Automated Indicator Sharing (AIS) Brokering Between the Non-Federal Entities Sharing Community and the Federal Entities Sharing Community

V2.0

Publication: November 2021
Cybersecurity and Infrastructure Security Agency

Table of Contents

1 Executive Summary 4

2 Introduction 5

2.1 Overview of Brokering 5

2.2 Scope of Document 6

2.3 Sharing Infrastructure 7

3 Brokering from Non-Federal Entities to Federal Entities 7

3.1 Non-Federal Entity Originated Information Use Case 7

3.2 Non-Federal Entity Markings 8

3.3 DHS/CISA Non-Federal to Federal Brokering 9

3.3.1 Markings Translation 9

3.3.2 Describing ACS Marking Properties 15

4 Brokering from Federal Entities to Non-Federal Entities 17

4.1 Federal Entity Originated Information Use Case 17

4.2 DHS/CISA Federal Entity to non-Federal Entity Brokering 18

4.2.1 STIX Translation 18

4.2.2 Personal Information 19

4.2.3 Federal Entity Originated Information Data Stewardship 20

4.2.4 Describing ACS Marking Properties 20

5 Anonymization (AIS consent) 22

5.1 Non-Federal Submissions 22

5.2 Federal Submissions 23

6 Appendix A: Acronyms 24

7 Appendix B: Definitions 25

8 Appendix C: Non-Federal Submissions to Federal/Non-Federal Feeds Examples 26

8.1 Example C.1: No AIS Consent, TLP:White (Row 1) 29

8.2 Example C.2. ais-consent-none, TLP:Green (Row 5) 32

8.3 Example C.3. ais-consent-none, TLP:Amber (Row 6) 35

8.4 Example C.4. ais-consent-usg, TLP:Green (Row 8) 38

8.5 Example C.5. ais-consent-everyone, TLP:White (Row 10) 41

8.6 Example C.6. ais-consent-everyone-cisa-proprietary, TLP:Amber (Row 15) 43

9 Appendix D: Federal Submissions to Federal/Non-Federal Feeds Examples 45

9.1 Example D.1. PUBREL, privdefault = permit, no ais-consent (Row 2) 48

9.2 Example D.2. PUBREL, privdefault = deny, ais-consent-none (Row 5) 50

9.3 Example D.3. FOUO/AIS, privdefault = permit, ais-consent-everyone (Row 19) 52

9.4 Example D.4. PUBREL, privdefault = deny/IDSRC=permit, ais-consent-everyone (Row 20a) 54

9.5 Example D.5. FOUO/AIS, privdefault = deny, ais-consent-everyone (Row 22).....56

9.6 Example D.6. PUBREL, privdefault = deny, ais-consent-everyone (Row 23).....58

10 Appendix E: Federal Submissions of Non-Federal Content Examples..... 60

10.1 Non-Federal Submissions to Federal Entities.....61

10.1.1 Non-Federal Content as STIX / ais-consent-everyone-cisa-proprietary (Scenario 1).....61
10.1.2 Non-Federal Content as text / ais-consent-everyone-cisa-proprietary (Scenario 2) 62
10.1.3 Non-Federal Content as STIX / ais-consent-everyone (Scenario 3) 62
10.1.4 Non-Federal Content as text / ais-consent-everyone (Scenario 4).....63
10.1.5 Non-Federal Content as STIX / ais-consent-none (Scenario 5) 63
10.1.6 Non-Federal Content as text / ais-consent-none (Scenario 6).....64
10.1.7 Non-Federal Content as STIX / n/a (default to ais-consent-none) (Scenario 7).....64
10.1.8 Non-Federal Content as text / no ais-consent information given (Scenario 8) 65
10.1.9 Non-Federal Content as STIX / ais-consent-usg (Scenario 9).....65
10.1.10 Non-Federal Content as text / ais-consent-usg (Scenario 10) 66

10.2 Federal Submissions of Non-Federal Submissions to AIS 67

10.2.1 Federal Submission for Scenario 1 & 2 67
10.2.2 Federal Submission for Scenario 3 & 4 69
10.2.3 Federal Submission for Scenario 5 & 6 71
10.2.4 Federal Submission for Scenario 7 & 8 73
10.2.5 Federal Submission for Scenario 9 & 10 75

11 Appendix F: CUST and ORIG values..... 77

1 Executive Summary

In the cyber ecosystem, we are working as fast as we can to keep up with the scale and speed of cyber intrusions and attacks. The malicious actors are leveraging each other's tools and knowledge to get better at what they do, as fast if not faster than we are getting better at what we do.

In December 2015, Congress enacted the Cybersecurity Information Sharing Act of 2015 (CISA 2015) to create a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators (CTIs) and defensive measures (DMs) while protecting classified information, intelligence sources and methods, and privacy and civil liberties.

The Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (DHS/CISA), in coordination with interagency partners as required by CISA 2015, provides operational procedures and guidelines for Federal and non-Federal entities to share CTIs and DMs. In real time, Federal entities exchange unclassified CTIs and DMs under the Multi-lateral Information Sharing Agreement (MISA), using DHS/CISA-hosted infrastructure. Non-Federal entities exchange CTIs and DMs in real time under the Automated Indicator Sharing initiative (AIS) Terms of Use (ToU), also using DHS/CISA-hosted infrastructure. These two communities, Federal and Non-Federal entities, form two independent sharing communities but are able to leverage information between them as an important tool to quickly mitigate cyber threats and enable defensive measures.

This document describes the processing performed by DHS/CISA, who provides brokering capabilities that enable the two independent cyber information sharing communities to exchange unclassified or declassified CTIs and DMs in an automated, real-time manner. More specifically, brokering enables (1) the AIS-participating non-Federal entities to receive, in real time, information that originates in the Federal Cybersecurity Information Sharing Community and (2) the Federal Cybersecurity Information Sharing Community to receive, in real time, information that originates from non-Federal entities.

There is significant existing documentation on both the non-Federal and Federal Cybersecurity Information Sharing Communities, including the agreements, policies, and processes that govern community members plus descriptions of the language, format, and types of data each community uses. Those documents are referenced and summarized, as appropriate, within this document. Also, note that nothing in this document precludes other sharing among and between Federal entities and the non-Federal entities.

2 Introduction

In December 2015, Congress enacted the Cybersecurity Information Sharing Act of 2015 (CISA 2015)[1] to create a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators (CTIs) and defensive measures (DMs) while protecting classified information, intelligence sources and methods, and privacy and civil liberties. In accordance with CISA 2015, the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (DHS/CISA), in coordination with interagency partners as required, provided operational procedures and guidelines[2] for Federal and non-Federal entities to share CTIs and DMs.

Federal entities exchange classified and unclassified cyber information in real time under the Multi-lateral Information Sharing Agreement (MISA)[3]. Unclassified Federal entity cyber information exchange uses DHS/CISA-hosted infrastructure. Non-Federal entities exchange CTIs and DMs in real time under the Automated Indicator Sharing (AIS) Terms of Use (ToU), also using DHS/CISA-hosted infrastructure.[4] The Federal and non-Federal entities form two independent sharing communities but are able to share and leverage information between them via machine-to-machine exchanges and processing[5] to quickly mitigate cyber threats and enable defensive measures. DHS/CISA provides a capability to interface between the two communities that includes processing, filtering, and marking translations.

2.1 Overview of Brokering

A "Broker" provides a secure, reliable means to transfer information from one Trust Community to another, where the transfer is consistent and compatible with the Information Technology safeguards of each. Each sharing community independently shares information within a dedicated sharing infrastructure, but the ability to exchange information between communities requires intermediary brokering that allows communities to connect to each other. In this case, the two trust communities are the Federal entities (under MISA) and non-Federal entities (under AIS ToU) while DHS/CISA (the broker) automatically moves information between the communities in a way that is transparent to the information producers and consumers. DHS/CISA also plays the role of member and Shared Capability Provider (SCP). DHS/CISA's role in these environments is outlined in Figure 1.

[1] CISA 2015 is codified at 6 U.S.C. §§ 1501-1510. For ease of reference, this document generally cites to the sections as codified in title 6 of the U.S. Code.

[2] Current versions of the relevant documents are available at cisa.gov/ais.

[3] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

[4] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

[5] Automation is enabled by standards such as STIX and TAXII, which define a common language and transport mechanism.

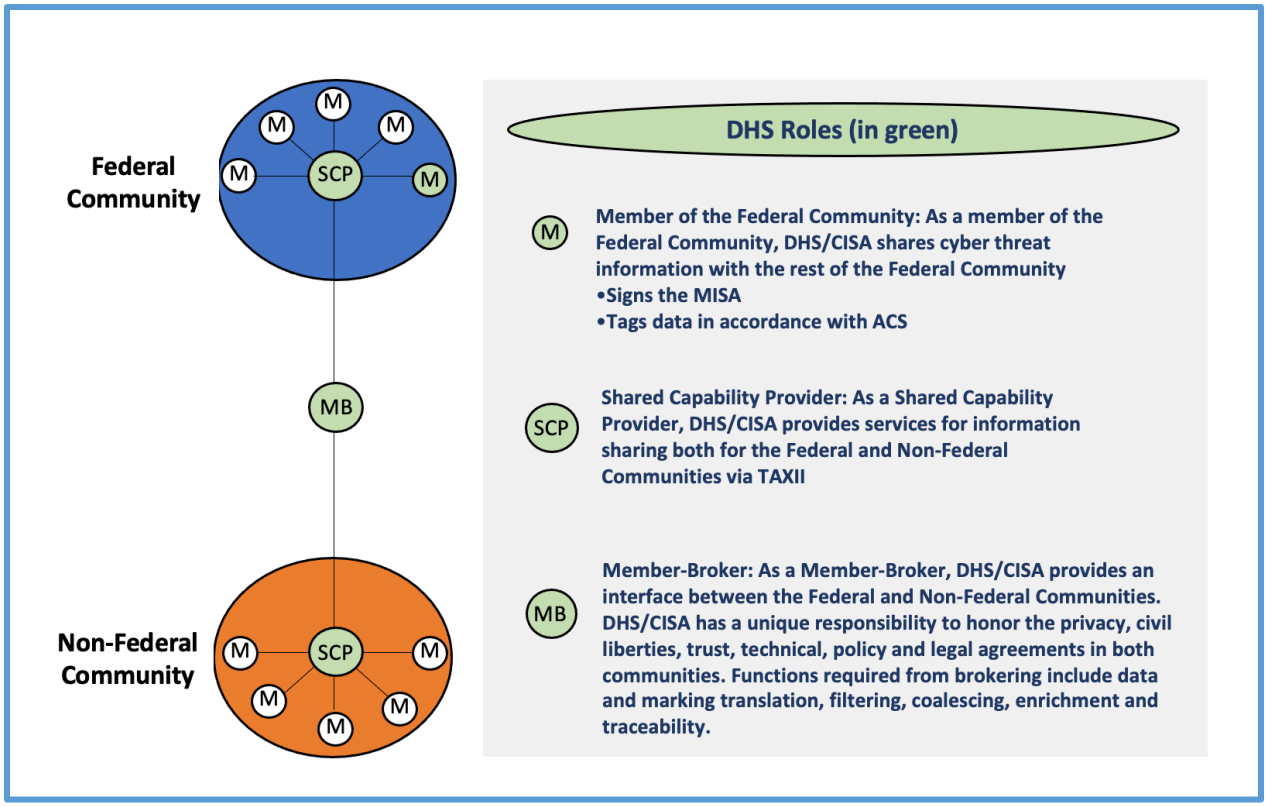

Figure 1: DHS/CISA Roles in Context of the Federal and Non-Federal Trust Communities

Information existing within a Trust Community carries restrictions defined by the originating Trust Community. Brokering includes the interpretation of undocumented, ambiguous, evolving intra-Trust-Community access restrictions into unambiguous terms that can be honored outside the originating Trust Community.

Brokering also includes such functions as translating, filtering, and anonymizing between the two communities. DHS/CISA filters information received from the Federal entity producers, absent explicit markings that permit dissemination to non-Federal entities, so that it is only delivered to Federal entity participants. In a similar fashion, non-Federal entity originated information may require filtering prior to dissemination to the Federal Cybersecurity Information Sharing Community. DHS/CISA understands the needs of each Community so the translation can be targeted and specific.

2.2 Scope of Document

This document describes the processing performed by DHS/CISA, as the broker, to enable the Federal and non-Federal cyber information sharing communities to exchange information. DHS/CISA shares:

- Non-Federal entity-originated CTI and DM in real-time to Federal Cybersecurity Information Sharing Community participants in a format that fully describes handling, access control and usage constraints that were specified by the non-Federal entity using Traffic Light Protocol (TLP) markings as described in 2.2 below. The TLP markings are translated by DHS/CISA into the Information Sharing Architecture (ISA) Access Control Specification (ACS) markings prior to sharing with Federal entities.[6]
- Unclassified Federal entity-originated information in real-time to non-Federal entities per the access

[6] "ISA Access Control Specification v3.0a" June 2019

control markings affixed by the Federal entity originator. The Federal entity originator must explicitly elect to share with non-Federal entities before DHS/CISA will disseminate information to non-Federal entities. The designation for AIS sharing by the Federal entity originator is documented in ACS, and translated by DHS/CISA into TLP markings.

- Unclassified Federal entity-originated information marked for dissemination to non-Federal entities with the rest of the Federal community. Because this information destined for the non-Federal community is filtered and modified due to privacy and security requirements, DHS/CISA acts a broker when disseminating this information to the non-Federal entities. DHS/CISA applies appropriate TLP markings for information disseminated to the non-Federal entities. DHS/CISA shares the information with the original ACS markings to Federal entities.

This document is not intended to be a standalone document. There is significant existing documentation on both the Non-Federal and Federal Cybersecurity Information Sharing Communities, including the agreements, policies and processes that govern members of each Community plus descriptions of the language, format, and types of data that each community uses. Those documents are referenced and briefly summarized, as appropriate, within this document.

