ACS Marking Definition Version 3.0a for STIX™ Version 2.1

Final

1 December 2021

​Integrated Cyber Defense Working Group (ICDWG)

​Editors:

ICDWG - Access Control Specification Sub-Working Group

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

* Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a
* Intelligence Community Authorized Classification and Control Markings, Register and Manual (Version 5.1)
* Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community
* STIX™ Version 2.1 – OASIS specification

Related work:

This specification replaces or supersedes:

* *N/A*

Abstract:

Initially developed to support information sharing by the Enhance Shared Situational Awareness (ESSA) initiative across the Federal Cyber Centers, the Information Sharing Architecture (ISA) Access Control Specification (ACS) document specifies a common set of elements for tagging information and related common attributes that indicate characteristics of a person or system that allow automated decisions to be made regarding information sharing. This document defines an approach to express ACS using Structured Threat Information Expression (STIXTM) language via the use of a marking definition.

# 1.​ Data Markings in STIX

Data markings represent restrictions, permissions, and other guidance for how data can be used and shared. For example, data may be shared with the restriction that it must not be re-shared, or that it must be encrypted at rest. In STIX, data markings are specified using the marking-definition object.

This document defined the Access Control Specification (ACS) Marking as expressed as a STIX 2.1 marking-definition object. For general information on data markings in STIX, including TLP markings see section 7 of STIX™ Version 2.1 - OASIS specification.

### ​**2.****Access Control Specification (ACS) Marking Object Type**

The Access Control Specification (ACS) marking type defines the object types required to implement automated access control systems based on the relevant policies governing sharing between participants.

Because ACS data markings are not part of the STIX 2.1 specification, they must be specified using the Extension Definition object as described in section 7.3 of the specification.

Information sharing across a Federal Cybersecurity Information Sharing Community requires a capability to protect and allow access to information in accordance with applicable information sharing agreements, policies, and laws. This marking definition is the result of collaboration among this community.

Please refer to "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a" for more information on creating ACS data marking definitions. Many of the definitions found below are derived directly from that document.

