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

JULY 2016

Version 1.0.1

This page intentionally left blank.

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.

On December 18, 2015, Congress signed the Cybersecurity Information Sharing Act of 2015 (CISA) to create a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties.

The Department of Homeland Security (DHS) provides operational procedures and guidelines for Federal and non-Federal entities to share Cybersecurity Threat Indicators (CTIs) and Defensive Measures (DMs) information. In real time, Federal entities exchange unclassified CTIs and DMs under the Enhance Shared Situational Awareness (ESSA) Multi-lateral Information Sharing Agreement (MISA), using DHS-hosted infrastructure. Non-Federal entities exchange CTIs and DMS in real time under the Automated Indicator Sharing initiative (AIS) Terms of Use, also using DHS-hosted infrastructure. These two communities, Federal and Non-Federal entities, form two independent sharing communities but have the ability 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, 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 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 that 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.

This page intentionally left blank

Table of Contents

1 Introduction

On December 18, 2015, Congress signed the Cybersecurity Information Sharing Act of 2015 (CISA)[1] to create a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. In response, the Department of Homeland Security (DHS) provided operational procedures and guidelines[2] for Federal and non-Federal entities to share cyber threat indicators (CTIs) and defensive measures (DMs) information.

Federal entities exchange classified and unclassified cyber information in real time under the Enhance Shared Situational Awareness (ESSA) Multi-lateral Information Sharing Agreement (MISA)[3]. Unclassified Federal entity cyber information exchange uses DHS-hosted infrastructure. Non-Federal entities exchange CTIs and DMS in real time under the Automated Indicator Sharing (AIS) initiative Terms of Use, also using DHS-hosted infrastructure. The Federal and non-Federal entities form two independent sharing communities but have the ability to share and leverage information between them via machine-to-machine exchanges and processing[4] to quickly mitigate cyber threats and enable defensive measures.

This information sharing ecosystem contributes to:

- protecting public health and safety, national and economic security;
- improving the ability of an information consumer to assess confidence in CTI and DMs;
- improving the ability to prevent rather than just respond, and
- reducing duplication of analytic efforts that are collectively and individually time consuming and expensive, including discovery and course of action development

1.1 Overview of Brokering

A Broker provides a secure, reliable means to transfer information from one Trust Community to the other, 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 (ESSA) and non-Federal (AIS) entities (see Figure 1) while DHS (the broker) automatically moves information between the communities in a way that is transparent to the information producers and consumers as authorized under CISA.

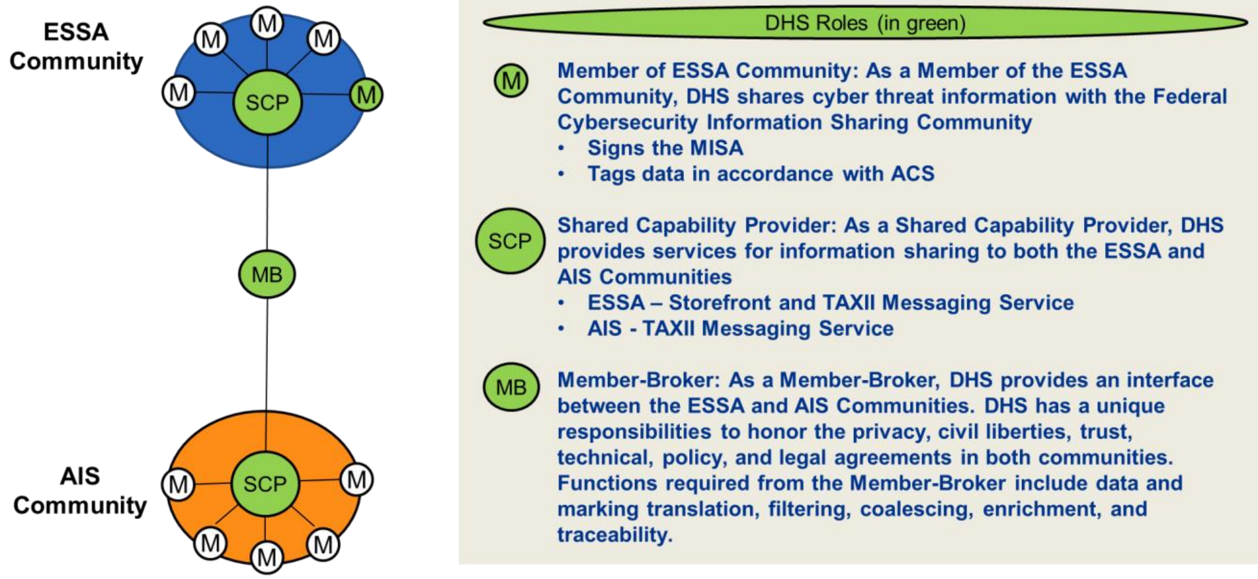
[1] "Cybersecurity Act of 2015," specifically Division N, Title I – Cybersecurity Information Sharing

[2] "Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government," June 15, 2016; "Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015," June 15, 2016; Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with the Federal Government under the Cybersecurity Information Sharing Act 2015," June 15, 2016; Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015," February 16, 2016.