2.3 Sharing Infrastructure

To participate in machine-to-machine sharing via AIS, the non-Federal and Federal entity participants host a small amount of client software that interfaces with DHS/CISA Central Shared Infrastructure. The messaging hub and client software uses the Trusted Automated eXchange of Intelligence Information (TAXII) protocol over an encrypted connection. The DHS/CISA messaging infrastructure authenticates the non-Federal and Federal entities identity using trusted public key infrastructure (PKI) certificates. Non-Federal and Federal entities must submit documents formatted in machine-readable file (Structured Threat Information eXpression (STIX) format) containing data properties to be shared in accordance with the AIS Profile and AIS Submission Guidance.[7] The TAXII client software pushes the STIX content to the DHS/CISA shared infrastructure. The DHS/CISA shared infrastructure receives the STIX content, processes it, and publishes it for all entities authorized to receive it. The receiving entity's TAXII client receives STIX content and as a participant, may parse and use the content with their own tools for further analysis.

A STIX document is viewable in a web browser but is not intended for human readability. Each consumer is responsible for building and maintaining systems that parse and process, store, perform quality checks, enforce access controls, display, and track the STIX information they receive. There is expectation that use of commercial tools will facilitate this system development.

3 Brokering from Non-Federal Entities to Federal Entities

AIS enables non-Federal entities to exchange unclassified CTIs and DMs amongst each other and with Federal entities in real time. Each non-Federal entity participant agrees and signs the AIS ToU. The non-Federal entities have the option to actively participate or passively monitor the shared CTI and DM information.

3.1 Non-Federal Entity Originated Information Use Case

Non-Federal entity A creates a machine-readable document containing CTIs that they want to share with Federal entities and non-Federal entities via AIS. Figure 2 shows the flow of the CTIs submitted by the non-Federal entity to DHS/CISA, the brokering that is performed, and the flow of the indicator back out to the two trust communities.

[7] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

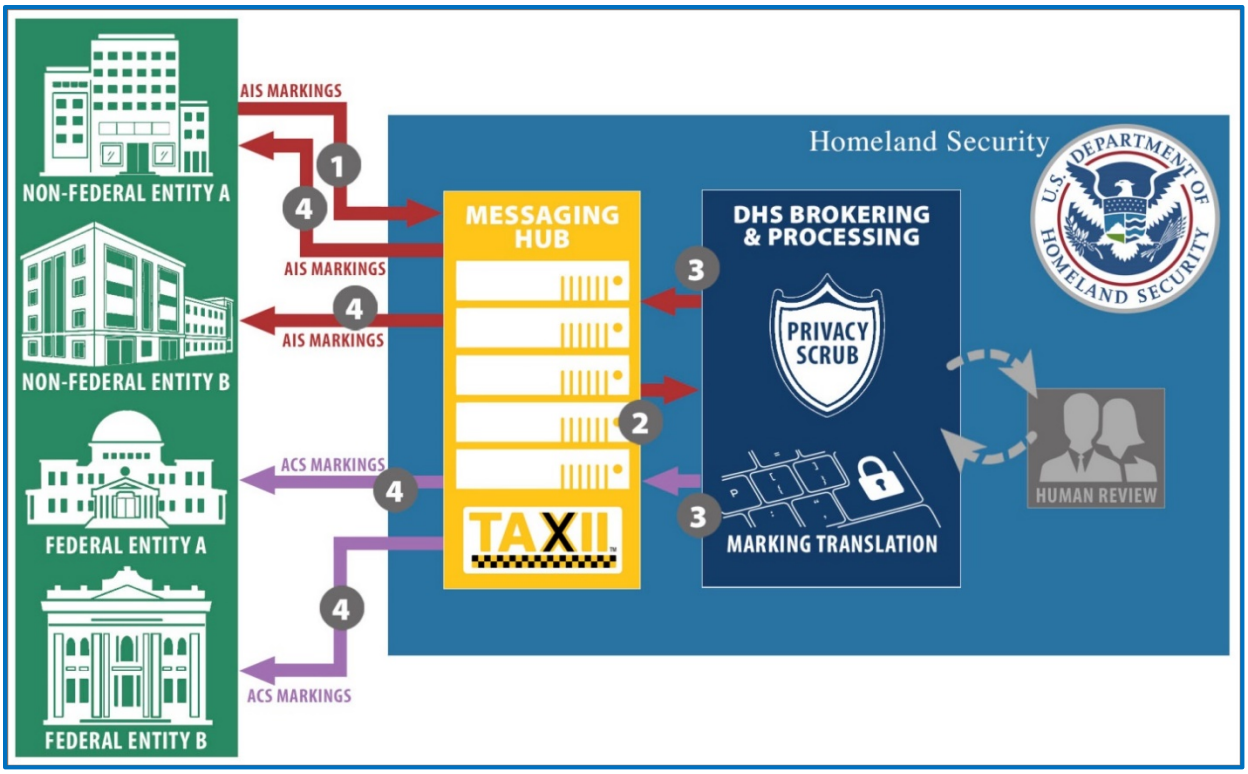

Figure 2: Non-Federal Entity Originated Indicator Sharing

1. Non-Federal Entity A publishes a machine-readable document containing CTIs to DHS/CISA-hosted messaging hub.
2. DHS/CISA receives the CTIs from the hub and automatically processes it (technical and privacy mitigations applied). Note: human review may be required in some instances.
3. DHS/CISA creates two new messages (one for the non-Federal entities subscribed to AIS and the other to the Federal entities) and publishes them to the messaging hub.
4. The CTIs are disseminated to subscribed, non-Federal entities and to Federal entities.

See *Appendix C* for examples.

3.2 Non-Federal Entity Markings

All non-Federal entity-originated STIX submissions are sent via the DHS/CISA-hosted TAXII server with information concerning three aspects of data marking:

- **TLP**[8]: Traffic Light Protocol (TLP) employs four colors, White, Green, Amber, and Red[9] to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). This is a mandatory STIX property for non-Federal entity submitters of information to AIS that defines how information can be shared between the communities.
- **Anonymization** and **Proprietary Information ("AIS Consent"):** This is a mandatory STIX marking for non-federal entities submitting producer Identity Objects. AIS Consent labels found on any STIX Object

[8] TLP reference: https://www.us-cert.gov/tlp
[9] If a non-Federal entity applies TLP:Red to submitted content, no automated sharing with Federal Entities occurs. DHS/CISA will work with the producer to determine next steps.

other than an Identity object will be ignored.

- For **Anonymization**, producers use the created_by_ref property, in conjunction with the Identity object, to indicate if they provide consent to share their identity in association with other STIX objects and, if so, with whom. It is applied to STIX objects by creating a producer Identity object with one of the anonymizing AIS Consent labels (`ais-consent-none, ais-consent-usg,` or `ais-consent-everyone`) and then assigning that Identity object to the created_by_ref property of the STIX objects to be anonymized. See *AIS Identity Anonymization Process* for more details.[10]
- For **Proprietary Information**, producers can use this property to mark information as Proprietary per CISA 2015. The AIS Consent label `ais-consent-everyone-cisa-proprietary` indicates that the submission should be treated as proprietary per CISA 2015. It is applied to STIX objects by creating a producer Identity object with the `ais-consent-everyone-cisa-proprietary` label and then assigning that Identity object to the created_by_ref property of the STIX objects to be considered proprietary.

A non-Federal Entity receiving an AIS document from DHS/CISA is responsible for processing the TLP color in accordance with the guidelines for TLP in accordance with the AIS ToU.

3.3 DHS/CISA Non-Federal to Federal Brokering

DHS/CISA brokers non-Federal entity information to Federal entity participants. As a broker, DHS/CISA is responsible for translating the AIS markings (TLP and AIS Consent) to markings used by the Federal community (ISA ACS Markings).[11]

3.3.1 Markings Translation

The markings used by the Federal sharing community are prescribed in the ISA ACS. The ACS provides markings to allow several types of limitations to be placed on information in support of machine-to-machine information sharing:

- Access Control – constrains access within the Community
- Usage Restrictions – indicates restrictions placed on the usage of the information assuming that a person or entity is granted access within the Community
- Further Sharing Restrictions – provides an indication to an information broker of the restrictions on sharing outside of the Community (brokering to another Community)
- Formal Determinations and Caveats – allow a producer to indicate specific characteristics of the information.

In addition, the ACS provides specifications for resource accounting tags on the information including a unique identifier, a creation date and time, the producer of the information, and policy and authority related references.

The following sections describe the use of these markings to reflect the policies translated from the AIS markings submitted by non-Federal entities. Following this section are specific tables that map, based on each TLP color, between the AIS markings and the Federal ACS markings.

STIX supports granular markings, which is the ability to mark each property of an object differently. However,

[10] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[11] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

AIS will ignore any granular markings (i.e., markings on individual properties rather than objects as a whole) in submissions, and only supports data markings at the object level. Care should be taken to make sure that the specified object marking is appropriate for the content in the object.

3.3.1.1 Resource Accounting

All objects that DHS/CISA brokers from AIS participating non-Federal entities to Federal entities includes an Identifier and creation date and time in accordance with the ACS. The producer information is reflected in the Responsible Entity properties with a Custodian of USA.DHS.CISA and an Originator of NONFED.

The Authority Reference is included and uses the value urn:isa:authority:ais to indicate that DHS/CISA is providing this information under AIS authorities.

3.3.1.2 Access Restrictions

All objects that DHS/CISA brokers from AIS non-Federal entities to the Federal entities is Unclassified and marked as such with ISA ACS Markings.

When the non-Federal entity producer consents (via appropriate markings at submission) to share their identity with only Federal entities, Federal entities can only share the non-Federal entity's identity with other Federal entities. Anonymized Identity objects are created when necessary.

3.3.1.3 Usage Restrictions

The usage restrictions placed on AIS objects shared with the Federal Cybersecurity Information Sharing Community are specified in CISA 2015 (6 U.S.C. § 1504(d)(5)). The ACS attribute value used to restrict actions outlined in CISA 2015 is CISAUSES. All AIS information brokered to Federal entities by DHS/CISA includes this usage restriction.

3.3.1.4 Further Sharing Restrictions

When a Federal entity receives the identity of a submitter that has consented to sharing their identity with Federal entities only, the Federal Entity is restricted from further sharing that identity outside of the Federal Government. Therefore, the ACS data marking includes a restriction on further sharing. When a Federal entity receives the identity of a submitter that has consented to sharing their identity with both non-Federal and Federal entities, the Federal Entity may share that identity outside of the Federal Government if permitted by the TLP data markings.

3.3.1.5 Formal Determinations and Caveats

Because DHS/CISA is performing automated processing of many properties for real-time dissemination, some properties may contain personal information of a specific individual or information that identifies a specific individual that is directly related to the cybersecurity threat (e.g., threat actor email address). DHS/CISA assigns *all* information originating from the AIS Community a formal determination FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT to indicate that any identified personal information of a specific individual or information that identifies a specific individual has been determined to be directly related to a cybersecurity threat. This marking indicates that DHS/CISA has processed the information through automated or manual privacy checks and either did not identify any personal information of a specific individual or information that identifies or specific individual, or that any such information has been reviewed and determined to be directly related to a cybersecurity threat. Federal entity participants must protect the document in accordance with their internal policies and procedures based on this knowledge.

The ACS also allows a caveat of CISAPROPRIETARY to support information submitted from non-Federal entities via AIS marked as proprietary. The CISAPROPRIETARY caveat marking indicates that the recipient must observe appropriate restrictions as requested by the originator in accordance with CISA 2015. Note that CISAPROPRIETARY does not carry the same processing/handling restrictions as PROPIN. The AIS Profile and

AIS Submission Guidance only permit a non-Federal submission to be marked as proprietary if the producer Identity pointed to by the created_by_ref property contains the `ais-consent-everyone-cisa-proprietary` label.

3.3.1.6 Traffic Light Protocol Translations

The following sections outline the markings translations that DHS/CISA does when an AIS file is marked with specific TLP colors. Failure to mark submissions with a valid TLP marking object will default the submission to TLP:Green.

3.3.1.6.1 TLP:White Information

When DHS/CISA receives a submission marked TLP:White from a non-Federal entity, as per the definition, DHS/CISA creates new content and marks it with ACS markings as publicly releasable (Formal Determination (FD) as Publicly Releasable or FD:PUBREL). Federal entities are free to share that object publicly provided that any originator identity information is anonymized by DHS/CISA when appropriate based on the AIS Consent label.

The AIS Consent label also can indicate that the content is to be treated as proprietary under CISA 2015, which is only permitted when the anonymization consent is "everyone" (i.e., `ais-consent-everyone-cisa-proprietary`). Non-Federal entities are discouraged from marking content as proprietary per CISA 2015 when using TLP:White; however, this combination is not prohibited. If DHS/CISA receives an indicator marked TLP:White and `ais-consent-everyone-cisa-proprietary`, DHS/CISA translates to ACS markings as if it was received as TLP:Green.

A submission from a non-Federal entity whose non-Identity object data marking is TLP:White will be translated to an object containing ACS data markings for dissemination to Federal entities. The following policies must be expressed in the ACS data marking of the object:

- Federal Community access restriction: None
- Formal Determination: Publicly Releasable
- Usage restrictions: CISAUSES are permitted
- Further sharing: All further sharing is permitted
- Caveat: If the AIS Consent label is `ais-consent-everyone-cisa-proprietary`, the Caveat: CISAPROPRIETARY should be added to the ACS data. For all other values of the AIS Consent label, the Caveat: CISAPROPRIETARY must not be included in the ACS data marking.

Table 1 describes the ACS Marking placed on the Identity object related to the submitter of a TLP:White submission. If no label is assigned, the AIS Consent label will default to `ais-consent-none`.

