number**

### 4.5.1. Version

4.5.1.1 The version number of the Security Metadata Universal and Local Set for Digital Motion Imagery is indicated via the Version Key. For MISB RP 0102.4, Standard 0102.5, and later versions, this key *shall* be required.

4.5.1.2 In the absence of this key, the version RP 0102.3 *shall* be assumed.

**UNCLASSIFIED**

**4.6 Summary of Security Metadata Universal Set Elements**

Metadata elements allowed in a Security Metadata Universal Set are summarized in Table 1.

**Table 1 - Security Metadata Universal Set Elements (Normative)**

16-byte UL	Name	Data Type or References	Allowed Values or References	Maximum or Default Length (Bytes)	Required/Optional/Context
06 0E 2B 34 01 01 01 03 02 08 02 01 00 00 00 00	Security Classification	ISO 7 bit Enumerated Text	TOP SECRET// SECRET// CONFIDENTIAL// RESTRICTED// UNCLASSIFIED//	14	Required
06 0E 2B 34 01 01 01 03 07 01 20 01 02 07 00 00	Classifying Country and Releasing Instructions Country Coding Method	ISO 7 bit Enumerated Text	ISO-3166 Two Letter ISO-3166 Three Letter ISO-3166 Numeric FIPS 10-4 Two Letter FIPS 10-4 Four Letter 1059 Two Letter 1059 Three Letter  FIPS 10-4 Mixed ISO 3166 Mixed STANAG 1059 Mixed	21 (40 max)	Required
06 0E 2B 34 01 01 01 03 07 01 20 01 02 08 00 00	Classifying Country	Enumerated Text from the appropriate standard preceded by ‘//’	FIPS 10-4 ISO-3166 STANAG 1059	6	Required
06 0E 2B 34 01 01 01 01 0E 01 02 03 02 00 00 00	Security-SCI/SHI Information	ISO 7 bit	Security Ref 2.1.1	40	Context
06 0E 2B 34 01 01 01 03 02 08 02 02 00 00 00 00	Caveats	Free Text	Security Ref 2.1.2	20 (32 max)	Context
06 0E 2B 34 01 01 01 03 07 01 20 01 02 09 00 00	Releasing Instructions	ISO 7 bit Free Text	Security Ref 2.1.1 Refs 2.1.11, 2.1.12, 2.1.13	40	Context
06 0E 2B 34 01 01 01 03 02 08 02 03 00 00 00 00	Classified By	ISO 7 bit Free Text	Security Refs 2.1.2, 2.2.11	40	Context
06 0E 2B 34 01 01 01 03 02 08 02 06 00 00 00 00	Derived From	ISO 7 bit	Security Refs 2.1.2,	40	Context