**Type Name:** isa-acs-3-0-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **identifier** (required) | string | This required property holds a single unique identifier associated with the resource. This value can be used for tracking data provenance, executing data retraction, and enforcing auditing requirements. The Resource Identifier **MUST** use a format that includes a prefix and an RFC4122 suffix. The prefix used will include the ISA common prefix (GUIDE prefix). The ISA has been assigned a GUIDE (Globally Unique Identifier for Everything) prefix of 19001 for production and 999191 for test use.  It is recommended that RFC 4122 Version 4 UUIDs be used for the suffix; however, other versions are permitted. |
| **name** (optional) | string | This property provides a "handle" to identify and describe this marking definition.  Note that the **name** property in no way defines the data marking. It is simply provided as a convenience for users. |
| **create\_date\_time** (required) | timestamp | This required property provides the creation date and time of the associated resource as identified by the Identifier. This value supports a number of functions including enforcing data retention policies and auditing requirements. |
| **responsible\_entity\_custodian** (required) | open-vocab | This property represents the data producer that is responsible for providing the associated resource to be shared. It is represented as an organization value. This value is necessary for auditing and enforcing data retention and provenance policies.  Allowable values, listed in Appendix A: List of Organizations of "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a"**, SHOULD** be used.  The set of allowable values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **responsible\_entity\_originator**  (optional) | open-vocab | This optional property represents the originating organization for the associated resource. If not present, then the origin of the information is unspecified. It is represented as an organization value. An appropriate value from the organizations in Appendix A: List of Organizations of "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a" **SHOULD** be used. However, additional values may be created to specify the originator.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification.  Certain Originators may require anonymity to protect their identity. This is common when dealing with a cybersecurity threat or incident where the originator is an entity in the Private Sector. Cover terms (e.g., USENERGY01) assigned to an entity should be carried through anytime the resource is shared. |
| **authority\_reference**  (optional) | list of type string | This property captures the legal authority under which the content was created, not the limitation on sharing the content. This property is used for auditing and records management, not for access control decisions. In some cases, the Authority Reference is needed by ESSA Participants to be included in the Control Policy Group as well as the Resource Accounting Group.  Each entry in the list **MUST** be of the of the format *urn(:\w+)+.* |
| **policy\_reference** (required) | string | This property provides the means of indicating a particular policy related to the sharing of the resource.  Multiple URNs can be included, separated by a space, but one of the following **MUST** be included:   * urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit * urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=deny * urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit * urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny   Each value **MUST** be of the format *urn(:\w+)+.* |
| **original\_classification**  (optional) | isa-acs-original-classification-type | This property provides details for generating a classification authority block for presentation of a classified resource to an operator.  Either the Original Classification or the Derivative Classification **MUST** be provided for classified resources, as appropriate.  Details regarding the basic encoding specification detail for Original Classification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community. |
| **derivative\_classification**  (optional) | isa-acs-derivative-classification-type | This property provides details for generating a classification authority block for presentation of a classified resource to an operator.  Either the Original Classification or the Derivative Classification **MUST** be provided for classified resources, as appropriate.  Details regarding the basic encoding specification detail for Original Classification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community. |
| **declassification**  (optional) | isa-acs-declassification-type | This property provides the declassification instructions associated with an original or derived classification for generating a classification authority block for presentation of a classified resource to an operator.  Details regarding the basic encoding specification detail for Declassification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community. |
| **resource\_disposition** (optional) | isa-acs-resource-  disposition-type | This property can be used to provide a fixed date and time at which an action is to be taken on the associated resource, such as destruction. Retention can be enforced through the use of this property or through the use of policies.  This property allows for specifying ad hoc (i.e., not policy based) retention limitation requests from information creators such as private industry.  Details regarding the basic encoding specification detail for Resource Disposition are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community. |
| **public\_release**  (optional) | isa-acs-public-release-type | This property is used to provide the release authority and date for resources that have been through a formal public release determination process or note that the resource has not been publicly released.  Details regarding the basic encoding specification detail for Public Release are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community.  This property **SHOULD** be present if the **control\_set/formal\_determination** property contains PUBREL. |
| **access\_privilege** (optional) | list of type isa-acs-access-privilege-type | This property provides a means of limiting or permitting specific actions once access control decisions have been made. |
| **further\_sharing** (optional) | list of type isa-acs-further-sharing-type | This property provides a means of limiting or permitting further sharing once original access control decisions have been made. |
| **control\_set**  (required) | isa-acs-control-set-type | The **control\_set** property is the group of data tags that are used to inform automated access control decisions. |

#### 2.1 ACS Original Classification Object Type

**Type Name:** isa-acs-original-classification-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **classified\_by** (required) | string | This property contains the name of person with the original classification authority who made a classification determination. |
| **classified\_on** (optional) | timestamp | This property contains the date an original classification determination was made. |
| **classification\_reason** (optional) | string | This property contains the rationale for an original classification determination. |
| **compilation\_reason**  (optional) | string | This property contains the rationale for assigning a higher classification level than a simple roll-up of its portions would indicate. |

#### 2.2 ACS Derivative Classification Object Type

**Type Name:** isa-acs-derivative-classification-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **classified\_by** (required) | string | This property contains the name of person with the derivative[[1]](#footnote-1) classification authority who made a classification determination. |
| **classified\_on** (optional) | timestamp | This property contains the date an original classification determination was made. |
| **derived\_from** (required) | string | This property contains the citation of the original classification guidance used for a derivative classification. |

#### 2.3 ACS Declassification Object Type

**Type Name:** isa-acs-declassification-type

All properties in this object type are optional. To make use of this object type, at least one property **MUST** be present.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **declass\_exemption** (optional) | string | This property contains the basis for a resource not being subject to standard automatic declassification processes. |
| **declass\_period** (optional) | integer | This property contains the duration of time in years for calculating from a create date or classification date when a resource will be automatically declassified if not exempt. |
| **declass\_date** (optional) | timestamp | This property contains the date upon which a resource will be automatically declassified if not exempt. |
| **declass\_event** (optional) | string | This property contains the future occurrence upon which a resource will be automatically declassified if not exempt. |