Table 1: AIS Consent effect on the Identity object associated with TLP:White Submission

TLP:White	
AIS Consent	**Related Identity object data markings**
ais-consent-usg	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal

TLP:White	
AIS Consent	**Related Identity object data markings**
	Entities is denied
ais-consent-none	The identity is anonymized using a consistent random generated name
ais-consent-everyone	Federal Community Sharing restriction: None Formal Determination: Publicly Releasable Usage restrictions: CISAUSES are permitted Further sharing: All further sharing is permitted
ais-consent-everyone-cisa-proprietary[12]	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV Caveat: CISAPROPRIETARY

3.3.1.6.2 TLP:Green Information

When an AIS submission marked TLP:Green is received, DHS/CISA translates to ACS markings in accordance with Table 2. The ACS markings included in the table show that Federal entities are free to use the information within their organization but not via publicly accessible channels. In addition, an ACS marking is provided to indicate that further sharing with the following entities is permitted:

- Other Federal Entities
  (sharingScope:USA.USG, ruleEffect:permit)
- Non-Federal entities within the consuming Federal entity's sector
  (sharingScope:SECTOR, ruleEffect:permit)
- Foreign governments
  (sharingScope:FOREIGNGOV, ruleEffect:permit)

In addition, any submitter identity information must be protected in accordance with anonymization by DHS/CISA when appropriate based on the AIS Consent label.

A submission from a non-Federal entity whose non-Identity object data marking is TLP:Green will be translated to one containing ACS data markings for dissemination to Federal entities. The following policies must be expressed in the ACS data marking of the object. Differences from TLP:White are in green text.

- Federal Community access restriction: Federal Entities only

[12] TLP:White/ais-consent-everyone-cisa-proprietary is processed as TLP:Green

- Usage restrictions: CISAUSES are permitted
- Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV
- Caveat: If the AIS Consent label is `ais-consent-everyone-cisa-proprietary`, the Caveat: CISAPROPRIETARY should be added to the ACS data. For all other values of the AIS Consent label, the Caveat: CISAPROPRIETARY must not be included in the ACS data marking.

Table 2 describes the ACS Marking placed on the Identity object related to the submitter of a TLP:Green submission. If no label is assigned, the AIS Consent label will default to `ais-consent-none`.

Table 2: AIS Consent effect on the Identity object associated with TLP:Green Submission

TLP:Green	
AIS Consent	**Related Identity object data markings**
ais-consent-usg	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied
ais-consent-none	The identity is anonymized using a consistent random generated name
ais-consent-everyone	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV
ais-consent-everyone-cisa-proprietary	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV Caveat: CISAPROPRIETARY

3.3.1.6.3 TLP:Amber Information

When an AIS submission marked TLP:Amber is received, DHS/CISA translates the AIS marking and marks the document with ACS markings to indicate that Federal entities are free to use only within the Federal Government.

A submission from a non-Federal entity whose non-Identity object data marking is TLP:Amber will be translated to one containing ACS data markings for dissemination to Federal entities. The following policies must be expressed in the ACS data marking of the cyber information. Differences from TLP:Amber are in amber text.

Federal Community access restriction: Federal Entities only

Usage restrictions: CISAUSES are permitted

Further sharing: Further sharing outside Federal Entities is denied

Caveat: If the AIS Consent label is `ais-consent-everyone-cisa-proprietary`, the Caveat: CISAPROPRIETARY should be added to the ACS data. For all other values of the AIS Consent label, the Caveat: CISAPROPRIETARY must not be included in the ACS data marking.

Table 3 describes the ACS Marking placed on the Identity object related to the submitter of a TLP:Amber submission. If no label is assigned, the AIS Consent label will default to `ais-consent-none`.

Table 3: AIS Consent effect on the Identity object associated with TLP:Amber Submission

TLP:Amber	
AIS Consent	**Related Identity object data markings**
ais-consent-usg	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied
ais-consent-none	The identity is anonymized using a consistent random generated name
ais-consent-everyone	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied
ais-consent-everyone-cisa-proprietary	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied Caveat: CISAPROPRIETARY

3.3.1.6.4 TLP Red Information

TLP:Red is restricted such that the recipient may not share TLP:Red information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed. Non-Federal entities are directed not to use AIS for TLP:Red information. If DHS/CISA receives a TLP:Red content, DHS/CISA will notify the originator and determine next steps. The content is not automatically disseminated to the AIS Community or Federal Entities.

3.3.2 Describing ACS Marking Properties

Each property of an ACS marking is described in the following subsections.

3.3.2.1 Identifier

DHS/CISA will include a unique identifier for the STIX document in ACS format[13]. For example:

```
"identifier": "isa:guide.19001.0080f787-10ea-5084-ac16-b76d4147f8b3",
```

3.3.2.2 CreateDateTime

DHS/CISA will provide the creation date and time associated with the creation of the document associated with the unique identifier. For example:

```
"create_date_time": "2020-05-12T12:52:40Z",
```

3.3.2.3 ResponsibleEntities

DHS/CISA will provide a single mandatory Custodian (CUST:) token with a suffix value of USA.DHS.CISA. Additionally, DHS/CISA will provide a single Originator (ORIG:) token of suffix value NONFED. For example:

```
"responsible_entity_custodian": "USA.DHS.CISA",
"responsible_entity_originator": "NONFED"
```

3.3.2.4 Policies (PolicyRef)

DHS/CISA will provide one PolicyRef per the ACS[14]. The query components of the PolicyRef set the default for Usage and FurtherSharing restrictions and are either set to permit or deny dependent upon the marking assigned by the originator. Additional information of the rules that DHS/CISA uses to broker between the originator markings and the ACS markings is found in this document.

For example:

```
urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny
```

or

```
urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit
```

3.3.2.5 Authorities (AuthRef)

DHS/CISA will provide one reference to the authority with a value of urn:isa:authority:ais to indicate that the resource has been processed through AIS. For example:

```
"authority_reference": "urn:isa:authority:ais
```

3.3.2.6 Usage Restrictions (AccessPrivilege)

The usage restrictions placed on AIS objects shared with the Federal Cybersecurity Information Sharing Community are specified in CISA 2015 (6 U.S.C. § 1604(d)(5)). All AIS information brokered to Federal entities by DHS/CISA includes this usage restriction. The privdefault set in the PolicyRef will be deny[15] and the only expected values are:

```
"access_privilege": [
   {
       "privilege_action": "CISAUSES",
```

[13] ISA ACS Version 3.0a Section 2.1.1
[14] ISA ACS Version 3.0a Section 2.2.1
[15] ISA ACS Version 3.0a Section 2.2.2

```
        "privilege_scope": {
            "entity": ["ALL"],
            "permitted_nationalities": ["ALL"],
            "permitted_organizations": ["ALL"],
            "shareability": ["ALL"]
        },
        "rule_effect": "permit"
    }
 ]
```

3.3.2.7 Further Sharing Restrictions (FurtherSharing)

When a Federal entity receives the identity of a non-Federal submitter that has consented to their identity being shared with Federal entities only, the Federal Entity is restricted from further sharing that identity outside of the Federal Government. When a Federal entity receives the identity of a submitter that has consented to sharing their identity with both non-Federal and Federal entities, the Federal Entity may share that identity outside of the Federal Government if permitted by the TLP data markings.

When the sharedefault set to deny in the PolicyRef[16], the ACS restriction on further sharing can be used to allow for restricted sharing. For instance, a TLP:Green submission allows for the following sharing:

```
"further_sharing": [
   {
       "sharing_scope": [
          "USA.USG"
       ],
       "rule_effect": "permit"
   },
   {
       "sharing_scope": [
          "FOREIGNGOV"
       ],
       "rule_effect": "permit"
   },
   {
       "sharing_scope": [
          "SECTOR"
       ],
       "rule_effect": "permit"
    }
 ]
```

3.3.2.8 Access Restrictions (Control Set)

DHS/CISA will apply a specific set of allowable values for the control set when the information has originated from AIS. For example:

```
"control_set": {
   "classification": "U",
   "formal_determination": [
       "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
   ],
   "caveat": [
       "CISAPROPRIETARY"
   ]
}
```

[16] ISA ACS Version 3.0a Section 2.2.2.2

Another possible set of Control Set values (for TLP:White) are:

```
"control_set": {
   "classification": "U",
   "formal_determination": [
       "PUBREL",
       "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
   ],
   "caveat": [
       "CISAPROPRIETARY"
   ]
}
```

STIX objects marked with a formal determination of PUBREL will also include the public_release property that includes the release authority and date.

The CISAPROPRIETARY caveat is optionally present. In addition, the FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT will be present.

4 Brokering from Federal Entities to Non-Federal Entities

4.1 Federal Entity Originated Information Use Case

Federal Entity A creates a machine-readable submission containing CTIs that they want to share with non-Federal entities via AIS and with the rest of the Federal entities. Figure 3 shows the flow of the submission by the Federal entity to DHS/CISA, the brokering that is performed, and the flow of the CTIs back out to the two trust communities.

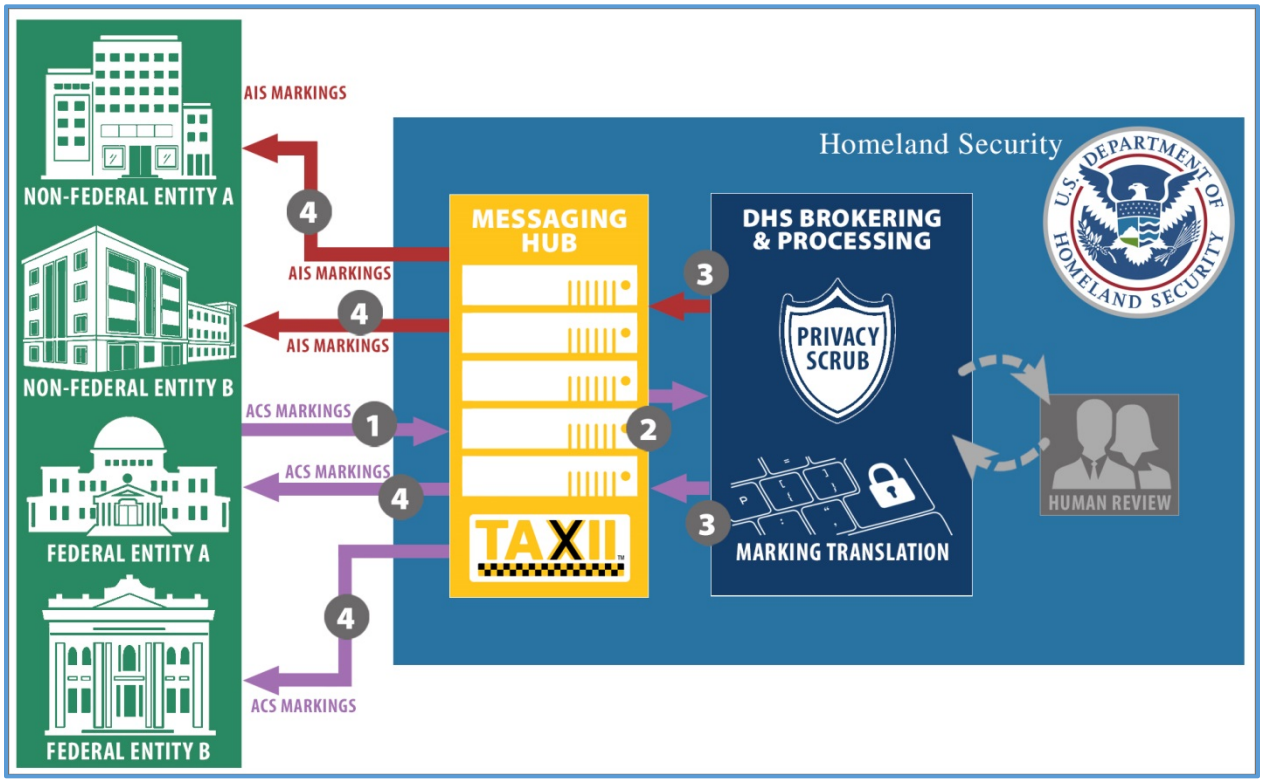

Figure 3: Federal Entity Originated Indicator Sharing through AIS Processing

1. Federal Entity A publishes indicator (with ACS) to the DHS/CISA-hosted messaging hub.
2. DHS/CISA receives the indicator from the hub and the DHS/CISA-hosted brokering capability immediately and automatically processes the information, anonymizes the results as appropriate, and appropriately marks the indicators (technical and privacy mitigations applied).
3. DHS/CISA creates two new messages and publishes them to the messaging hub.
4. The CTIs are disseminated to Federal Entities (with ACS) and non-Federal entities (with TLP).

See *Appendix D* for examples.

4.2 DHS/CISA Federal Entity to non-Federal Entity Brokering

DHS/CISA brokers Federal entity-originated information sent to the DHS/CISA-hosted TAXII server intended for dissemination via AIS to non-Federal entities. In addition, DHS/CISA publishes these CTIs and DMs to all of the Federal entity community. Federal submissions specifically marked for further sharing to the AIS community are also brokered by DHS/CISA to the Federal entities after undergoing AIS processing similar to submissions shared with the non-Federal community (i.e., translating from ACS to TLP markings). Submissions shared with the Federal entities are be marked with ACS markings.

4.2.1 STIX Translation

Federal entities **must** submit information in accordance with the AIS Profile and AIS Submission Guide and marked with ACS markings as described below.

Federal entity-originated information is published by DHS/CISA to the non-Federal entities as either completely releasable with no usage constraints (TLP:White) or released to and used by the AIS Community only (TLP:Amber) with no further sharing allowed. The ambiguity associated with TLP:Green is not useful for Federal entity-originated information, and cannot be generated via brokering.