**UNCLASSIFIED**

		Free Text	2.2.11		
<b>06 0E 2B 34 01 01 01 03 02 08 02 04 00 00 00 00</b>	Classification Reason	ISO 7 bit Free Text	Security Refs 2.1.2, 2.2.11	40	Context
<b>06 0E 2B 34 01 01 01 03 02 08 02 05 00 00 00 00</b>	Declassification Date	ISO 7 bit Free Text	YYYYMMDD Or MR	8 (32 max)	Context
<b>06 0E 2B 34 01 01 01 03 02 08 02 08 00 00 00 00</b>	Classification and Marking System	ISO 7 bit Free Text	N/A	40	Context
<b>06 0E 2B 34 01 01 01 03 07 01 20 01 02 06 00 00</b>	Object Country Coding Method	ISO 7 bit Enumerated Text	ISO-3166 Two Letter ISO-3166 Three Letter ISO-3166 Numeric FIPS 10-4 Two Letter FIPS 10-4 Four Letter 1059 Two Letter 1059 Three Letter	21 (40 max)	Required
<b>06 0E 2B 34 01 01 01 03 07 01 20 01 02 01 01 00</b>	Object Country Codes	16-bit UNICODE string Free Text	Refs 2.1.11, 2.1.12	40	Required
<b>06 0E 2B 34 01 01 01 03 02 08 02 07 00 00 00 00</b>	Classification Comments	ISO 7 bit Free Text	N/A	480	Optional
<b>06 0A 2B 34 01 01 01 01 01 01 01 XY 00 00 00 00</b>	UMID Video	SMPTE RP210	SMPTE 330M	32	Context
<b>06 0A 2B 34 01 01 01 01 01 01 01 02 XY 00 00 00 00</b>	UMID Audio	SMPTE RP210	SMPTE 330M	32	Context
<b>06 0A 2B 34 01 01 01 01 01 01 03 XY 00 00 00 00</b>	UMID Data	SMPTE RP210	SMPTE 330M	32	Context
<b>06 0A 2B 34 01 01 01 01 01 01 04 XY 00 00 00 00</b>	UMID System	SMPTE RP210	SMPTE 330M	32	Context
<b>06 0E 2B 34 01 01 01 03 01 03 04 02 00 00 00 00</b>	Stream ID	Integer	ISO/IEC 13818-1	1	Context
<b>06 0E 2B 34 01 01 01 03 01 03 04 03 00 00 00 00</b>	Transport Stream ID	Integer	ISO/IEC 13818-1	2	Context
<b>06 0E 2B 34 01 01 01 03 01 03 06 01 00 00 00 00</b>	Item Designator ID (16 byte)	SMPTE 336M	SMPTE 336M	16	Context
<b>06 0E 2B 34 01 01 01 01 0E 01 02 05 04 00 00 00</b>	Version	UInt16	Value is version number of this document; e. g. for STD 0102.8, this value is 0d08	2	Required

Note: XY = 10, 11, 12, 20, 21, or 22.

**4.7 Summary of Security Metadata Local Set Elements**

Metadata elements allowed in a Security Metadata Local Set are summarized in Table 2.

**Table 2 - Security Metadata Local Set Elements (Normative)**

<b>Tag</b>	<b>Name</b>	<b>Data Type or References</b>	<b>Allowed Values or References</b>	<b>Maximum or Default Length (Bytes)</b>	<b>Required/Optional/Context</b>
<b>1</b>	Security Classification	Unsigned Integer	UNCLASSIFIED// (0x01) RESTRICTED// (0x02) CONFIDENTIAL// (0x03) SECRET// (0x04) TOP SECRET// (0x05)	1	Required
<b>2</b>	Classifying Country and Releasing Instructions Country Coding Method	Unsigned Integer	ISO-3166 Two Letter (0x01) ISO-3166 Three Letter (0x02) FIPS 10-4 Two Letter (0x03) FIPS 10-4 Four Letter (0x04) ISO-3166 Numeric (0x05) 1059 Two Letter (0x06) 1059 Three Letter (0x07) <i>Omitted Value (0x08)</i> <i>Omitted Value (0x09)</i> FIPS 10-4 Mixed (0x0A) ISO 3166 Mixed (0x0B) STANAG 1059 Mixed (0x0C)	1	Required
<b>3</b>	Classifying Country	Enumerated Text from the appropriate standard preceded by ‘//’	FIPS 10-4 ISO-3166 STANAG 1059	6	Required
<b>4</b>	Security-SCI/SHI information	ISO7	Security Ref 2.1.1	40	Context
<b>5</b>	Caveats	Free Text	Security Ref 2.1.2	20 (32 max)	Context
<b>6</b>	Releasing Instructions	Free Text	Security Ref 2.1.1 Refs 2.1.11, 2.1.12, 2.1.13	40	Context
<b>7</b>	Classified By	Free Text	Security Refs 2.1.2, 2.2.11	40	Context
<b>8</b>	Derived From	Free Text	Security Refs 2.1.2, 2.2.11	40	Context
<b>9</b>	Classification Reason	Free Text	Security Refs 2.1.2, 2.2.11	40	Context