## 2.4 ACS Resource Disposition Object Type

**Type Name:** isa-acs-resource-disposition-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **disposition\_date** (required) | timestamp | This property contains the date upon which the declared disposition process is to be initiated. |
| **disposition\_process** (required) | string | This property contains the  allowed disposition process to be performed (e.g., destruction). |

## 2.5 ACS Public Release Object Type

**Type Name:** isa-acs-public-release-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **released\_by** (required) | string | This property contains the authority that authorized the public release. |
| **released\_on** (optional) | timestamp | This property contains the date of public release. |

## 2.6 ACS Access Privilege Object Type

**Type Name:** isa-acs-access-privilege-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **privilege\_action**  (required) | open-vocab | This property indicates the action that may be taken when the access privilege is allowed.  This is an open vocabulary and values **SHOULD** come from isa-privilege-action-ov vocabulary. |
| **privilege\_scope** (required) | isa-acs-privilege-scope-type | This property indicates the scope of the access privilege. |
| **rule\_effect** (required) | isa-acs-rule-effect-enum | This property indicates if actions are permitted or denied.  The values of this property **MUST** come from the isa-acs-rule-effect-enum enumeration. |

## 2.7 ACS Privilege Scope Object Type

**Type Name:** isa-acs-privilege-scope-type

All properties in this object type are optional. To make use of this object type, at least one property **MUST** be present.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **permitted\_nationalities**  (optional) | list of type string | The **permitted\_nationalities**  (CTRY) property identifies the limitation on the distribution of the resource based on nationality.  The values of this property **MUST** either contain a list with the single literal "ALL" or contain one or more values listed in Geopolitical Entities, Names, and Codes (GENC) Standard Edition 1[[2]](#footnote-2). |
| **permitted\_organizations** (optional) | list of type open-vocab | The **permitted\_organizations** (ORG) property identifies the limitation on the distribution of the resource based on organization.  The values of this property **MUST** either contain a list with the single literal "ALL" or contain one or more values listed in Appendix A: List of Organizations of "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a".  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **shareability** (optional) | list of type isa-acs-shar-enum | The **shareability** (SHAR) property is used to identify the shareability of a resource that may be released based on the determination of an originator in accordance with established disclosure procedures.  The values of this property **MUST** either contain a list with the single literal "ALL" or contain one or more values from the isa-acs-shar-enum enumeration. |
| **entity** (optional) | list of type isa-acs-entity-enum | The **entity** (ENTITY) property is used to identify the entities to which information may be released based on the determination of an originator.  The values of this property **MUST** either contain a list with the single literal “ALL” or contain one or more values from the isa-acs-entity-enum enumeration. |

## 2.8 ACS Further Sharing Object Type

**Type Name:** isa-acs-further-sharing-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **sharing\_scope** (required) | list of type open-vocab | This property indicates the scope of the further sharing. The organizations in Appendix A: List of Organizations of "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a" **SHOULD** be used. The values, FOREIGNGOV or SECTOR **MAY** also be used.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **rule\_effect** (required) | isa-rule-effect-enum | This property indicates if further sharing is permitted or denied.  The values of this property **MUST** come from the isa-acs-rule-effect-enum enumeration. |