4.2.1.1 Markings Translations

As a broker, DHS/CISA translates the ACS markings to TLP Markings required for non-Federal entity sharing. Specifically:

- DHS/CISA translates ACS Markings to TLP:White or Amber based on the ACS Marking of the Federal entity-originated STIX submission. DHS/CISA identifies information for dissemination to AIS from a Federal entity by one of the following ControlSet markings.
    - When DHS/CISA receives STIX content from a Federal Entity with a marking containing the formal determination (abbreviated as FD where needed) of PUBREL, DHS/CISA shares this publicly with anyone, including AIS members. This is marked TLP:White.

ACS Marking to TLP:White

Object Marking must be:

```
"control_set": {
   "classification": "U",
   "formal_determination": [
     "PUBREL"[17]
   ],
 }
```

[17] The FD may also include:
INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT

- When DHS/CISA receives STIX content from a Federal Entity with a marking containing the formal determination of AIS and a formal determination of For Offical Use Only (FOUO), DHS/CISA shares the file with members of AIS. This is not considered publicly released and is marked TLP:Amber.

ACS Marking to TLP:Amber

Object Marking must be:

```
"control_set": {
   "classification": "U",
   "formal_determination": [
     "FOUO",
     "AIS"[18]
   ],
 }
```

- If neither FD=PUBREL or (FD=AIS and FD=FOUO) is specified (including when only AIS or only FOUO is specified with or without PUBREL), the submission will not be brokered to non-Federal entities. It will only be shared with Federal entities.
- If the object marking contains either FD=PUBREL or (FD=AIS and FD=FOUO), this is an indication, by the Federal entity originator, that DHS/CISA may release the information to the non-Federal entities.
- If the object marking contains FD=PUBREL and (FD=AIS and FD=FOUO), the more restrictive marking (FOUO) will take precedence and it will be shared accordingly.
- DHS/CISA ignores any granular markings (i.e., markings on individual properties) contained in a STIX object.

4.2.2 Personal Information

Federal entities must ensure that no personal information of a specific individual or information that identifies a specific individual unless directly related to a cybersecurity threat is present in any information destined for the non-Federal entity Sharing Community. Federal entities may **optionally** make a formal determination that the submitted information is directly related to the cybersecurity threat and apply the following marking as defined in the ACS:

FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT

DHS/CISA applies Privacy Scrubbing algorithms to all Federal entity-originated STIX content (as is done with non-Federal entities). Free text fields identified by automated processing as containing potential PII are sent for human analyst review prior to non-Federal dissemination.

The use of the following formal determinations on information submitted for dissemination to non-Federal Entities is not permitted:

- FD:PII-NECESSARY-TO-UNDERSTAND-THREAT
- FD:NO-PII-PRESENT
- FD:PII-NOT-PRESENT.

[18] The FD may also include:
INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT

4.2.3 Federal Entity Originated Information Data Stewardship

To ensure that sensitive information is removed, DHS/CISA removes and replaces STIX identifiers (ID) for all information to be shared via AIS prior to dissemination. Note that DHS/CISA does not update relationship identifiers where the new STIX document refers to a DHS/CISA-defined STIX ID from a previously shared STIX document. When Federal entities share STIX documents that revise or revoke or refer to previously shared STIX documents, the Federal entities must use the IDs that they used in their original submissions. To ensure data integrity, DHS/CISA maintains traceability between those IDs and the DHS/CISA-assigned IDs and appropriately substitute IDs before dissemination to non-Federal entities.

Note that the originator of a Federal submission could be NONFED if the federal agency received the content from a non-Federal source, outside of the AIS sharing context.

4.2.4 Describing ACS Marking Properties

Each property of an ACS marking is described in the following subsections.

4.2.4.1 Identifier

Federal entities must provide a single unique identifier in the ACS specified format[19] as shown in the example. This identifier is associated with the entire STIX document. For example:

```
"identifier": "isa:guide.19001.EDH2-0080f787-10ea-5084-ac16-b76d4147f8a6"
```

4.2.4.2 CreateDateTime

Federal entities must provide the creation date and time associated with the creation of the unique identifier. For example:

```
"create_date_time": "2020-05-12T12:52:40Z"
```

4.2.4.3 ResponsibleEntities

Federal entities must provide a single mandatory Custodian (CUST) token using the values to indicate the organization that created the document. Optionally, a single Originator (ORIG) token may be included with the values for the suffix from the same appendix, to indicate the Originator of the document. For example:

```
"responsible_entity_custodian": "USA.DOD"
    "responsible_entity_originator": "NONFED"
```

Values for CUST and ORIG are discussed in *Appendix F*.

4.2.4.4 Policies (PolicyRef)

There will be at most one Policy Reference that indicates that the submission is in accordance with the ACS. The query components of the PolicyRef set the default for Usage and Further Sharing restrictions and are either set to permit or deny depending upon whether Usage or Further Sharing restrictions are required by the Federal entity. Setting the default values to deny requires the inclusion of an AccessPrivilege or FurtherSharing attribute to indicate exceptions to how the resource may be used and shared. Additional information on the use of these markings is available in the ACS[20]. The following are the permitted values showing the use of this property. Permitted values for AIS:

- `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`

[19] ISA ACS Version 3.0a Section 2.1.1
[20] ISA ACS Version 3.0a Section 2.2.2

- `urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny`

4.2.4.5 Authorities (AuthRef)

At least one reference to an authority must be provided within the ACS markings but if multiple authorities are referenced, they are provided as space delimited URNs. Federal entities must provide a reference to the authority under which they share the resource such as urn:isa:authority:misa. DHS/CISA will use the value urn:isa:authority:ais to indicate that the resource has been processed through AIS. Therefore, Federal entities will not use urn:isa:authority:ais. For example:

```
"authority_reference": "urn:isa:authority:misa"
```

4.2.4.6 Usage Restrictions (AccessPrivilege)

The AccessPrivilege property allows restrictions on the actions that are permitted by the consumer following an access decision.[21] The default for all access privileges is set with the query component of the PolicyRef.

For example, if privdefault=deny in the PolicyRef, a specific privilege_action of CISAUSES must be provided.

```
"access_privilege": [
    {
       "privilege_action": "CISAUSES",
       "privilege_scope": {
          "entity": ["ALL"],
          "permitted_nationalities": ["ALL"],
          "permitted_organizations": ["ALL"],
          "shareability": ["ALL"]
       },
       "rule_effect": "permit"
    }
]
```

Another privilege_action to be used when privdefault=deny in the PolicyRef is IDSRC, which is related to anonymization. Anonymization is discussed in Section 5.

```
{
    "privilege_action": "IDSRC",
    "privilege_scope": {
       "entity": ["ALL"],
       "permitted_nationalities": ["ALL"],
       "permitted_organizations": ["ALL"],
       "shareability": ["ALL"]
    },
    "rule_effect": "permit"
}
```

4.2.4.7 Further Sharing Restrictions (FurtherSharing)

The FurtherSharing attribute allows restriction on the further sharing that is permitted following an access decision.[22] From the above example, if the sharedefault=deny in the Policy Reference, the following is expected by AIS:

```
"further_sharing": [
 {
     "sharing_scope": [
         "USA.USG"
```

[21] ISA ACS Version 3.0a Section 2.2.2.1
[22] ISA ACS Version 3.0a Section 2.2.2.2

```
            ],
            "rule_effect": "permit"
        }
    ]
```

4.2.4.8 Access Restrictions (Control Set)

The Control Set provides the group of space-delimited key value pair tokens that are used to inform automated access control decisions within the Federal sharing community. A specific set of allowable token values is expected by DHS/CISA to further share via AIS. The submitted Control Set values allow DHS/CISA to determine how to translate ACS markings to TLP markings as detailed above.

The following are the possible set of ControlSet values (for TLP:Amber):

```
"control_set": {
    "classification": "U",
    "formal_determination": [
       "FOUO",
       "AIS"
    ]
 }
```

or (for TLP:White)

```
"control_set": {
    "classification": "U",
    "formal_determination": [
        "PUBREL"
    ]
}
```

5 Anonymization (AIS consent)

The AIS Anonymization policy is explained in the *AIS Identity Anonymization Process*.

This section discusses the implications of that policy using examples. DHS/CISA is responsible for determining when anonymization should take place and managing the correspondence between submitted identities and anonymized identities.

5.1 Non-Federal Submissions

The sharing of the identity of a non-federal content creator can be restricted by the submitter using the AIS Consent label, as described in section 3. The following table indicates if the anonymization of the identity is required for non-federal submissions.

Table 4: Anonymization with Non-Federal Submissions

AIS: Consent	Anonymization Outcome
not present	The identity is anonymized using a consistent random generated name.
ais-consent-none	The identity is anonymized using a consistent random generated name.

AIS: Consent	Anonymization Outcome
ais-consent-usg	Non-Federal AIS Sharing: The identity is anonymized using a consistent random generated name. USG Sharing: The identity is shared un-anonymized.
ais-consent-everyone	The identity is shared un-anonymized.
ais-consent-everyone-cisa-proprietary	The identity is shared un-anonymized.

When an identity needs to be anonymized, a new Identity object is created, with a randomly generated name, and a new STIX ID. If the sectors property is present in the original Identity object, it will be carried over into the anonymized Identity object. Because all other STIX objects associated with this producer contain the un-anonymized Identity object's ID in its created_by_ref property, all such objects must be duplicated, replacing the created_by_ref property with the anonymized Identity's object ID.

The created_by_ref property is recommended but is not required. If an object is received and it does not have a created_by_ref property, it is considered anonymized and sent out to participants according to its data markings.

Additionally, the created_by_ref property could be present, yet the related Identity object may not be. In this case, a new STIX ID corresponding to an anonymized Identity object is created by CISA and the submission is re-created with the created_by_ref property containing the new anonymized ID.

5.2 Federal Submissions

The identity of a federal content creator can also be anonymized for sharing with non-federal entities, based on the use of AIS Consent label and the value of the access_privilege action of IDSRC. The following table shows the anonymization outcome for federal submissions to the non-federal feed. All rows assume a policy_reference privdefault must be specified[23].

Table 5: Anonymization with Federal Submissions

AIS Consent	Privdefault=permit or ACS: IDSRC	Anonymization Outcome
not present or ais-consent-none or ais-consent-usg	permit or deny	The identity is anonymized to "USG".
ais-consent-everyone or ais-consent-everyone-cisa-proprietary	permit	The identity is shared un-anonymized.
ais-consent-everyone or ais-consent-everyone-cisa-proprietary	deny	The identity is anonymized using a consistent random generated name.

Note that there is a unique Identity object for the USG identity, and unique Identity objects for each individually anonymized federal agency. Additionally, an AIS Consent of `ais-consent-everyone-cisa-proprietary` is

[23] ISA ACS Version 3.0a Section 2.2.1

not valid for Federal submissions but will be accepted and processed as `ais-consent-everyone`.

For examples of anonymization, see *Appendices D and E*.

6 Appendix A: Acronyms

Acronym	Definition
ACS	Access Control Specification
AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
CISA 2015	Cybersecurity Information Sharing Act of 2015
CTI	Cybersecurity Threat Indicator
CUST	Custodian
DHS	Department of Homeland Security
DM	Defensive Measure
DOD	Department of Defense
FD	Formal Determination
FOREIGNGOV	Foreign Government
FOUO	For Official Use Only
ID	Identifiers
ISA	Information Sharing Architecture
MISA	Multi-lateral Information Sharing Agreement
ORIG	Originator
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PUBREL	Publicly Releasable
SCP	Shared Capability Provider
SECTOR	Sector
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic Light Protocol
ToU	Terms of Use
USG	United States Government

7 Appendix B: Definitions

Term	Definition
Federal Entity	Department or agency of the United States or any component of such department or agency.
Non-Federal Entity	Any private entity, non-Federal government agency or department, or State, tribal or local government (including a political subdivision, department or component thereof), including a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States
Shared Infrastructure	Hosted, shared Infrastructure available within a Trust Community for members to exchange information with each other according to the Trust Model for that particular Community. The Infrastructure may include services for member enrollment and authentication, information enrichment and consolidation, anonymity, logging (if required). The Infrastructure may include message hubs such as a TAXII server and on-line collaboration tools. The host of the shared infrastructure may have some unique role with the Community or the host may simply be a Member who has volunteered to provide the capabilities.
Trust Community	A group of entities that agree to work together under the auspices of a common Trust Model. Communities and membership may be transitory or permanent. Entities can join more than one Community and their interactions with each community are per the Trust Model for each.

8 Appendix C: Non-Federal Submissions to Federal/Non-Federal Feeds Examples

This Appendix contains six examples for Non-Federal submissions. Properties that are significant to the examples are in red. Table 6 shows all the possible combinations of AIS data markings that can be found in Non-Federal submissions, but the examples selected for this Appendix were chosen based on the most likely expected submissions.

All ACS marking output to the Federal feed contains:

```
INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
```

The same UUID is used for the ACS marking-definition id as in the identifier property, but this is not required.

These examples assume the existence of the following Extension Definition object.

```
{
    "id": "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce",
    "type": "extension-definition",
    "spec_version": "2.1",
    "name": "isa-ais-3-0",
    "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"]
}
```

Table 6: Possible Combinations of AIS Data Markings

	Non-Fed Submission Marking Input		Published Marking/Anonymization Output				
	AIS: Consent	**TLP**	**PUBREL**	**sharedefault (Further Sharing)**	**CAVEAT: CISAPROPRIETARY**	**Anonymization**	**Example**
1	**N/A** **(default to ais-consent-none)**	White	X	permit	N/A	The identity is anonymized using a consistent random generated name.	**C.1**
2	**N/A** **(default to ais-consent-none)**	Green		deny (FOREIGNGOV, SECTOR, USG)	N/A	The identity is anonymized using a consistent random generated name.	
3	**N/A** **(default to ais-consent-none)**	Amber		deny (USG)	N/A	The identity is anonymized using a consistent random generated name.	