[3] ESSA Multilateral Information Sharing Agreement (MISA), March 2015

[4] Automation is enabled by standards such as STIX and TAXII which define a common language and transport mechanism. Ensuring that the knowledge model or semantics are also shared within a Trust Community is likely to be an emerging area of research and development.

Figure 1 demonstrates that in addition to acting as a broker, DHS also plays the role of member and Shared Capability Provider (SCP).



DHS Roles (in green)

M Member of ESSA Community: As a Member of the ESSA Community, DHS shares cyber threat information with the Federal Cybersecurity Information Sharing Community

- Signs the MISA
- Tags data in accordance with ACS

SCP Shared Capability Provider: As a Shared Capability Provider, DHS provides services for information sharing to both the ESSA and AIS Communities

- ESSA – Storefront and TAXII Messaging Service
- AIS - TAXII Messaging Service

MB Member-Broker: As a Member-Broker, DHS provides an interface between the ESSA and AIS Communities. DHS has a unique responsibilities to honor the privacy, civil liberties, trust, technical, policy, and legal agreements in both communities. Functions required from the Member-Broker include data and marking translation, filtering, coalescing, enrichment, and traceability.

Figure 1: DHS Roles in Context of CISA 2015

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 ensures that information received from the Federal entity producers, absent explicit markings that permit dissemination to non-Federal entities, is filtered (removed) and 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. By definition, DHS understands the needs of each Community so the translation can be targeted and specific rather than an ubiquitous Rosetta Stone.

1.2 Scope of Document

This document describes the processing performed by DHS, as the broker, to enable the Federal and non-Federal cyber information sharing communities to exchange information. DHS 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 specified by the non-Federal entity.
- unclassified Federal entity originated information in real-time to non-Federal entities per the access control markings affixed by the Federal entity originator. The Federal entity originator must explicitly elect to share with non-Federal entities. The designation for AIS sharing by the Federal entity originator is documented in the Information Sharing Architecture (ISA) Access Control Specification (ACS).[5]

[5] "ISA Access Control Specification v3.0" February 2016

- 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 acts a broker when disseminating this information to the Federal entities. DHS applies appropriate ACS markings for information disseminated to the 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. This is *a living document* and will be periodically revisited and updated accordingly as technical advancements are made while fulfilling obligations to the Cybersecurity Information Act of 2015.

1.3 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 National Cybersecurity and Communications Integration Center (NCCIC) Shared Infrastructure. The messaging hub and client software uses the Trusted Automated eXchange of Indicator Information (TAXII™) protocol over an encrypted connection. The DHS 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 fields to be shared in accordance with the AIS STIX profile[6]. The TAXII client software pushes the STIX file to the DHS shared infrastructure. The DHS shared infrastructure receives the STIX file, processes it, and publishes it for all allowable entities to receive. The allowable entity's TAXII client also receives STIX files and as a participant, may parse and use the files 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.

[6] AIS Profile can be found at: AIS Profile excel spreadsheet

2 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 Terms of Use. The non-Federal entities have the option to actively participate or passively monitor the shared CTI and DM information.