## 2.9 ACS Control Set Object Type

**Type Name:** isa-acs-control-set-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **classification**  (required) | isa-acs-classification-enum | This property contains information specifying the classification level.  The Classification value contains the classification of the data based on the Executive Order 13526, Classified National Security Information and the Information Security Manual (ISM) marking system. Unclassified information will include a classification marking.  The value of this property **MUST** come from the isa-acs-classification-enum enumeration. |
| **sci\_controls** (optional) | list of type open-vocab | The appropriate values for the sensitive compartmented information (SCI) property are listed in MDM SCI Control List.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **logical\_authority\_category** (optional) | list of type open-vocab | The **logical\_authority\_category** (LAC) property represent classes of authority upon which data can be generated or acquired and that can be used to apply mandatory special access control and handling policies.  The allowable values are listed in the NSA’s Master Data Registry.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **formal\_determination** (optional) | list of type isa-acs-fd-enum | The **formal\_determination** (FD) property is used to Indicate other formal determinations beyond classification that have been applied to a resource.  The values of this property **MUST** come from the isa-acs-fd-enum enumeration. |
| **caveat** (optional) | list of type isa-acs-cvt-enum | The **caveat** (CVT) property is used to indicate a specific control.  The values of this property **MUST** come from the isa-acs-cvt-enum enumeration. |
| **sensitivity** (optional) | list of type isa-acs-sens-enum | The **sensitivity** (SENS) property is used to specify an inherent sensitivity about the data that requires specific restrictions in access or handling.  The values of this property **MUST** come from the isa-acs-sens-enum enumeration. |
| **shareability** (optional) | list of type isa-acs-shar-enum | The **shareability** (SHAR) property is used to identify the shareability of a resource that may be released based on the determination of an originator in accordance with established disclosure procedures.  The values of this property **MUST** come from the isa-acs-shar-enum enumeration. |
| **entity** (optional) | list of type isa-acs-entity-enum | The **entity** (ENTITY) property is used to identify the entities to which information may be released based on the determination of an originator.  The values of this property **MUST** come from the isa-acs-entity-enum enumeration. |
| **permitted\_nationalities**  (optional) | list of type string | The **permitted\_nationalities**  (CTRY) property identifies the limitation on the distribution of the resource based on nationality.  Allowable values are listed in Geopolitical Entities, Names, and Codes (GENC) Standard Edition 1[[3]](#footnote-3) **MUST** be used. |
| **permitted\_organizations** (optional) | list of type open-vocab | The **permitted\_organizations** (ORG) property identifies the limitation on the distribution of the resource based on organization.  Allowable values listed in Appendix A: List of Organizations of "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a" **MUST** be used.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |

## 2.10 ACS Privilege Action Open Vocabulary

**Type Name**: isa-as-privilege-action-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| DSPLY | The action of displaying, either in a hard copy document or a visual presentation of the resource. DSPLY should be used to permit display when there is generally a global deny for all actions. |
| IDSRC | The action of identifying the source of the resource further than the entity receiving the resource. When set to deny, attributes or elements in the resource that identify the source and custodian must be removed or replaced prior to additional actions being taken. This restriction applies not only to the elements in the header of the resource but may also apply to elements within the body of the document being shared. The use of IDSRC does not authorize any changes to markings on the resource. For example, the removal of the source information will not change the classification of the resource. |
| TENOT | The action of notifying a targeted entity of a cybersecurity incident based on the resource. |
| NETDEF | The action of taking network defense actions including detection and mitigation, remediation, and local analysis and signature development, based on the resource. |
| LEGAL | The action of using the resource in legal proceedings. |
| INTEL | The action of conducting additional intelligence analysis based on the resource. |
| TEARLINE | The action of removing and taking further action on components of a resource based on their component markings. To be tear-lineable indicates that marked components of a document may be removed and treated as individually marked components. When set to deny, even though there may be components with fewer restrictions than the overall document, they may not be removed. |
| OPACTION | The action of conducting cyber-based operations applied to adversary capabilities based on the resource. |
| REQUEST | The action of requesting a waiver to an access privilege restriction. When set to deny, the originator will not consider specific requests to take actions based on the resource. |
| ANONYMOUSACCESS | The action of allowing anonymous access to the resource. This action is included to support the restrictions placed on the indicators shared with the US government from the DHS Automated Indicator Sharing (AIS) program. |
| CISAUSES | The cybersecurity purposes allowed in the Cybersecurity Information Sharing Act of 2015 |