	Non-Fed Submission Marking Input		Published Marking/Anonymization Output				
	AIS: Consent	TLP	PUBREL	sharedefault (Further Sharing)	CAVEAT: CISAPROPRIETARY	Anonymization	Example
4	ais-consent-none	White	X	permit	N/A	The identity is anonymized using a consistent random generated name.	
5	ais-consent-none	Green		deny (FOREIGNGOV, SECTOR, USG)	N/A	The identity is anonymized using a consistent random generated name.	C.2
6	ais-consent-none	Amber		deny (USG)	N/A	The identity is anonymized using a consistent random generated name.	C.3
7	ais-consent-usg	White	X	permit	N/A	**AIS Sharing**: The identity is anonymized using a consistent random generated name. **USG Sharing**: The identity is shared un-anonymized.	
8	ais-consent-usg	Green		deny (FOREIGNGOV, SECTOR, USG)	N/A	**AIS Sharing**: The identity is anonymized using a consistent random generated name. **USG Sharing**: The identity is shared un-anonymized.	C.4
9	ais-consent-usg	Amber		deny (USG)	N/A	**AIS Sharing**: The identity is anonymized using a consistent random generated name. **USG Sharing**: The identity is shared un-anonymized.	
10	ais-consent-everyone	White	X	permit	N/A	The identity is shared un-anonymized.	C.5

	Non-Fed Submission Marking Input		Published Marking/Anonymization Output				
	AIS: Consent	TLP	PUBREL	sharedefault (Further Sharing)	CAVEAT: CISAPROPRIETARY	Anonymization	Example
11	ais-consent-everyone	Green		deny (FOREIGNGOV, SECTOR, USG)	N/A	The identity is shared un-anonymized.	
12	ais-consent-everyone	Amber		deny (USG)	N/A	The identity is shared un-anonymized.	
13	ais-consent-everyone-cisa-proprietary	White[24]		deny (FOREIGNGOV, SECTOR, USG)	X	The identity is shared un-anonymized.	
14	ais-consent-everyone-cisa-proprietary	Green		deny (FOREIGNGOV, SECTOR, USG)	X	The identity is shared un-anonymized.	
15	ais-consent-everyone-cisa-proprietary	Amber		deny (USG)	X	The identity is shared un-anonymized.	C.6

[24] TLP:White/ais-consent-everyone-cisa-proprietary is processed as TLP:Green

8.1 Example C.1: No AIS Consent, TLP:White (Row 1)

Non-Federal AIS Submission

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--e5f1b90a-d9b6-40ab-81a9-8a29df4b6b65",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--e5f1b90a-d9b6-40ab-81a9-8a29df4b6b65",  -- self-referential
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"      -- TLP:White
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Federal AIS Brokered Output

FD: PUBREL, INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
Access Privilege: CISAUSES,
sharedefault: permit,
Identity: anonymize (random)

No AIS Consent defaults to ais-consent-none

```
{
   "created": "2021-03-18T20:03:00.000Z",
   "modified": "2021-03-18T20:03:00.000Z",
   "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
         "access_privilege": [
            {
               "privilege_action": "CISAUSES",
               "privilege_scope": {
                      "entity": ["ALL"],
                      "permitted_nationalities": ["ALL"],
                      "permitted_organizations": ["ALL"],
                      "shareability": ["ALL"]
               },
               "rule_effect": "permit"
               }
         ],
         "control_set": {
            "classification": "U",
            "formal_determination": [
               "PUBREL",
               "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
            ]
         },
         "create_date_time": "2021-03-18T20:03:00.000Z",
```

```
            "extension_type": "property-extension",

            "identifier": "isa:guide.19001.ACS3-f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3",
            "name": "Example C.1",
            "authority_reference": ["urn:isa:authority:ais"],
            "public_release": {
                "released_by": "NONFED"
                "released_on": "2021-03-18T20:03:00.000Z"
            },
            "policy_reference":
                "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",
            "responsible_entity_custodian": "USA.DHS.CISA",
            "responsible_entity_originator": "NONFED",
        }
    },
    "id": "marking-definition--f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3",
    "type": "marking-definition",
    "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--496b17c2-1b5e-4ec0-b0d3-46ab7334ac5f",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-none"
  ],
  "name": "RunningTableChair",
  "object_marking_refs": [
      "marking-definition--f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3"
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

Identity: anonymize (random)

No AIS Consent processed as ais-consent-none

No need for ACS Marking

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--4211a70c-d4c7-4638-af45-4fb41a0acf21",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-none"
  ],
  "name": "RunningTableChair",
  "object_marking_refs": [
```

```
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"      -- TLP:White
    ],
    "sectors": [
      "technology"
    ],
    "identity_class": "organization"
}
```

8.2 Example C.2. ais-consent-none, TLP:Green (Row 5)

Non-Federal AIS Submission

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--0d775c0f-ecdf-41c8-b25f-ce80713e1365",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--0d775c0f-ecdf-41c8-b25f-ce80713e1365",  -- self-referential
  "labels": [
      "ais-consent-none"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"      - TLP:Green
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Federal AIS Brokered Output

FD: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
Access Privilege: CISAUSES,
Further Sharing: FOREIGNGOV, SECTOR, USA.USG
sharedefault: deny,
Identity: anonymize (random)

```
{
   "created": "2021-03-18T20:03:00.000Z",
   "modified": "2021-03-18T20:03:00.000Z",
   "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
      "access_privilege": [
          {
            "privilege_action": "CISAUSES",
            "privilege_scope": {
               "entity": ["ALL"],
               "permitted_nationalities": ["ALL"],
               "permitted_organizations": ["ALL"],
               "shareability": ["ALL"]
            },
            "rule_effect": "permit"
          }
       ],
      "further_sharing": [
          {
             "sharing_scope": [
```

```
                "FOREIGNGOV"
            ],
            "rule_effect": "permit"
        },
        {
            "sharing_scope": [
                "SECTOR"
            ],
            "rule_effect": "permit"
        },
        {
            "sharing_scope": [
                "USA.USG"
            ],
            "rule_effect": "permit"
        }
    ],
    "control_set": {
        "classification": "U",
        "formal_determination": [
                    "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
        ]
    },
    "create_date_time": "2021-03-18T20:03:00.000Z",
    "extension_type": "property-extension",
    "identifier": "isa:guide.19001.ACS3-85f8047c-ba3d-4f44-a845-061a71819066",
    "name": "Example C.2",
    "authority_reference": ["urn:isa:authority:ais"],
    "policy_reference":
        "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",
    "responsible_entity_custodian": "USA.DHS.CISA",
    "responsible_entity_originator": "NONFED"
    }
  },
  "id": "marking-definition--85f8047c-ba3d-4f44-a845-061a71819066",
  "type": "marking-definition",
  "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--3d90cf54-196d-4d7d-a09e-63a44f87f160",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-none"
  ],
  "name": "RunningTableChair",
  "object_marking_refs": [
      "marking-definition--85f8047c-ba3d-4f44-a845-061a71819066"
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

Identity: anonymize (random)

No need for ACS Marking

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--4b9872db-f6d1-4f9e-908b-efe9513d0632",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-none"
  ],
  "name": "RunningTableChair",
  "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"      -- TLP:Green
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

8.3 Example C.3. ais-consent-none, TLP:Amber (Row 6)

Non-Federal AIS Submission

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--0217bd86-8561-40bd-8176-797cc175f06c",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--0217bd86-8561-40bd-8176-797cc175f06c",  - self-referential
  "labels": [
      "ais-consent-none"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"     -- TLP:Amber
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Federal AIS Brokered Output

FD: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
Access Privilege: CISAUSES,
Further Sharing: USA.USG
sharedefault: deny,
Identity: anonymize (random)

```
{
   "created": "2021-03-18T20:03:00.000Z",
   "modified": "2021-03-18T10:31:00.000Z",
   "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
      "access_privilege": [
          {
            "privilege_action": "CISAUSES",
            "privilege_scope": {
               "entity": ["ALL"],
               "permitted_nationalities": ["ALL"],
               "permitted_organizations": ["ALL"],
               "shareability": ["ALL"]
            },
            "rule_effect": "permit"
          }
       ],
      "further_sharing": [
          {
             "sharing_scope": [
                 "USA.USG"
```

```
            ],
            "rule_effect": "permit"
        }
    ],
    "control_set": {
        "classification": "U",
        "formal_determination": [
               "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
        ]
    },
    "create_date_time": "2021-03-18T20:03:00.000Z",
    "extension_type": "property-extension",
    "identifier": "isa:guide.19001.ACS3-f5c4e341-b384-46d3-b6d4-990faaa8bbe5",
    "name": "Example C.3",
    "authority_reference": ["urn:isa:authority:ais"],
    "policy_reference":
        "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",
    "responsible_entity_custodian": "USA.DHS.CISA",
    "responsible_entity_originator": "NONFED"
    }
  },
  "id": "marking-definition--f5c4e341-b384-46d3-b6d4-990faaa8bbe5",
  "type": "marking-definition",
  "spec_version": "2.1"
}
```

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--23a3f071-da8d-4c1a-b9a2-5b528499b6c1",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-none"
  ],
  "name": "RunningTableChair",
  "object_marking_refs": [
      "marking-definition--f5c4e341-b384-46d3-b6d4-990faaa8bbe5"
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

Identity: anonymize (random)
No need for ACS Marking

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--8053edae-92b5-4c96-8545-367cf777d380",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
```

```
        "ais-consent-none"
    ],
    "name": "RunningTableChair",
    "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"     -- TLP:Amber
    ],
    "sectors": [
      "technology"
    ],
    "identity_class": "organization"
}
```

8.4 Example C.4. ais-consent-usg, TLP:Green (Row 8)

Non-Federal AIS Submission

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--6b3f46e8-8a6b-428f-8d19-fc7d6f34f47d",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--6b3f46e8-8a6b-428f-8d19-fc7d6f34f47d",  -- self-referential
  "labels": [
      "ais-consent-usg"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"      -- TLP:Green
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Federal AIS Brokered Output

FD: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
Access Privilege: CISAUSES,
Further Sharing: FOREIGNGOV, SECTOR, USA.USG
sharedefault: deny,
Identity: un-anonymized

```
{
   "created": "2021-03-18T20:03:00.000Z",
   "modified": "2021-03-18T10:31:00.000Z",
   "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
              "access_privilege": [
          {
            "privilege_action": "CISAUSES",
            "privilege_scope": {
               "entity": ["ALL"],
               "permitted_nationalities": ["ALL"],
               "permitted_organizations": ["ALL"],
               "shareability": ["ALL"]
            },
            "rule_effect": "permit"
          }
       ],
      "further_sharing": [
          {
             "sharing_scope": [
                 "FOREIGNGOV"
```

```
            ],
            "rule_effect": "permit"
        },
        {
            "sharing_scope": [
                "SECTOR"
            ],
            "rule_effect": "permit"
        },
        {
            "sharing_scope": [
                "USA.USG"
            ],
            "rule_effect": "permit"
        }
    ],
    "control_set": {
        "classification": "U",
        "formal_determination": [
              "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
        ],
    },
    "create_date_time": "2021-03-18T20:03:00.000Z",
    "extension_type": "property-extension",
    "identifier": "isa:guide.19001.ACS3-64f92049-88a0-4fd5-8bc9-b3fc962f466a",
    "name": "Example C.4",
    "authority_reference": ["urn:isa:authority:ais"],
    "policy_reference":
        "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",
    "responsible_entity_custodian": "USA.DHS.CISA",
    "responsible_entity_originator": "NONFED"
    }
  },
  "id": "marking-definition--64f92049-88a0-4fd5-8bc9-b3fc962f466a",
  "type": "marking-definition",
  "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--eb98c427-7a64-405b-851f-33c95d22af99",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-usg"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--64f92049-88a0-4fd5-8bc9-b3fc962f466a"
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

Identity: anonymize (random)
No need for ACS Marking

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--89a00372-ce5f-48fe-8b5b-37032d3e2daa",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-usg"
  ],
  "name": "RunningTableChair",
  "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"      - TLP:Green
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

8.5 Example C.5. ais-consent-everyone, TLP:White (Row 10)

Non-Federal AIS Submission

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--985ed55e-30c4-4bd8-ac4a-a470cc0578fb",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--985ed55e-30c4-4bd8-ac4a-a470cc0578fb",  -- self-referential
  "labels": [
      "ais-consent-everyone"
  ],
  "sectors": [
    "technology"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"      -- TLP:White
  ],
  "identity_class": "organization"
}
```

Federal AIS Brokered Output

FD: PUBREL, INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
Access Privilege: CISAUSES,
sharedefault: permit,
Identity: un-anonymized

```
{
   "created": "2021-03-18T20:03:00.000Z",
   "modified": "2021-03-18T20:03:00.000Z",
   "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
       "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
              "access_privilege": [
         {
           "privilege_action": "CISAUSES",
           "privilege_scope": {
              "entity": ["ALL"],
              "permitted_nationalities": ["ALL"],
              "permitted_organizations": ["ALL"],
              "shareability": ["ALL"]
           },
           "rule_effect": "permit"
         }
       ],
       "control_set": {
           "classification": "U",
           "formal_determination": [
              "PUBREL",
```

```
                "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
            ]
        },
        "create_date_time": "2021-03-18T20:03:00.000Z",
        "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3-4ee59215-154f-48a2-8da2-5e288824792b",
        "name": "Example C.5",
        "authority_reference": ["urn:isa:authority:ais"],
        "public_release": {
           "released_by": "NONFED",
           "released_on": "2021-03-18T20:03:00.000Z"

        }
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",
        "responsible_entity_custodian": "USA.DHS.CISA",
        "responsible_entity_originator": "NONFED"
        }
   },
   "id": "marking-definition--4ee59215-154f-48a2-8da2-5e288824792b",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--e5442cd7-c11a-4453-ab9e-b49f3ef6dee1",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-everyone"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--4ee59215-154f-48a2-8da2-5e288824792b"
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```


Non-Federal AIS Brokered Output

Identity: un-anonymized
No need for ACS Marking

The submitted Identity can be reshared, as is.

8.6 Example C.6. ais-consent-everyone-cisa-proprietary, TLP:Amber (Row 15)

Non-Federal AIS Submission

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--e608bdef-cf42-4e68-be20-c8a36d90b708",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--e608bdef-cf42-4e68-be20-c8a36d90b708",  -- self-referential
  "labels": [
      " ais-consent-everyone-cisa-proprietary"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"      -- TLP:Amber
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Federal AIS Brokered Output

FD: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
CAVEAT: CISAPROPRIETARY
Access Privilege: CISAUSES,
sharedefault: deny,
Identity: un-anonymized