2.1 Non-Federal Entity Originated Information Use Case

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

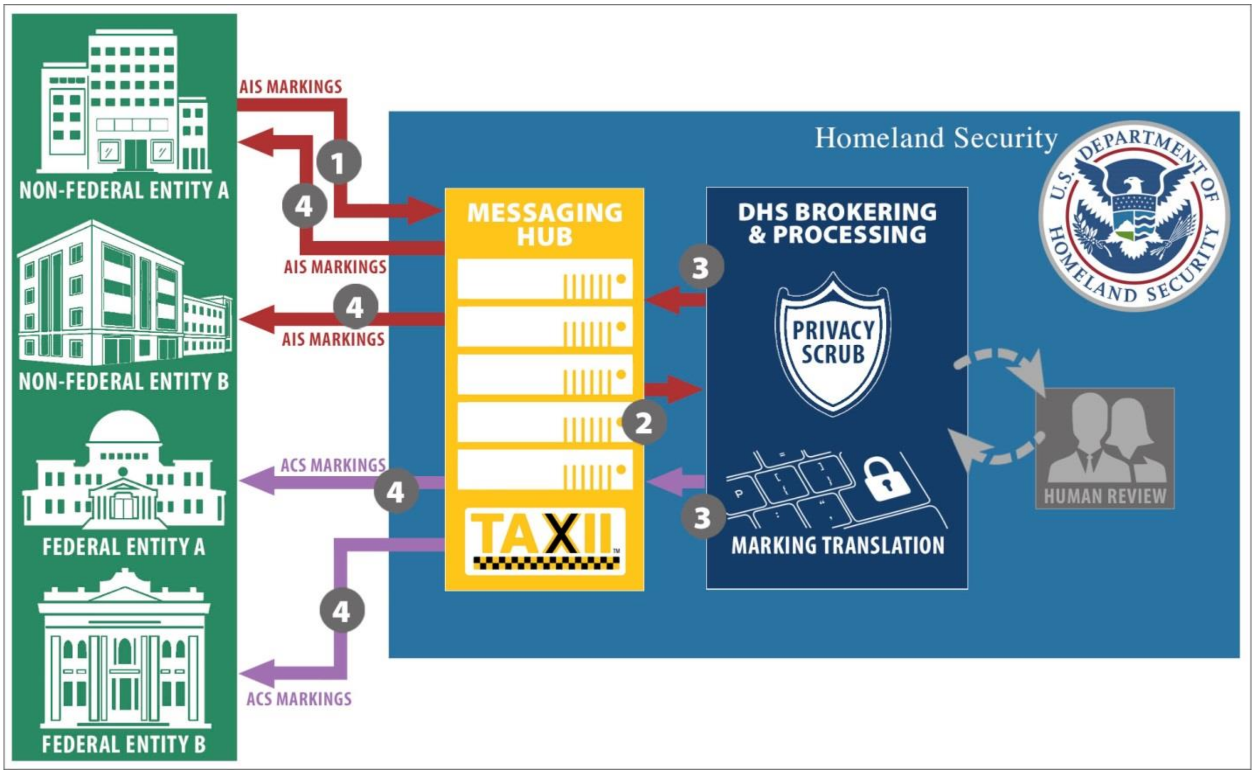


Figure 2: Non-Federal Entity Originated Indicator Sharing

1. Non-Federal Entity A publishes a machine-readable document containing an indicator to DHS-hosted messaging hub.
2. DHS receives the indicator from the hub and automatically processes the indicator (technical and privacy mitigations applied). Note: human review may be required in some instances.
3. DHS 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 indicators are disseminated to subscribed, non-Federal entities and to Federal entities.

2.2 Non-Federal Entity Markings

All non-Federal entity originated STIX files are sent via the DHS-hosted TAXII server with three markings:

- TLP: TLP employs four colors, White, Green, Amber, and Red[7] to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). This is a mandatory STIX field for the non-Federal entity producer that defines coarsely how information can be shared between the communities.
- AIS Consent: This is a mandatory STIX field used by non-Federal entities to indicate if they provide consent to share their identity with everyone, with Federal entities, or with no one (allowable values: United States Government (USG), None, Everyone). DHS anonymizes the identity of the submitter prior to publishing to:
    - Non-Federal entities if AIS Consent is set to USG or None
    - Everyone if AIS Consent is set to None.
- CISA Proprietary: This allows a participant to mark information as Proprietary per the CISA.

A non-Federal Entity receiving an AIS document from DHS is responsible for processing the TLP color in accordance with the guidelines for TLP[8] and based on their own policies.

2.3 DHS Non-Federal to Federal Brokering

DHS brokers non-Federal entity information to Federal entity participants. As a broker, DHS is responsible for:

- STIX profile translation from the AIS STIX profile to the profile used by the Federal community;
- Markings translations from the AIS markings to markings used by the Federal community (ISA ACS Markings).

2.3.1 Profile Translation

In the current release of AIS, the information is formatted in accordance with the AIS STIX Profile. No translation (other than marking) to the Federal entity STIX profile takes place.

2.3.2 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 non-person 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);

[7] If a non-Federal entity applies TLP Red to a submitted file, no automated sharing with Federal Entities occur. DHS will work with the producer to determine next steps.

[8] TLP reference: https://www.us-cert.gov/tlp

- 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.

The ACS provides guidance to mark each part of a document differently, as required by some use cases. This is referred to as field level markings and may be used, in the case of AIS, to further protect identity information shared with the Federal Entities. At this time, the brokering capability does not support field level markings.