## 2.11 ACS Rule Effect Enumeration

**Type Name**: isa-acs-rule-effect-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| permit | The specified action, privilege, etc is permitted |
| deny | The specified action, privilege, etc is denied |

## 2.12 ACS Classification Enumeration

**Type Name**: isa-acs-classification-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| U | Unclassified |
| C | Confidential |
| S | Secret |
| TS | Top Secret |

## 2.13 ACS Formal Determination Enumeration

**Type Name**: isa-acs-fd-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| AIS | The resource is appropriate for AIS (Automated Indicator Sharing) |
| FOUO | The resource is appropriate For Official Use Only. |
| NF | Indicates that the resource is releasable to U.S. citizens and not releasable to foreign nationals without the permission of the originator. |
| PII-NECESSARY-TO-UNDERSTAND-THREAT | Personally identifiable information (PII) necessary to understand the context of the resource is present. |
| NO-PII-PRESENT | Personally identifiable Information (PII) is not present. |
| PUBREL | Approved for Public Release |
| INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT | Indicates that any personal information of a specific individual or information that identifies a specific individual has been determined to be directly related to a cybersecurity threat |

## 2.14 ACS Caveat Enumeration

**Type Name**: isa-acs-cvt-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| FISA | The FISA caveat marking denotes the presence of Foreign Intelligence Surveillance Act (FISA) (Reference 18) or FISA-derived information in the document. This is an informational marking only to highlight such information. Recipients of resources with the FISA control marking are responsible for ensuring that the resource is protected in conformance with the legal requirements of the FISA for limitations on use and warning displays. |
| POSSIBLEPII | The POSSIBLEPII caveat marking indicates to the recipient that the resource may contain Personally Identifiable Information (PII). Recipients are responsible for ensuring that the resource is protected according to their agencies policies related to PII. |
| CISAPROPRIETARY | The CISAPROPRIETARY caveat marking indicates that the resource must observe appropriate restrictions as requested by the originator in accordance with the Cybersecurity Information Sharing Act of 2015. |

## 2.15 ACS Sensitivity Enumeration

**Type Name**: isa-acs-sens-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| NTOC\_DHS\_ECYBER\_SVC\_SHARE.NSA.NSA | Enhanced Cybersecurity Services |
| PCII | Protected Critical Infrastructure Information |
| LES | Law Enforcement Sensitive Information |
| INT | Intelligence Information |
| PII | Personally Identifiable Information |
| PR | Cybersecurity Targeted Entity Information |
| TEI | Commercial Proprietary Information |

## 2.16 ACS Shareability Enumeration

**Type Name**: isa-acs-shar-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| NCC | National Cyber Centers |
| EM | Emergency Management |
| LE | Law Enforcement |
| IC | Intelligence Community |

## 2.17 ACS Entity Enumeration

**Type Name**: isa-acs-entity-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| MIL | Military service member |
| GOV | U.S. federal government civilian employee |
| CTR | Contractor |
| SVR | Server |
| SVC | Service, Widget, Application, Software, etc |
| DEV | End-point device |
| NET | Network device |

## 2.18 Examples

Notice these examples of the ACS marking definitions appear as part of a marking-definition STIX object type (see section 7 of STIX™ Version 2.1 - Committee Specification 02).

The Extension Definition object is:

{  
 "id": "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce",  
 "type": "extension-definition",  
 "spec\_version": "2.1",  
 "name": "Extension to support ACS 3.0a Data Markings",  
 "description": "This schema adds ACS data markings",  
 "created": "2021-02-01T00:00:00.000000Z",  
 "modified": "2021-02-01T00:00:00.000000Z",  
 "created\_by\_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id  
 "schema": "<https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/acs-data-markings>",  
 "version": "1.0.0",  
 "extension\_types": ["property-extension"]  
}

The following example describes an ACS marking definition at the Top-Secret level. It was created on 27 June 2016 and originally classified on 10 June 2017 by the NSA. It can be used within DHS/CISA but cannot be shared with anonymous entities. It can be shared with the “FVEY” nations.