```
{
   "created": "2021-03-18T20:03:00.000Z",
   "modified": "2021-03-18T20:03:00.000Z",
   "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
         "access_privilege": [
          {
            "privilege_action": "CISAUSES",
            "privilege_scope": {
               "entity": ["ALL"],
               "permitted_nationalities": ["ALL"],
               "permitted_organizations": ["ALL"],
               "shareability": ["ALL"]
            },
            "rule_effect": "permit"
          }
        ],
        "control_set": {
            "classification": "U",
```

```
            "formal_determination": [
              "INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT"
            ],
            "caveat": [
              "CISAPROPRIETARY"
            ]
        },
        "further_sharing": [
            {
               "sharing_scope": [
                   "USA.USG"
               ],
               "rule_effect": "permit"
            }
        ],
        "create_date_time": "2021-03-18T20:03:00.000Z",
        "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3-1e4a8ce3-13df-4b20-8fd0-2667d19b9bc9",
        "name": "Example C.6",
        "authority_reference": ["urn:isa:authority:ais"],
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",
        "responsible_entity_custodian": "USA.DHS.CISA",
        "responsible_entity_originator": "NONFED"
        }
   },
   "id": "marking-definition--1e4a8ce3-13df-4b20-8fd0-2667d19b9bc9",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--83e0f42b-e029-4c96-bfa6-7a506e44dbc4",
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-everyone-cisa-proprietary"
  ],
  "name": "ACME, Inc.",
  "object_marking_refs": [
      "marking-definition--1e4a8ce3-13df-4b20-8fd0-2667d19b9bc9"
  ],
  "sectors": [
    "technology"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

Identity: un-anonymized
No need for ACS Marking

The submitted Identity can be reshared, as is.

9 Appendix D: Federal Submissions to Federal/Non-Federal Feeds Examples

This Appendix contains six examples for Non-Federal submissions. Properties that are significant to the examples are in red. Table 7 shows all the possible combinations of ACS data markings that can be found in Federal submissions, but the examples selected for this Appendix were chosen based on the most likely expected submissions.

The name property of the Federal submitter on the Identity object, the responsible_entity_custodian and responsible_entity_originator properties on the ACS data marking object are represented by the placeholder *<Fed Agency #-Ex#>*. See *Appendix F* for information on acceptable values. The values in the three properties need not all be different. There are no implied similar choices between examples. The same UUID is used for the ACS marking-definition id as in the identifier property, but this is not required.

These examples assume the existence of the following Extension Definition object.

```
{
    "id": "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce",
    "type": "extension-definition",
    "spec_version": "2.1",
    "name": "isa-ais-3-0",
    "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"]
}
```

Table 7: Possible Combinations for AIS Data Markings

	Federal Submission Marking Input				Published Marking/Anonymization Non-Federal Output		
	AIS: Consent	ACS: IDSRC Intend with Policy Ref Combination (Either the privdefault, or IDSRC, if present)	FOUO/AIS	PUBREL	TLP	Anonymization	Example
1	*n/a* (default to ais-consent-none)	permit	X		Amber	The identity is anonymized to USG.	
2	*n/a* (default to ais-consent-none)	permit		X	White	The identity is anonymized to USG.	D.1
3	*n/a* (default to ais-consent-none)	permit	X	X	Amber	The identity is anonymized to USG.	

	Federal Submission Marking Input				Published Marking/Anonymization Non-Federal Output		
	AIS: Consent	ACS: IDSRC Intend with Policy Ref Combination (Either the privdefault, or IDSRC, if present)	FOUO/AIS	PUBREL	TLP	Anonymization	Example
1a	*n/a* (default to ais-consent-none)	deny/IDSRC=permit	X		Amber	The identity is anonymized to USG.	
2a	*n/a* (default to ais-consent-none)	deny/IDSRC=permit		X	White	The identity is anonymized to USG.	
3a	*n/a* (default to ais-consent-none)	deny/IDSRC=permit	X	X	Amber	The identity is anonymized to USG.	
4	ais-consent-none	deny	X		Amber	The identity is anonymized to USG.	
5	ais-consent-none	deny		X	White	The identity is anonymized to USG.	D.2
6	ais-consent-none	deny	X	X	Amber	The identity is anonymized to USG.	
7	ais-consent-none	permit	X		Amber	The identity is anonymized to USG.	
8	ais-consent-none	permit		X	White	The identity is anonymized to USG.	
9	ais-consent-none	permit	X	X	Amber	The identity is anonymized to USG.	
7a	ais-consent-none	deny/IDSRC=permit	X		Amber	The identity is anonymized to USG.	
8a	ais-consent-none	deny/IDSRC=permit		X	White	The identity is anonymized to USG.	
9a	ais-consent-none	deny/IDSRC=permit	X	X	Amber	The identity is anonymized to USG.	
10	ais-consent-none	deny	X		Amber	The identity is anonymized to USG.	
11	ais-consent-none	deny		X	White	The identity is anonymized to USG.	
12	ais-consent-none	deny	X	X	Amber	The identity is anonymized to USG.	
13	ais-consent-usg	permit	X		Amber	The identity is anonymized to USG.	
14	ais-consent-usg	permit		X	White	The identity is anonymized to USG.	
15	ais-consent-usg	permit	X	X	Amber	The identity is anonymized to USG.	
13a	ais-consent-usg	deny/IDSRC=permit	X		Amber	The identity is anonymized to USG.	
14a	ais-consent-usg	deny/IDSRC=permit		X	White	The identity is anonymized to USG.	
15a	ais-consent-usg	deny/IDSRC=permit	X	X	Amber	The identity is anonymized to USG.	
16	ais-consent-usg	deny	X		Amber	The identity is anonymized to USG.	
17	ais-consent-usg	deny		X	White	The identity is anonymized to USG.	
18	ais-consent-usg	deny	X	X	Amber	The identity is anonymized to USG.	
19	ais-consent-everyone	Permit	X		Amber	The identity is shared un-anonymized.	D.3

	Federal Submission Marking Input				Published Marking/Anonymization Non-Federal Output		
	AIS: Consent	ACS: IDSRC Intend with Policy Ref Combination (Either the privdefault, or IDSRC, if present)	FOUO/AIS	PUBREL	TLP	Anonymization	Example
20	ais-consent-everyone	Permit		X	White	The identity is shared un-anonymized.	
21	ais-consent-everyone	Permit	X	X	Amber	The identity is shared un-anonymized.	
19a	ais-consent-everyone	deny/IDSRC=permit	X		Amber	The identity is shared un-anonymized.	
20a	ais-consent-everyone	deny/IDSRC=permit		X	White	The identity is shared un-anonymized.	**D.4**
21a	ais-consent-everyone	deny/IDSRC=permit	X	X	Amber	The identity is shared un-anonymized.	
22	ais-consent-everyone	Deny	X		Amber	The identity is anonymized using a consistent random generated name.	**D.5**
23	ais-consent-everyone	Deny		X	White	The identity is anonymized using a consistent random generated name.	**D.6**
24	ais-consent-everyone	Deny	X	X	Amber	The identity is anonymized using a consistent random generated name.	
25	ais-consent-everyone-cisa-proprietary	Permit	X		Amber	The identity is shared un-anonymized.	
26	ais-consent-everyone-cisa-proprietary	Permit		X	White	The identity is shared un-anonymized.	
27	ais-consent-everyone-cisa-proprietary	Permit	X	X	Amber	The identity is shared un-anonymized.	
25a	ais-consent-everyone-cisa-proprietary	deny/IDSRC=permit	X		Amber	The identity is shared un-anonymized.	
26a	ais-consent-everyone-cisa-proprietary	deny/IDSRC=permit		X	White	The identity is shared un-anonymized.	
27a	ais-consent-everyone-cisa-proprietary	deny/IDSRC=permit	X	X	Amber	The identity is shared un-anonymized.	

	Federal Submission Marking Input				Published Marking/Anonymization Non-Federal Output		
	AIS: Consent	ACS: IDSRC Intend with Policy Ref Combination (Either the privdefault, or IDSRC, if present)	FOUO/AIS	PUBREL	TLP	Anonymization	Example
28	ais-consent-everyone-cisa-proprietary	Deny	X		Amber	The identity is anonymized using a consistent random generated name.	
29	ais-consent-everyone-cisa-proprietary	Deny		X	White	The identity is anonymized using a consistent random generated name.	
30	ais-consent-everyone-cisa-proprietary	Deny	X	X	Amber	The identity is anonymized using a consistent random generated name.	

Although all different combinations are allowed for submissions, the ones selected for the examples in the Appendix were chosen based on the most likely expected submissions.

9.1 Example D.1. PUBREL, privdefault = permit, no ais-consent (Row 2)

Federal ACS Submission

```
{
    "created": "2020-10-01T00:00:00Z",
    "created_by_ref": "identity--c407acde-e6b1-4e09-ba39-d5cacebcfd1e",
    "extensions": {
        "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
            "control_set": {
            "classification": "U",
            "formal_determination": [
                    "PUBREL"
                ]
            },
            "create_date_time": "2020-04-06T20:03:00.000Z",
                "extension_type": "property-extension",
            "identifier": "isa:guide.19001.EDH2-f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3",
            "name": "Example D.1",
            "authority_reference": ["urn:isa:authority:misa"],
            "public_release": {
                        "released_by": <some authority>
                        "released_on": "2020-04-06T20:03:00.000Z"
            },
            "policy_reference":
                "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",
            "responsible_entity_custodian": <Fed Agency 1-Ex1>,
            "responsible_entity_originator": <Fed Agency 2-Ex1>,
        }
    },
```

```
    "id": "marking-definition--f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3",
    "type": "marking-definition",
    "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--c407acde-e6b1-4e09-ba39-d5cacebcfd1e",
  "created": "2020-04-06T20:03:00.000Z",
  "modified": "2020-04-06T20:03:00.000Z",
  "created_by_ref": "identity--c407acde-e6b1-4e09-ba39-d5cacebcfd1e",  -- self-referential
  "name": <Fed Agency 3-Ex1>,
  "object_marking_refs": [
      "marking-definition--f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

USA.USG Identity is always ais-consent-everyone/TLP:White. The actual Identity object might be slightly different.

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--f8d34e5b-fbf0-451c-9fa3-d1312372bef5",       -- Fixed USA.USG Identity id
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
       "ais-consent-everyone"
  ],
  "name": "USA.USG",
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"      -- TLP:White
  ],
  "identity_class": "organization"
}
```

9.2 Example D.2. PUBREL, privdefault = deny, ais-consent-none (Row 5)

Federal ACS Submission


```
{
    "created": "2020-10-01T00:00:00Z",
    "created_by_ref": "identity--e726a145-47aa-4108-a56b-db5c8bc0d98c",
    "extensions": {
        "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
            "access_privilege": [
                {
                        "privilege_action": "CISAUSES",
                        "privilege_scope": {
                                "entity": ["ALL"],
                                "permitted_nationalities": ["ALL"],
                                "permitted_organizations": ["ALL"],
                                "shareability": ["ALL"]
                        },
                        "rule_effect": "permit"
                        }
                ],
            "control_set": {
                "classification": "U",
                    "formal_determination": [
                        "PUBREL"
                    ]
            },
            "create_date_time": "2020-04-06T20:03:00.000Z",
                "extension_type": "property-extension",
            "identifier": "isa:guide.19001.EDH2-1b1ec528-4a64-41c0-b0ab-d9533d9591c3",
            "name": "Example D.2",
            "authority_reference": ["urn:isa:authority:misa"],
            "public_release": {
                "released_by": <some authority>
                        "released_on": "2020-04-06T20:03:00.000Z"

            },
            "policy_reference":
                "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",
            "responsible_entity_custodian": <Fed Agency 1-Ex2>,
            "responsible_entity_originator": <Fed Agency 2-Ex2>,
        }
    },
    "id": "marking-definition--1b1ec528-4a64-41c0-b0ab-d9533d9591c3",
        "type": "marking-definition",
    "spec_version": "2.1"

}

{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--e726a145-47aa-4108-a56b-db5c8bc0d98c",
    "created": "2020-04-06T20:03:00.000Z",
    "labels": [
            "ais-consent-none"
```

```
    ],
    "modified": "2020-04-06T20:03:00.000Z",
    "created_by_ref": "identity--e726a145-47aa-4108-a56b-db5c8bc0d98c",  -- self-referential
    "name": <Fed Agency 3-Ex2>,
    "object_marking_refs": [
        "marking-definition--1b1ec528-4a64-41c0-b0ab-d9533d9591c3"
        ],
        "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

USA.USG Identity is always ais-consent-everyone/TLP:White

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--f8d34e5b-fbf0-451c-9fa3-d1312372bef5",         -- Fixed USA.USG Identity id
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
       "ais-consent-everyone"
  ],
  "name": "USA.USG",
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
  ],
  "identity_class": "organization"
}
```