2.3.2.1 Resource Accounting

All cyber information that DHS brokers from AIS non-Federal entities to the Federal entities includes an Identifier and creation date and time in accordance with the ACS. The producer information is reflected in the ResponsibleEntity field with a Custodian of US-CERT and an Originator of either USA.USG or NONFED (CUST:USA.USG.US-CERT ORIG:USA.USG).

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

2.3.2.2 Access Restrictions

All cyber information that DHS 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 (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. This restriction related to the non-Federal entity's identity can be marked via ACS field level marking on the source organization name (ORG:USA.USG). If field level marking is not used, the entire STIX document is marked with the most restrictive marking.

2.3.2.3 Usage Restrictions

The usage restrictions placed on AIS cyber information shared with the Federal Cybersecurity Information Sharing Community are specified in the CISA (Sec.105.(d).(5).(A)). The ACS attribute value used to restrict actions outlined in the CISA is CISAUSES. All AIS information brokered to Federal entities by DHS includes this usage restriction.

2.3.2.4 Further Sharing Restrictions

When a Federal entity receives the identity of a submitter that has consented to sharing their identity, the Federal Entity is restricted from further sharing that identity outside of the Federal Government. Therefore, the ACS tags include a restriction on further sharing.

2.3.2.5 Formal Determinations and Caveats

Because DHS is doing automated processing of many fields for real-time dissemination, some fields (e.g. threat email address) may contain personal information of a specific individual or information that identifies a specific individual that is directly related to the cybersecurity threat. DHS assigns all information originating from the AIS Community a formal determination FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT to indicate that any personal information of a specific individual or information that identifies a specific individual has been determined to be directly related to a cybersecurity threat (effective end of summer 2016). This marking indicates that DHS has processed the information through automated or manual privacy checks. 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 resource must observe appropriate restrictions as requested by the originator in accordance with the CISA. Note that CISAProprietary does not carry the same processing/handling restrictions as PROPIN. The AIS profile schema does not permit the use of CISAPROPRIETARY when CONSENT=USG or None.

2.3.2.6 Traffic Light Protocol Translations

The following sections outline the markings translations that DHS does when an AIS file is marked with specific TLP colors.

2.3.2.6.1 TLP White Information

When DHS receives an AIS file marked TLP White from a non-Federal entity, as per the definition, DHS updates the file and marks it with ACS markings as publicly released (Formal Determination (FD) as Publicly Releasable or FD:PUBREL). Federal entities are free to share that cyber information publicly provided that any originator identity information is protected in accordance with any field level tags (removed if marked ORG:USA.USG or retained if marked FD:PUBREL).

The AIS schema does not permit CISAProprietary and CONSENT=USG or None. Non-Federal entities are discouraged from setting the CISA Proprietary flag to true and using TLP White; however, this combination is not prohibited. If DHS receives an indicator marked TLP White and CISAProprietary = true, DHS translates to ACS markings as if received as TLP Green.

Table 1 describes the translations that take place from information submitted with TLP White and AIS Consent and CISA Proprietary markings to ACS Markings placed on the cyber information and the originator information.

Table 1: TLP White, AIS Consent and CISA Proprietary Markings

<table>
<tr><th rowspan="2"></th><th colspan="4">TLP White</th></tr>
<tr><th colspan="2">Cyber Information</th><th colspan="2">Originator Field</th></tr>
<tr><td rowspan="3">Consent=
USG</td><td colspan="2">Federal Community access restriction: None
Formal Determination: Publically Releaseable
Usage restrictions: CISAUSES are permitted
Further sharing: All further sharing is permitted</td><td colspan="2">Federal Community access restriction:: Federal Entities only
Usage restrictions: CISAUSES are permitted
Further sharing: Further sharing outside Federal Entities is denied</td></tr>
<tr><td>Proprietary</td><td>Not Proprietary</td><td>Proprietary</td><td>Not Proprietary</td></tr>
<tr><td>Not a valid combination</td><td><no Proprietary caveat></td><td><Not applicable></td><td><Not applicable></td></tr>
<tr><td rowspan="3">Consent=
None</td><td colspan="2">Federal Community access restriction: None
Formal Determination: Publically Releaseable
Usage restrictions: CISAUSES are permitted
Further sharing: All further sharing is permitted</td><td colspan="2">Source information is removed</td></tr>
<tr><td>Proprietary</td><td>Not Proprietary</td><td>Proprietary</td><td>Not Proprietary</td></tr>
<tr><td>Not a valid combination</td><td><no Proprietary caveat></td><td><Not applicable></td><td><Not applicable></td></tr>
<tr><td rowspan="3">Consent=
Everyone</td><td colspan="2">Federal Community access restriction: None
Formal Determination: Publically Releaseable
Usage restrictions: CISAUSES are permitted
Further sharing: All further sharing is permitted</td><td colspan="2">Federal Community Sharing restriction: None
Formal Determination: Publically Releaseable
Usage restrictions: CISAUSES are permitted
Further sharing: All further sharing is permitted</td></tr>
<tr><td>Proprietary</td><td>Not Proprietary</td><td>Proprietary</td><td>Not Proprietary</td></tr>
<tr><td>CISAProprietary</td><td><no Proprietary caveat></td><td><Not applicable></td><td><Not applicable></td></tr>
</table>