{ "type": "marking-definition",  
 "id": "marking-definition--f4d1771b-d6a6-4eb1-9768-9686efeeb89a",  
 "created": "2021-02-01T00:00:000Z",  
 "extensions": {

"extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {

       "extension\_type": "property\_extension",

"identifier": "isa:guide.19001.ACS3-bc9034f8-c732-5328-b9df-d9d72aae480b",

"name": "banner\_marking",  
 "create\_date\_time": "2016-06-27T14:10:26.723Z",  
 "responsible\_entity\_custodian": "USA.NSA",  
 "responsible\_entity\_originator": "USA.NSA",  
 "authority\_reference": [ "urn:isa:authority:CFR2013\_32\_2\_236" ],

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",  
 "original\_classification": {

"classification\_reason": "Example",  
 "classified\_by": "Available-On-Request",  
 "classified\_on": "2017-01-10T00:00:00Z",  
 "compilation\_reason": "Orig-Doc"  
 },  
 "derivative\_classification": {  
 "classified\_by": "Available-On-Request",  
 "classified\_on": "2018-02-20T00:00:00Z",  
 "derived\_from": "Orig-Doc"  
 },  
 "declassification": {  
 "declass\_period": 32,  
 "declass\_date": "2020-02-20T00:00:00Z",  
 "declass\_event": "Per Exec Order blah-blah-blah"  
 },

"access\_privilege": [

{

"privilege\_action": "CISAUSES",

"privilege\_scope": {

"permitted\_nationalities": ["USA", "AUS", "CAN", "GBR", "NZL"]

},

"rule\_effect": "permit"

},

{

"privilege\_action": "ANONYMOUSACCESS",

"privilege\_scope": {

"permitted\_nationalities": ["ALL"]

},

"rule\_effect": "deny"

}

],  
 "control\_set": {  
 "classification": "TS",

"sci\_controls": ["SI"],

"logical\_authority\_category": ["LAC12345"],

"formal\_determination": [

"AIS",

"INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"

],

"sensitivity": ["NTOC\_DHS\_ECYBER\_SVC\_SHARE.NSA.NSA"],

"permitted\_nationalities": ["USA", "AUS", "CAN", "GBR", "NZL"],  
 "permitted\_organizations": ["USA.NSA", "USA.DHS"]

}  
 }  
 }  
}

The following example describes an ACS marking definition at the Unclassified level, but determined to be FOUO. It was created on 27 June 2016 by the NSA. It can be used within DHS/CISA, shared on AIS and with other known entities, but cannot be shared with anonymous entities.

{  
 "type": "marking-definition",  
 "id": "marking-definition--11b6042f-7b98-4b97-a168-bec4c025dda9",

"created": "2021-02-01T00:00:000Z",  
 "extensions": {

"extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {

       "extension\_type": "property\_extension",

"identifier": "isa:guide.19001.ACS3-f556c2fb-9d75-4733-8d79-db311ed992d5",

"name": "some\_unclassified\_marking",   
 "create\_date\_time": "2016-06-27T14:10:26.723Z",  
 "responsible\_entity\_custodian": "USA.NSA",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",

"access\_privilege": [

{

"privilege\_action": "CISAUSES",

"privilege\_scope": {

"permitted\_nationalities": ["ALL"],

"permitted\_organizations": ["ALL"]

},

"rule\_effect": "permit"

},

{

"privilege\_action": "ANONYMOUSACCESS",

"privilege\_scope": {

"permitted\_nationalities": ["ALL"],

"permitted\_organizations": ["ALL"]

},

"rule\_effect": "deny"

}

],  
 "control\_set": {  
 "classification": "U",

"formal\_determination": ["FOUO", "AIS"],  
 "permitted\_organizations": ["USA.NSA", "USA.DHS"]  
 }

}  
 }  
}​

The following example describes an ACS marking definition at the Unclassified level with only the required properties present.