**UNCLASSIFIED**

<b>10</b>	Declassification Date	Free Text	YYYYMMDD Or MR	8	Context
<b>11</b>	Classification and Marking System	Free Text	N/A	40	Context
<b>12</b>	Object Country Coding Method	Unsigned Integer	ISO-3166 Two Letter (0x01) ISO-3166 Three Letter (0x02) ISO-3166 Numeric (0x03) FIPS 10-4 Two Letter (0x04) FIPS 10-4 Four Letter (0x05) 1059 Two Letter (0x06) 1059 Three Letter (0x07)	1	Required
<b>13</b>	Object Country Codes	Free Text	Refs 2.1.11, 2.1.12	40	Required
<b>14</b>	Classification Comments	Free Text	N/A	480	Optional
<b>15</b>	UMID Video	SMPTE RP210	SMPTE 330M	32	Context
<b>16</b>	UMID Audio	SMPTE RP210	SMPTE 330M	32	Context
<b>17</b>	UMID Data	SMPTE RP210	SMPTE 330M	32	Context
<b>18</b>	UMID System	SMPTE RP210	SMPTE 330M	32	Context
<b>19</b>	Stream ID	Integer	ISO/IEC 13818-1	1	Context
<b>20</b>	Transport Stream ID	Integer	ISO/IEC 13818-1	2	Context
<b>21</b>	Item Designator ID (16 byte)	SMPTE 336M	SMPTE 336M	16	Context
<b>22</b>	Version	UInt16	Value is version number of this document; <i>e. g.</i> for STD 0102.8, this value is 0d08	2	Required

## 4.8 Conversion of Security Metadata Elements between Universal and Local Sets

For bandwidth efficiency, some elements in the local set are formatted differently than the Universal set equivalent. This section provides conversion information for the differing items.

### 4.7.1. Security Classification

From Universal Set to Local Set:

Convert string to unsigned integer.

From Local Set to Universal Set:

Convert unsigned integer to all uppercase string.

### 4.7.2. Classifying Country and Releasing Instructions Country Code

From Universal Set to Local Set:

Convert string to unsigned integer.

From Local Set to Universal Set:

Convert unsigned integer to all uppercase string.

### 4.7.3. Object Country Coding Method

From Universal Set to Local Set:

Convert string to unsigned integer.

From Local Set to Universal Set:

Convert unsigned integer to all uppercase string.

## 4.9 “Mixed” Country Coding Methods

1. **(Normative)** The *CAPCO Authorized Classification and Control Marking Register Annex F* is the approved source of (coalition and other multi-national organization) tetragraphs.
2. **(Normative)** The Mixed Country Coding Method *shall* be used to support di- or tri-graphs (but not both) from FIPS 10-4, ISO 3166, and STANAG 1059, respectively, *and* approved tetragraphs in the same field. That is, a Tag 2 value of “0C” would indicate that the payload of Tag 6 consists of STANAG 1059 di-graphs or tri-graphs (but not both) **and** one or more tetragraphs from the *CAPCO Authorized Classification and Control Marking Register*.
3. **(Informative)** DISA recommends (but does not require) that di-graphs come from *FIPS 10-4* and tri-graphs come from *ISO 3166* (of which *STANAG 1059* is a profile).
4. **(Informative)** CAPCO requires that *document* header/footer and portion mark classification country codes be ISO 3166 trigraphs.

### ACRONYMS/Abbreviations

CAPCO	Controlled Access Program Coordination Office
DCID	Director of Central Intelligence Directive
EG	Engineering Guidelines
ES	Element Stream
FIPS	Federal Information Processing Standard
ICD	Intelligence Community Directive
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KLV	Key Length Value
LDS	Local Data Sets
MISB	Motion Imagery Standards Board
MPEG	Moving Picture Expert Group
ODNI	Office of the Director of National Intelligence
PS	Program Stream
RP	Recommended Practices
RTP	Real-time Transport Protocol
SCI	Sensitive Compartmented Information
SMPTE	Society of Motion Picture and Television Engineers
STANAG	NATO Standardization Agreement
TS	Transport Stream
UDS	Universal Data Sets
UMID	Unique Material ID