2.3.2.6.2 TLP Green Information

When an AIS file marked TLP Green is received, DHS 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 publically accessible channels (where a publically accessible channel is one that can be accessed anonymously). 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 the field level tags (removed if marked for Federal entities only (ORG:USA.USG) or retained if marked FD:PUBREL).

Table 2 describes the translations that take place from information submitted with TLP Green and AIS Consent and CISA Proprietary markings to ACS Markings placed on the cyber information and the originator information.

Table 2: TLP Green, AIS Consent and CISA Proprietary Markings

	TLP Green			
	Cyber Information		Originator Field	
Consent= USG	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV		Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied	
	Proprietary	No Proprietary	Proprietary	Not Proprietary
	Not a valid combination	<no Proprietary caveat>	<Not applicable>	<Not applicable>
Consent= None	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV		Source information is removed	
	Proprietary	Not Proprietary	Proprietary	Not Proprietary
	Not a valid combination	<no Proprietary caveat>	<Not applicable>	<Not applicable>
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		Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing is permitted to SECTOR, Federal Entities, and FOREIGNGOV	
	Proprietary	Not Proprietary	Proprietary	Not Proprietary
	Caveat: CISAProprietary	<no Proprietary caveat>	<Not applicable>	<Not applicable>

2.3.2.6.3 TLP Amber Information

When an AIS file marked TLP Amber is received, DHS translates the AIS marking and marks the document with ACS markings to indicate that Federal entities are free to use within that organization (no further sharing is allowed.)

Table 3 describes the translations that take place from information submitted with TLP Amber and AIS Consent and CISA Proprietary markings to ACS Markings placed on the cyber information and the originator information.

Table 3: TLP Amber, AIS Consent and CISA Proprietary Markings

	TLP AMBER			
	Cyber Information		Originator Field	
Consent= USG	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied		Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied	
	Proprietary	No Proprietary	Proprietary	Not Proprietary
	Not a valid combination	<no Proprietary caveat>	<Not applicable>	<Not applicable>
Consent= None	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied		Source information is removed	
	Proprietary	Not Proprietary	Proprietary	Not Proprietary
	Not a valid combination	<no Proprietary caveat>	<not applicable>	<not applicable>
Consent= Everyone	Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied		Federal Community access restriction: Federal Entities only Usage restrictions: CISAUSES are permitted Further sharing: Further sharing outside Federal Entities is denied	
	Proprietary	Not Proprietary	Proprietary	Not Proprietary
	Caveat: CISAProprietary	<no Proprietary caveat>	<Not applicable>	<Not applicable>

2.3.2.6.4 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 receives a TLP Red file, DHS contacts the originator and determines next steps. The file is not automatically disseminated to the AIS Community or Federal Entities.

2.3.3 AIS Data Stewardship

To ensure that sensitive information is removed, DHS replaces STIX identifiers (ID) for all information shared via AIS prior to dissemination. Note that DHS does not update relationship identifiers where the new STIX document refers to a DHS-defined STIX ID from a previously shared STIX document.

3 Brokering From Federal Entities to Non-Federal Entities

3.1 Federal Entity Originated Information Use Case

Federal Entity A creates a machine-readable document containing indicators 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 indicator submitted by the Federal entity to DHS, the brokering that is performed, and the flow of the indicator back out to the two trust communities.