{  
 "type": "marking-definition",  
 "id": "marking-definition--0b853b6b-82fd-4396-b239-2eed3dfc8f3f",

"created": "2021-02-01T00:00:000Z",  
 "extensions": {

"extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {

       "extension\_type": "property\_extension",

"identifier": "isa:guide.19001.ACS3-c4438c90-94c5-445c-8d05-162b1d135f26",  
 "create\_date\_time": "2018-09-07T12:17:46.793Z",  
 "responsible\_entity\_custodian": "USA.NSA",  
 "authority\_reference": [ "urn:isa:authority:CFR2013\_32\_2\_236" ],

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",   
 "control\_set": {  
 "classification": "U",

}

}  
 }  
}​

# ​3.​ ACS High-Water Data Marking

Most classified documents have a data marking for the entire document that specifies the “high-water” data marking – the most restrictive data marking found in the document. To support this concept, a custom property can be added to the taxii-envelope object that is used to deliver data from a TAXII server. The property name of this custom property is **x\_usa\_gov\_banner\_marking\_ref** and it is optional. For more information see section 3.7 of the TAXII™ Version 2.1 specification.

## 3.1 Example

{

  "more": true,

  "next": "123456789",

"x\_usa\_gov\_banner\_marking\_ref":"marking-definition--f4d1771b-d6a6-4eb1-9768-9686efeeb89a,

  "objects": [

    {

      "type": "indicator",

      "id": "indicator--252c7c11-daf2-42bd-843b-be65edca9f61",

"object\_marking\_ref": "marking-definition--f4d1771b-d6a6-4eb1-9768-9686efeeb89a",

      ...

    },

...

  ]

}

The marking definition referred to in the above example can be found in section 2.18. The assumption in this example is that of all of the data markings found in this TAXII envelope, marking-definition--f4d1771b-d6a6-4eb1-9768-9686efeeb89a is a reference to the “high-water” data marking.

# ​Appendix A. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| 01 | 2018-10-23 | Gregory Cheatham  Terri Hayes  Toni Haynes  Ivan Kirillov  Timothy Lachapelle  Mark Munoz  Rich Piazza  Scott Pinkerton  David Schuler  Craig Schweinhart  Kathy Simunich  Marlon Taylor  David Thomas | Initial Version |
| 02 | 2019-09-30 | Gregory Cheatham  Terri Hayes  Toni Haynes  Ivan Kirillov  Timothy Lachapelle  Mark Munoz  Rich Piazza  Scott Pinkerton  David Schuler  Craig Schweinhart  Kathy Simunich  Marlon Taylor  David Thomas | Redesign x-isa-acs-control-set-type. |
| 03 | 2020-03-30 | Ivan Kirillov  Rich Piazza  Gramm Richardson  Kathy Simunich  Marlon Taylor  Howard Tsai  Steve Tumbarello | Reformat as stand-alone document |
| 04 | 2020-05-13 | Rich Piazza  Marlon Taylor | Remove section on Bundle, replace with section on high-water data marking. |
| 05 | 2020-07-29 | Rich Piazza | Corrections to the examples |
| 06 | 2021-05-01 | Rich Piazza | Convert to use of Extension Definitions as defined in STIX 2.1 Committee Standard 02 |
| 07 | 2021-12-01 | Rich Piazza | Unify font usage, change to STIX 2.1 OASIS Standard |

1. "derivative" in this definition is different from "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a". The use of “original” in that document is assumed to be a typo, and the classified\_by property should contain the name of the person who created the derivative classification. [↑](#footnote-ref-1)
2. <https://api.nsgreg.nga.mil/geo-political/ISO3166-1/3/VI-12> [↑](#footnote-ref-2)
3. <https://api.nsgreg.nga.mil/geo-political/ISO3166-1/3/VI-12> [↑](#footnote-ref-3)