9.3 Example D.3. FOUO/AIS, privdefault = permit, ais-consent-everyone (Row 19)

Federal ACS Submission

```
{
       "created": "2020-10-01T00:00:00Z",
       "created_by_ref": "identity--43a4004c-74a5-42bc-b886-e8ed5b47308b",
       "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
          "control_set": {
                "classification": "U",
                "formal_determination": [
                   "FOUO",
                   "AIS"
                ]
           },
           "further_sharing": [
              {
                 "sharing_scope": [
                    "USA.USG"
                 ],
                 "rule_effect": "permit"
              }
           ],
           "create_date_time": "2020-04-06T20:03:00.000Z",
           "extension_type": "property-extension",
           "identifier": "isa:guide.19001.EDH2-29de1c26-0298-4ec1-8383-61e08e8e3e4a",
           "name": "Example D.3",
           "authority_reference": ["urn:isa:authority:misa"],
           "policy_reference":
               "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=deny",
           "responsible_entity_custodian": <Fed Agency 1-Ex3>,
           "responsible_entity_originator": <Fed Agency 2-Ex3>,
      }
   },
   "id": "marking-definition--29de1c26-0298-4ec1-8383-61e08e8e3e4a",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
       "type": "identity",
       "spec_version": "2.1",
       "id": "identity--43a4004c-74a5-42bc-b886-e8ed5b47308b",
       "created": "2020-04-06T20:03:00.000Z",
       "modified": "2020-04-06T20:03:00.000Z",
    "created_by_ref": "identity--43a4004c-74a5-42bc-b886-e8ed5b47308b",  -- self-referential
       "labels": [
          "ais-consent-everyone"
    ],
    "name": <Fed Agency 3-Ex3>,
    "object_marking_refs": [
       "marking-definition--29de1c26-0298-4ec1-8383-61e08e8e3e4a"
    ],
    "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--12176c6b-5b6b-45f1-9ab0-3b94a76306d5",
  "created": "2020-04-06T21:52:00.000Z",
  "modified": "2020-04-06T21:52:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-everyone"
  ],
  "name": <Fed Agency 3-Ex3>,
  "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82" -- TLP:Amber
  ],
  "identity_class": "organization"
}
```

9.4 Example D.4. PUBREL, privdefault = deny/IDSRC=permit, ais-consent-everyone (Row 20a)

Federal ACS Submission


```
{
   "created": "2020-10-01T00:00:00Z",
   "created_by_ref": "identity--fdcc63f0-cc2d-42bf-87ac-27e122819ed1",
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
           "access_privilege": [
               {
                      "privilege_action": "CISAUSES",
                      "privilege_scope": {
                             "entity": ["ALL"],
                             "permitted_nationalities": ["ALL"],
                             "permitted_organizations": ["ALL"],
                             "shareability": ["ALL"]
                      },
                      "rule_effect": "permit"
                      },
               {
                  "privilege_action": "IDSRC",
                  "privilege_scope": {
                     "entity": ["ALL"],
                     "permitted_nationalities": ["ALL"],
                     "permitted_organizations": ["ALL"],
                     "shareability": ["ALL"]
                   },
                   "rule_effect": "permit"
               }
           ],
           "control_set": {
                 "classification": "U",
                 "formal_determination": [
                    "PUBREL"
                 ]
           },
           "public_release": {
                "released_by": <some authority>
                      "released_on": "2020-04-06T20:03:00.000Z"
           },
           "create_date_time": "2020-04-06T20:03:00.000Z",
           "extension_type": "property-extension",
           "identifier": "isa:guide.19001.EDH2-a864a4e4-d5b0-44d9-99a6-a4e0f620645d",
           "name": "Example D.4",
           "authority_reference": ["urn:isa:authority:misa"],
           "policy_reference":
               "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",
           "responsible_entity_custodian": <Fed Agency 1-Ex4>,
           "responsible_entity_originator": <Fed Agency 2-Ex4>,
      }
   },
   "id": "marking-definition--a864a4e4-d5b0-44d9-99a6-a4e0f620645d",
   "type": "marking-definition",
   "spec_version": "2.1"
}
```

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--fdcc63f0-cc2d-42bf-87ac-27e122819ed1",
  "created": "2020-04-06T20:03:00.000Z",
  "modified": "2020-04-06T20:03:00.000Z",
  "created_by_ref": "identity--fdcc63f0-cc2d-42bf-87ac-27e122819ed1",  -- self-referential
  "labels": [
      "ais-consent-everyone"
  ],
  "name": <Fed Agency 3-Ex4>,
  "object_marking_refs": [
      "marking-definition--a864a4e4-d5b0-44d9-99a6-a4e0f620645d"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--8c877c45-8b6c-406c-9b7b-1bb4a1855038",
  "created": "2020-04-06T21:52:00.000Z",
  "modified": "2020-04-06T21:52:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-everyone"
  ],
  "name": <Fed Agency 3-Ex4>,
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
  ],
  "identity_class": "organization"
}
```

9.5 Example D.5. FOUO/AIS, privdefault = deny, ais-consent-everyone (Row 22)

Federal ACS Submission

```
{
   "created": "2020-10-01T00:00:00Z",
   "created_by_ref": "identity--005d5fd6-53c9-499e-9ca5-2af4b2e85206",
   "extensions": {
      "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
           "access_privilege": [
              {
                     "privilege_action": "CISAUSES",
                     "privilege_scope": {
                            "entity": ["ALL"],
                            "permitted_nationalities": ["ALL"],
                            "permitted_organizations": ["ALL"],
                            "shareability": ["ALL"]
                     },
                     "rule_effect": "permit"
                     }
                     ],
          "control_set": {
                "classification": "U",
                "formal_determination": [
                   "FOUO",
                   "AIS"
                ]
          },
          "create_date_time": "2020-04-06T20:03:00.000Z",
          "extension_type": "property-extension",
          "identifier": "isa:guide.19001.EDH2-fdb3acca-c402-414d-891c-9e94dbdd17b1",
          "name": "Example D.5",
          "authority_reference": ["urn:isa:authority:misa"],
          "policy_reference":
              "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",
          "responsible_entity_custodian": <Fed Agency 1-Ex5>,
          "responsible_entity_originator": <Fed Agency 2-Ex5>,
      }
   },
   "id": "marking-definition--fdb3acca-c402-414d-891c-9e94dbdd17b1",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--005d5fd6-53c9-499e-9ca5-2af4b2e85206",
  "created": "2020-04-06T20:03:00.000Z",
  "modified": "2020-04-06T20:03:00.000Z",
  "created_by_ref": "identity--005d5fd6-53c9-499e-9ca5-2af4b2e85206",  -- self-referential
  "labels": [
      "ais-consent-everyone"
  ],
  "name": <Fed Agency 3-Ex5>,
```

```
  "object_marking_refs": [
      "marking-definition--fdb3acca-c402-414d-891c-9e94dbdd17b1"
  ],
  "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--da0f913c-6921-4309-bda5-c5f02b32e0ce",
  "created": "2020-04-06T21:52:00.000Z",
  "modified": "2020-04-06T21:52:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
      "ais-consent-everyone"
  ],
  "name": "PortThinkYard", -- Anonymous name for Federal agency
  "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82" -- TLP:Amber
  ],
  "identity_class": "organization"
}
```

9.6 Example D.6. PUBREL, privdefault = deny, ais-consent-everyone (Row 23)

Federal ACS Submission


```
{
    "created": "2020-10-01T00:00:00Z",
    "created_by_ref": "identity--0f0fd59e-361e-4196-b39e-e4221a4bccc5",
    "extensions": {
        "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
            "access_privilege": [
                {
                        "privilege_action": "CISAUSES",
                        "privilege_scope": {
                                "entity": ["ALL"],
                                "permitted_nationalities": ["ALL"],
                                "permitted_organizations": ["ALL"],
                                "shareability": ["ALL"]
                        },
                        "rule_effect": "permit"
                        }
                ],
            "control_set": {
                "classification": "U",
                    "formal_determination": [
                        "PUBREL"
                    ]
            },
            "create_date_time": "2020-04-06T20:03:00.000Z",
            "extension_type": "property-extension",
            "identifier": "isa:guide.19001.EDH2-f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3",
            "name": "Example D.6",
            "authority_reference": ["urn:isa:authority:misa"],
            "public_release": {
                "released_by": <some authority>
                "released_on": "2020-04-06T20:03:00.000Z"
            },
            "policy_reference":
                "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",
            "responsible_entity_custodian": <Fed Agency 1-Ex6>,
            "responsible_entity_originator": <Fed Agency 2-Ex6>,
        }
    },
    "id": "marking-definition--f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3",
        "type": "marking-definition",
   "spec_version": "2.1"
}

{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--0f0fd59e-361e-4196-b39e-e4221a4bccc5",
    "created": "2020-04-06T20:03:00.000Z",
    "modified": "2020-04-06T20:03:00.000Z",
    "created_by_ref": "identity--0f0fd59e-361e-4196-b39e-e4221a4bccc5",  -- self-referential
    "labels": [
        "ais-consent-everyone "
```

```
    ],
    "name": <Fed Agency 3-Ex6>,
    "object_marking_refs": [
        "marking-definition--f2175d9c-c90c-4ef9-8af8-e09bdcdfa2c3"
    ],
    "identity_class": "organization"
}
```

Non-Federal AIS Brokered Output

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--6a6c6421-3858-4cfc-9b37-66340c6414e1"
  "created": "2020-04-06T21:52:00.000Z",
  "modified": "2020-04-06T21:52:00.000Z",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01", -- Fixed CISA Identity id
  "labels": [
        "ais-consent-everyone"
  ],
  "name": "SideBoxNature",  -- Anonymous name for Federal agency
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
  ],
  "identity_class": "organization"
}
```

10 Appendix E: Federal Submissions of Non-Federal Content Examples

Federal entities can receive CTIs and DMs directly from non-Federal sources, which the Federal entity will submit to AIS. The examples in this appendix describes the different scenarios that are involved. The choices for the TLP data marking of each example is only to provide coverage of the different TLP colors and was arbitrarily chosen. Properties that are significant to the examples are in red.

These examples assume the existence of the following Extension Definition object.

```
{
    "id": "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce",
    "type": "extension-definition",
    "spec_version": "2.1",
    "name": "isa-acs-3-0",
    "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"]
}
```

In Table 8, the Disposition could be one of the following:

- **Add ACS**: Using the original *STIX submission* as a base, *create a new STIX object with ACS markings*
- **Create with ACS**: Using the original *non-STIX submission* (e.g., email, web form) as a base, *create a new STIX object with ACS markings*

Table 8: Possible Combinations of Federal Submissions of Non-Federal Content

Scenario	Submission Format	AIS Consent	Disposition	Chosen TLP Marking	Output found in Section
1	STIX	ais-consent-everyone-cisa-proprietary	Add ACS	TLP:Green	10.2.1
2	Text	ais-consent-everyone-cisa-proprietary	Create w/ ACS	TLP:Green	10.2.1
3	STIX	ais-consent-everyone	Add ACS	TLP:White	10.2.2
4	Text	ais-consent-everyone	Create w/ ACS	TLP:White	10.2.2
5	STIX	ais-consent-none	Add ACS	TLP:Amber	10.2.3
6	Text	ais-consent-none	Create w/ ACS	TLP:Amber	10.2.3
7	STIX	*n/a (default to ais-consent-none)*	Add ACS	TLP:Green	10.2.4
8	Text	*n/a (default to ais-consent-none)*	Create w/ ACS	TLP:Green	10.2.4
9	STIX	ais-consent-usg	Add ACS	TLP:White	10.2.5
10	Text	ais-consent-usg	Create w/ ACS	TLP:White	10.2.5

In the following examples:

`"identity--3c039500-be42-45e9-b2ee-33494dddc210"` is the Identity ID of the Federal Entity.

10.1 Non-Federal Submissions to Federal Entities

10.1.1 Non-Federal Content as STIX / ais-consent-everyone-cisa-proprietary (Scenario 1)

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--8585cf35-681e-4f38-9df9-7181b3b42a38",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--8585cf35-681e-4f38-9df9-7181b3b42a38",  -- self-referential
  "labels": [
      "ais-consent-everyone-cisa-proprietary"
  ],
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da" -- TLP:Green
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--8585cf35-681e-4f38-9df9-7181b3b42a38",
    "created": "2021-03-06T20:03:48.000Z",
    "modified": "2021-03-06T20:03:48.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da" -- TLP:Green
    ],
     "pattern": "[file:hashes.'SHA-256' =
                        '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-03-01T00:00:00Z"
  }
```

10.1.2 Non-Federal Content as text / ais-consent-everyone-cisa-proprietary (Scenario 2)

To: <Fed Agency App-F>

From: Big Power Company

We want to make you aware of an indicator for Poison Ivy Malware. The file is part of Poison Ivy. Its SHA-256 hash is '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877'. Please treat this indicator as proprietary and marked as TLP:Green, but you can share my identity with everyone. The information can be used only for cybersecurity purposes allowed in the Cybersecurity Information Sharing Act of 2015.

10.1.3 Non-Federal Content as STIX / ais-consent-everyone (Scenario 3)

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--5c5e322a-c9ea-4b74-be3b-6e306630a850",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--5c5e322a-c9ea-4b74-be3b-6e306630a850",  -- self-referential
  "labels": [
      "ais-consent-everyone"
  ],
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--acfbc869-065c-4197-822d-26b9b7b6a3dc",
    "created_by_ref": "identity--5c5e322a-c9ea-4b74-be3b-6e306630a850",
    "created": "2021-03-18T10:31:00.000Z",
    "modified": "2021-03-18T10:31:00.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "The file is part of Poison Ivy",
    "object_marking_refs": [
       "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
     ],
     "pattern": "[file:hashes.'SHA-256' =
                        '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-03-01T00:00:00Z"
}
```

10.1.4 Non-Federal Content as text / ais-consent-everyone (Scenario 4)

To: <Fed Agency App-F>

From: Big Power Company

We want to make you aware of an indicator for Poison Ivy Malware. The file is part of Poison Ivy. Its SHA-256 hash is '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877'. My identity can be shared with everyone. The content is marked as TLP:White.