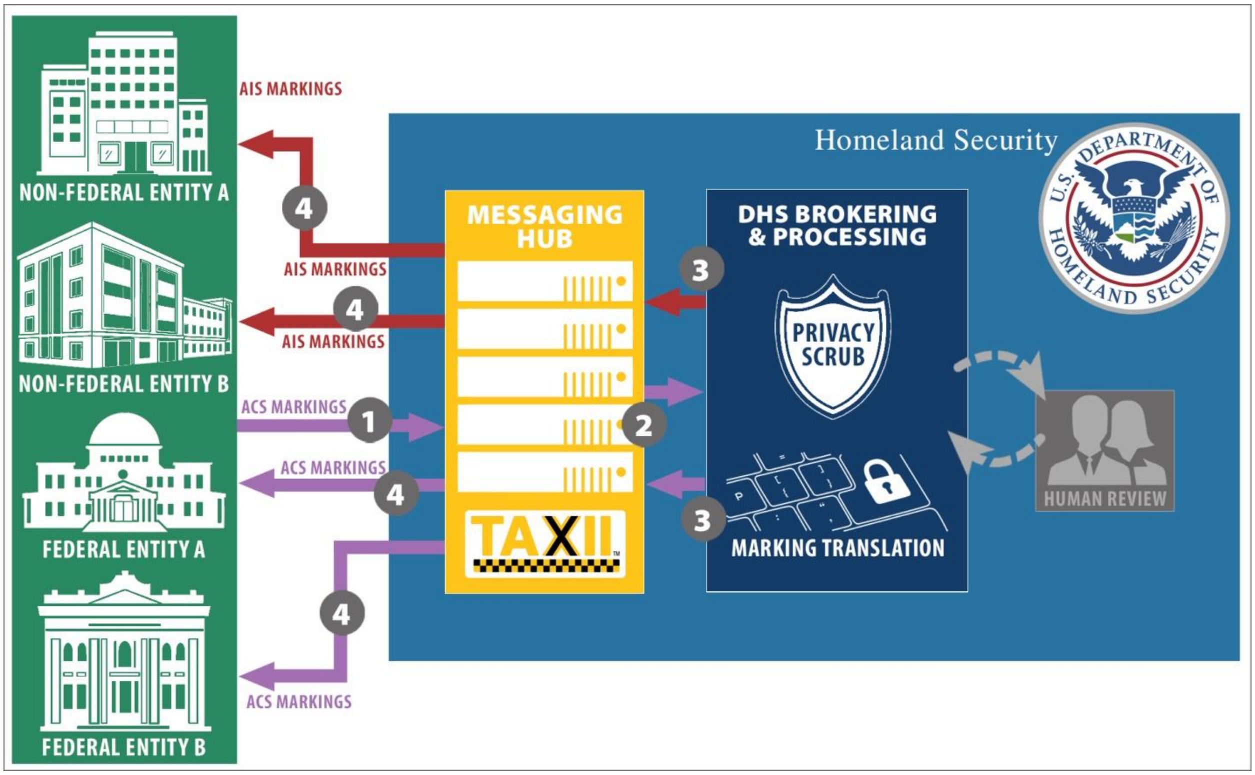


Figure 3: Federal Entity Originated Indicator Sharing through AIS Processing

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

3.2 DHS Federal Entity to non-Federal Entity Brokering

DHS brokers Federal entity-originated information sent to the DHS-hosted TAXII server intended for dissemination via AIS to non-Federal entities. In addition, DHS publishes these indicators to all of the Federal entity community. Indicators submitted by Federal entities specifically marked for further sharing to the AIS community are also brokered by DHS to the Federal entities after undergoing AIS processing similar to that conducted on indicators shared with the non-Federal community. Indicators shared with the Federal entities are be marked with ACS markings. This brokering is discussed in detail in Section 4.1.

3.2.1 STIX Profile Translation

In the initial implementation of the brokering capability, Federal entities **must** submit information in accordance with the AIS STIX Profile and marked with ACS markings as described below.

Federal entity-originated information is published by DHS 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.

3.2.2 Markings Translations

As a broker, DHS translates the ACS markings to the TLP and AIS Consent Markings required for non-Federal entity sharing. Initially, DHS does not process the entire set of ACS markings or provide support for field level markings. In the future, DHS will update the brokering capability to include the ISA ACS markings for default and most restrictive marking (per ACS) plus field level markings.

DHS performs translations from the ACS Markings to AIS Markings for non-Federal entities:

- DHS translates ACS Markings to TLP White or Amber based on the ACS Marking in the STIX Header of the Federal entity originated STIX document.
  - When DHS receives a STIX file from a Federal Entity with a marking in the STIX Header containing the formal determination (abbreviated as FD where needed) of PUBREL, DHS shares this publicly with anyone, including AIS members. This is marked TLP White.
  - When DHS receives a STIX file from a Federal Entity with a marking in the STIX Header containing the formal determination of AIS and a formal determination of FOUO, DHS shares the file with members of AIS. This is not considered publically released and is marked TLP Amber.
- In both cases (FD=PUBREL or (FD=AIS and FD:FOUO)), DHS does not share the specific identity of the Federal entity-originating organization to Non-Federal entities. DHS updates all Federal entity-originated information to indicate the source as “USA.USG” when released to the non-Federal entity Sharing Community. DHS does not pass any additional Originator information contained in the ACS markings.
- DHS replaces all identifiers within the document submitted to AIS prior to further sharing to both Federal and non-Federal Entities.

- If the STIX header marking contains either FD=PUBREL or (FD=AIS and FD:FOUO), this is an indication, by the Federal entity originator, that DHS may release the information to the non-Federal entities, upon removal of the identity of the Federal entity-originator.
- DHS removes any ACS field level markings from the STIX document prior to dissemination to both Federal Entities and non-Federal Entities.
- DHS does not process field level markings with this initial brokering capability. Therefore, Federal Entities must ensure that all of the indicators submitted in the document are submitted at the same level (either all FD:PUBREL or all (FD:AIS and FD:FOUO).

3.2.3 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 applies Privacy Scrubbing algorithms to all Federal entity originated STIX files (as is done with non-Federal entities). Free text fields, for which no privacy-scrubbing-mitigation exists, 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.

3.2.4 Authority Information

Information shared by Federal entities to DHS for further dissemination to non-Federal entities via AIS is shared under the authority of the MISA. Therefore, Federal entities include an authority reference with a value urn:isa:authority:misa.

3.2.5 Federal Entity Originated Information Data Stewardship

To ensure that sensitive information is removed, DHS removes and replaces STIX identifiers (ID) for all information to be shared via AIS prior to dissemination. Note that DHS does not update relationship identifiers where the new STIX document refers to a DHS-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 maintains traceability between those IDs and the DHS-assigned IDs and appropriately substitute IDs before dissemination to non-Federal entities.

4 Federal to Federal Flow for Cyber Threat Indicators and Defensive Measures

There are two types of flows of information from Federal entities that are disseminated to other Federal entities. In the first case, the information is shared with DHS as described in Section 3.1 for brokering and dissemination to the non-Federal entities. Section 4.1 describes the differences in processing for this information before it is disseminated to other Federal Entities. In the second case, Federal entities can share information directly to other Federal entities that are members of the Federal Cybersecurity Information Sharing Community by signing the MISA. This flow, described in Section 4.2, does not undergo privacy filtering, processing, or brokering by DHS.

4.1 Federal Entity to Federal Entity through AIS Processing

Figure 3 illustrated the Federal entity to Federal entity through AIS processing flow in addition to the Federal entity to non-Federal entity flow. The processing for the Federal entity information that is disseminated to Federal entities is slightly different than that performed for non-Federal submissions or for non-Federal dissemination. Federal entity originated information is tagged with ACS markings. However, by processing and modifying the document, including the identifiers, DHS becomes the responsible entity for the information.

In the initial capability, DHS does not process the entire set of ACS markings or provide support for field level markings. In the future, DHS will update the brokering capability to include the ISA ACS markings for default and most restrictive marking (per ACS) plus field level markings.

For this use case, DHS processing includes:

- DHS processes the document through the AIS profile to remove or forward to human review any attributes with a risk of containing privacy information. This is the same processing that is conducted on CTI/DM destined for the non-Federal community;
- DHS replaces all identifiers within the document prior to further sharing to Federal entities. This includes all STIX attribute identifiers but does not include identifiers found in text strings such as the Controlled Structures within the document.
- DHS replaces the submitted timestamp information with new timestamp information when it assigns new identifiers.
- DHS replaces the organization name within the STIX Information Source with USA.USG.
- DHS replaces the Responsible Entity information with CUST:USA.DHS.US-CERT and either ORIG:USA.USG or ORIG:NONFED based on the submitted value.
- DHS replaces the ingested authority information with an authority value for AIS.
- DHS translates the ACS markings from the ingested document to the output document in accordance with Tables 4-1 and 4-2.
- DHS does not process field level markings with this interim brokering capability. Therefore, Federal entities must ensure that all of the information submitted in the document is marked at the most restrictive level.

- Table 4-1 and 4-2 describe the expected ingested ACS values and their related translated outbound values. Unless otherwise noted, the expected ingested values are the only values expected. The AIS capability will drop any submissions that contain unexpected values.