10.1.5 Non-Federal Content as STIX / ais-consent-none (Scenario 5)

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--150127d6-d1f7-4b59-8edb-43ca1312414b",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--150127d6-d1f7-4b59-8edb-43ca1312414b ",  -- self-referential
  "labels": [
      "ais-consent-none"
  ],
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da" -- TLP:Green
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--dc4af32a-1195-46a5-8ed4-e003f6fdbab2 ",
    "created_by_ref": "identity--150127d6-d1f7-4b59-8edb-43ca1312414b",
    "created": "2021-03-06T20:03:48.000Z",
    "modified": "2021-03-06T20:03:48.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "object_marking_refs": [
      "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da" -- TLP:Green
    ],
     "pattern": "[file:hashes.'SHA-256' =
                         '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-03-01T00:00:00Z"
  }
```

10.1.6 Non-Federal Content as text / ais-consent-none (Scenario 6)

To: <Fed Agency App-F>

From: Big Power Company

We want to make you aware of an indicator for Poison Ivy Malware. The file is part of Poison Ivy. Its SHA-256 hash is '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877'. My identity should not be shared. The content is marked as TLP:Green.

10.1.7 Non-Federal Content as STIX / n/a (default to ais-consent-none) (Scenario 7)

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--6497b96b-490e-4ea1-9200-e26225e57bea",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--8585cf35-681e-4f38-9df9-7181b3b42a38",  -- self-referential
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82" -- TLP:Amber
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--f10fb83a-c5c8-4c15-bd74-13742ba3945c ",
    "created_by_ref": "identity--6497b96b-490e-4ea1-9200-e26225e57bea",
    "created": "2021-03-06T20:03:48.000Z",
    "modified": "2021-03-06T20:03:48.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82" -- TLP:Amber
    ],
     "pattern": "[file:hashes.'SHA-256' =
                        '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-03-01T00:00:00Z"
  }
```

10.1.8 Non-Federal Content as text / no ais-consent information given (Scenario 8)

To: <Fed Agency App-F>

From: Big Power Company

We want to make you aware of an indicator for Poison Ivy Malware. The file is part of Poison Ivy. Its SHA-256 hash is '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877'. The content is marked as TLP:Amber.

10.1.9 Non-Federal Content as STIX / ais-consent-usg (Scenario 9)

```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--571f7d54-3644-4086-983b-912d640b23b2 ",
  "created": "2021-03-18T10:31:00.000Z",
  "modified": "2021-03-18T10:31:00.000Z",
  "created_by_ref": "identity--5c5e322a-c9ea-4b74-be3b-6e306630a850",  -- self-referential
  "labels": [
      "ais-consent-usg"
  ],
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--676c817e-5a87-40db-b4ce-316ff7fc7fca ",
    "created_by_ref": "identity--571f7d54-3644-4086-983b-912d640b23b2 ",
    "created": "2021-03-18T10:31:00.000Z",
    "modified": "2021-03-18T10:31:00.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "The file is part of Poison Ivy",
    "object_marking_refs": [
       "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9" -- TLP:White
     ],
     "pattern": "[file:hashes.'SHA-256' =
                         '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-03-01T00:00:00Z"
}
```

10.1.10 Non-Federal Content as text / ais-consent-usg (Scenario 10)

To: <Fed Agency App-F>

From: Big Power Company

We want to make you aware of an indicator for Poison Ivy Malware. The file is part of Poison Ivy. Its SHA-256 hash is '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877'. My identity can only be shared with other US government agencies. The content is marked as TLP:White.

10.2 Federal Submissions of Non-Federal Submissions to AIS

10.2.1 Federal Submission for Scenario 1 & 2


```
{
        "created": "2021-03-18T20:03:00.000Z",
        "modified": "2021-03-18T20:03:00.000Z",
        "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
        "extensions": {
        "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
           "control_set": {
              "classification": "U",
              "caveat": [
                 "CISAPROPRIETARY"
              ],
           },
           "access_privilege": [
              {
                 "privilege_action": "CISAUSES",
                 "privilege_scope": {
                     "entity": ["ALL"],
                    "permitted_nationalities": ["ALL"],
                    "permitted_organizations": ["ALL"],
                    "shareability": ["ALL"]
                 },
                 "rule_effect": "permit"
              }
           ],
           "further_sharing": [
                 {
                    "sharing_scope": [
                        "FOREIGNGOV"
                    ],
                    "rule_effect": "permit"
                 },
                 {
                    "sharing_scope": [
                        "SECTOR"
                     ],
                     "rule_effect": "permit"
                 },
                 {
                     "sharing_scope": [
                        "USA.USG"
                     ],
                     "rule_effect": "permit"
                 }
           ]
        },
        "create_date_time": "2021-03-18T20:03:00.000Z",
        "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3-3fac2c76-c170-4ba7-8775-45cadc84b352",
        "name": "Example 10.1/2",
        "authority_reference": ["urn:isa:authority:misa"],
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",
        "responsible_entity_custodian": <Fed Agency App-F>,
        "responsible_entity_originator": "NONFED"
        }
   },
```

```
   "id": "marking-definition--3fac2c76-c170-4ba7-8775-45cadc84b352",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--6f67310e-0ce5-48e0-8991-1cd207516bfb",
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "labels": [
      "ais-consent-everyone-cisa-proprietary"
  ],
  "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--3fac2c76-c170-4ba7-8775-45cadc84b352",
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--df53618c-a85f-436e-b946-935f1d83acf6",
    "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
    "created": "2021-03-18T20:03:00.000Z",
    "modified": "2021-03-18T20:03:00.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "The file is part of Poison Ivy",
     "object_marking_refs": [
      "marking-definition--3fac2c76-c170-4ba7-8775-45cadc84b352",
        ],
     "pattern": "[file:hashes.'SHA-256' =
                        '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-01-01T00:00:00Z"
  }
```

10.2.2 Federal Submission for Scenario 3 & 4


```
{
       "created": "2021-03-18T20:03:00.000Z",
       "modified": "2021-03-18T20:03:00.000Z",
       "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
       "extensions": {
       "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
        "control_set": {
            "classification": "U",
            "formal_determination": [
               "PUBREL"
                ]
        },
        "create_date_time": "2021-03-18T20:03:00.000Z",
       "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3-248c1a9c-518c-4268-b0da-c5c22771d965",
        "name": "Example 10.3/4",
        "authority_reference": ["urn:isa:authority:misa"],
        "public_release": {
           "released_by": "NONFED"
              "released_on": "2020-04-06T20:03:00.000Z"
        },
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",
        "responsible_entity_custodian": <Fed Agency App-F>,
        "responsible_entity_originator": "NONFED"
        }
   },
   "id": "marking-definition--248c1a9c-518c-4268-b0da-c5c22771d965",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--6f67310e-0ce5-48e0-8991-1cd207516bfb",
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "labels": [
      "ais-consent-everyone"
  ],
  "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--248c1a9c-518c-4268-b0da-c5c22771d965",
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--df53618c-a85f-436e-b946-935f1d83acf6",
    "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
    "created": "2021-03-18T20:03:00.000Z",
```

```
  "modified": "2021-03-18T20:03:00.000Z",
  "indicator_types": ["malicious-activity"],
  "name": "Poison Ivy Malware",
  "description": "The file is part of Poison Ivy",
   "object_marking_refs": [
     "marking-definition--248c1a9c-518c-4268-b0da-c5c22771d965",
       ],
   "pattern": "[file:hashes.'SHA-256' =
                       '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
  "pattern_type": "stix",
  "valid_from": "2021-01-01T00:00:00Z"
}
```

10.2.3 Federal Submission for Scenario 5 & 6


```
{
       "created": "2021-03-18T20:03:00.000Z",
       "modified": "2021-03-18T20:03:00.000Z",
       "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
       "extensions": {
       "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
        "control_set": {
            "classification": "U",
          ]
        },
        "further_sharing": [
                {
                   "sharing_scope": [
                       "FOREIGNGOV"
                   ],
                   "rule_effect": "permit"
                },
                {
                   "sharing_scope": [
                       "SECTOR"
                    ],
                    "rule_effect": "permit"
                },
                {
                    "sharing_scope": [
                       "USA.USG"
                    ],
                    "rule_effect": "permit"
                }
        ],
        "create_date_time": "2021-03-18T20:03:00.000Z",
        "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3-3fac2c76-c170-4ba7-8775-45cadc84b352",
        "name": "Example 10.5/6",
        "authority_reference": ["urn:isa:authority:misa"],
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=deny",
        "responsible_entity_custodian": <Fed Agency App-F>,
        "responsible_entity_originator": "NONFED"
        }
   },
   "id": "marking-definition--eddcf8f5-db88-4611-ab1f-16b4fc871124",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity-- 9b38ddf4-a3c7-40cb-a2e4-9fe902e05fe6",
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "labels": [
      "ais-consent-none"
  ],
  "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
```

```
      "marking-definition--eddcf8f5-db88-4611-ab1f-16b4fc871124",
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--c2ee1843-2741-4334-9a70-1dfaca72d49a",
    "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
    "created": "2021-03-18T20:03:00.000Z",
    "modified": "2021-03-18T20:03:00.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "The file is part of Poison Ivy",
     "object_marking_refs": [
       "marking-definition--eddcf8f5-db88-4611-ab1f-16b4fc871124",
         ],
     "pattern": "[file:hashes.'SHA-256' =
                        '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "valid_from": "2021-01-01T00:00:00Z"
  }
```

10.2.4 Federal Submission for Scenario 7 & 8


```
{
       "created": "2021-03-18T20:03:00.000Z",
       "modified": "2021-03-18T20:03:00.000Z",
       "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
       "extensions": {
       "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
        "control_set": {
            "classification": "U"
        },
        "further_sharing": [
          {
             "sharing_scope": [
                 "USA.USG"
             ],
             "rule_effect": "permit"
          }
        ],
        "create_date_time": "2021-03-18T20:03:00.000Z",
        "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3-feef5b5d-d542-4b19-847f-fe200f7b9a2c",
        "name": "Example 10.7/8",
        "authority_reference": ["urn:isa:authority:misa"],
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",
        "responsible_entity_custodian": <Fed Agency App-F>,
        "responsible_entity_originator": "NONFED"
        }
   },
   "id": "marking-definition--feef5b5d-d542-4b19-847f-fe200f7b9a2c",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity-- 9b38ddf4-a3c7-40cb-a2e4-9fe902e05fe6",
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "labels": [
      "ais-consent-none"
  ],
  "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--feef5b5d-d542-4b19-847f-fe200f7b9a2c",
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--6b883612-433c-4377-87cb-e3dc79132dad",
    "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
```

```
  "created": "2021-03-18T20:03:00.000Z",
  "modified": "2021-03-18T20:03:00.000Z",
  "indicator_types": ["malicious-activity"],
  "name": "Poison Ivy Malware",
  "description": "The file is part of Poison Ivy",
   "object_marking_refs": [
     "marking-definition--feef5b5d-d542-4b19-847f-fe200f7b9a2c",
       ],
   "pattern": "[file:hashes.'SHA-256' =
                       '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
  "pattern_type": "stix",
  "valid_from": "2021-01-01T00:00:00Z"
}
```

10.2.5 Federal Submission for Scenario 9 & 10


```
{
       "created": "2021-03-18T20:03:00.000Z",
       "modified": "2021-03-18T20:03:00.000Z",
       "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
       "extensions": {
        "extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce": {
        "control_set": {
            "classification": "U",
            "formal_determination": [
               "PUBREL"
                ]
        },
        "create_date_time": "2021-03-18T20:03:00.000Z",
        "extension_type": "property-extension",
        "identifier": "isa:guide.19001.ACS3- 95b307b0-8ee4-4913-aae5-4652af278a05",
        "name": "Example 10.9/10",
        "authority_reference": ["urn:isa:authority:misa"],
        "public_release": {
           "released_by": "NONFED"
              "released_on": "2020-04-06T20:03:00.000Z"
        },
        "policy_reference":
           "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",
        "responsible_entity_custodian": <Fed Agency App-F>,
        "responsible_entity_originator": "NONFED"
        }
   },
   "id": "marking-definition-- 95b307b0-8ee4-4913-aae5-4652af278a05",
   "type": "marking-definition",
   "spec_version": "2.1"
}

{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--860a1941-6d38-4121-9932-1eff07011983",
  "created": "2020-01-01T00:00:00.000Z",
  "modified": "2020-01-01T00:00:00.000Z",
  "labels": [
      "ais-consent-usg"
  ],
  "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
  "name": "Big Power Company, Inc.",
  "object_marking_refs": [
      "marking-definition--95b307b0-8ee4-4913-aae5-4652af278a05",
  ],
  "sectors": [
    "utilities"
  ],
  "identity_class": "organization"
}

{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--48624f17-6531-4114-8bf6-deaa8cc21078",
    "created_by_ref": "identity--3c039500-be42-45e9-b2ee-33494dddc210",
    "created": "2021-03-18T20:03:00.000Z",
```

```
  "modified": "2021-03-18T20:03:00.000Z",
  "indicator_types": ["malicious-activity"],
  "name": "Poison Ivy Malware",
  "description": "The file is part of Poison Ivy",
   "object_marking_refs": [
     "marking-definition--95b307b0-8ee4-4913-aae5-4652af278a05",
       ],
   "pattern": "[file:hashes.'SHA-256' =
                       '4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
  "pattern_type": "stix",
  "valid_from": "2021-01-01T00:00:00Z"
}
```

11 Appendix F: CUST and ORIG values

The values that are appropriate for CUST and ORIG tokens in ACS data markings are described in Appendix A of *Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0a*. However, appropriate values are in constant flux, so any published list of values will usually be out of date. Table A1 in that appendix gives the schema for possible legal values.

In addition, the following references can be used to discover additional possible current values:

- https://www.usa.gov/federal-agencies/
- https://www.usgovernmentmanual.gov/ReadLibraryItem.ashx?SFN=NX4I/afytDHsPvUO6hCdhQ==&SF=VHhnJrOeEAnGaa/rtk/JOg==
- https://ucsd.libguides.com/govspeak/home
- https://www.usa.gov/states-and-territories