Table 4-1 Federal to Federal AIS Processed Translations (FD:PUBREL)

Ingested Attribute	Expected Ingested Value	Ingested Markings Acceptance Notes and Variances	Outbound Attribute	Outbound Value
Access Privilege			Access Privilege	
privDefault	deny -or- permit	If privdefault=deny, only a specific privilegeAction of CISAUSES will be accepted. If privdefaul=permit, the outbound privDefault will be set to deny and the CISAUSES action specifically permitted.	privDefault	deny
privilegeAction	CISAUSES		privilegeAction	CISAUSES
privilegeScope	ALL		privilegeScope	ALL
ruleEffect	permit		ruleEffect	permit
Control Set	CLS:U FD:PUBREL FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT	CLS:U and FD:PUBREL must be present. Optionally, FD: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT may be present.	Control Set	CLS:U FD:PUBREL FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
FurtherSharing	Default=permit		FurtherSharing	Default=permit
Identifier	isa:guide.19001.xxx	An identifier value is provided by the submitting organization in the ACS format. DHS replaces the identifier with an NCCIC identifier.	Identifier	NCCIC:xxx
ResponsibleEntit	CUST:USA.XXXORIG:US	Acceptable CUST and ORIG values are	ResponsibleEntit	CUST:USA.DHS.US-

Ingested Attribute	Expected Ingested Value	Ingested Markings Acceptance Notes and Variances	Outbound Attribute	Outbound Value
y	A.XXX	included in Appendix F. DHS replaces the ingested values with CUST:USA.DHS.US-CERT and ORIG:USA.USG or ORIG:NONFED.	y	CERT ORIG:USA.USG -or- CUST:USA.DHS.US-CERT ORIG:NONFED
CreateDateTime	2016-04-26T01:41:43Z	The CreateDateTime value is variable as assigned by the submitting organization. DHS replaces the CreateDateTime.	CreateDateTime	2016-04-26T01:43:21Z
AuthRef	urn:isa:authority:misa	Alternate authority references are permitted. DHS will replace any authority reference with the AIS reference.	AuthRef	urn:isa:authority:ais

Table 4-2 Federal to Federal AIS Processed Translations (FD:AIS and FD:FOUO)

Ingested Attribute	Ingested Value	Ingested Markings Acceptance Notes and Variances	Outbound Attribute	Outbound Value
Access Privilege			Access Privilege	
privDefault	deny -or- permit	If privdefault=deny, only a specific privilegeAction of CISAUSES will be accepted. If privdefaul=permit, the outbound privDefault will be set to deny and the CISAUSES action specifically permitted.	privDefault	deny
privilegeAction	CISAUSES		privilegeAction	CISAUSES
privilegeScope	ALL		privilegeScope	ALL
ruleEffect	permit		ruleEffect	permit
Control Set	CLS:U FD:AIS FD:FOUO FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT	CLS:U and FD:AIS and FD:FOUO must be present. Optionally, FD: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT may be present.	Control Set	CLS:U FD:AIS FD:FOUO FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT
FurtherSharing	Default=deny		FurtherSharing	Default=deny
sharingScope	USA.USG		sharingScope	USA.USG
ruleEffect	permit		ruleEffect	permit
Identifier	isa:guide.19001.xxx	An identifier value is provided by the submitting organization in the ACS format.	Identifier	NCCIC:xxx

Ingested Attribute	Ingested Value	Ingested Markings Acceptance Notes and Variances	Outbound Attribute	Outbound Value
		DHS replaces the identifier with an NCCIC identifier.		
ResponsibleEntity	CUST:USA.XXXORIG:USA.USG	Acceptable CUST and ORIG values are included in Appendix F. DHS replaces the ingested values with CUST:USA.DHS.US-CERT and ORIG:USA.USG or ORIG:NONFED.	ResponsibleEntity	CUST:USA.DHS.US-CERT ORIG:USA.USG -or- CUST:USA.DHS.US-CERT ORIG:NONFED
CreateDateTime	2016-04-26T01:41:43Z	The CreateDateTime value is variable as assigned by the submitting organization. DHS replaces the CreateDateTime.	CreateDateTime	2016-04-26T01:43:21Z
AuthRef	urn:isa:authority:misa	Alternate authority references are permitted. DHS will replace any authority reference with the AIS reference.	AuthRef	urn:isa:authority:ais

4.2 Federal Entity to Federal Entity with No DHS Processing

Federal Entity A creates a machine-readable document that they want to share with Federal entities without processing by DHS. Federal Entity A marks the STIX document with ACS tags, and, using their TAXII client, pushes the document to the DHS-hosted TAXII server (see Figure 4: Federal Entity Indicator Sharing with Federal Entity):

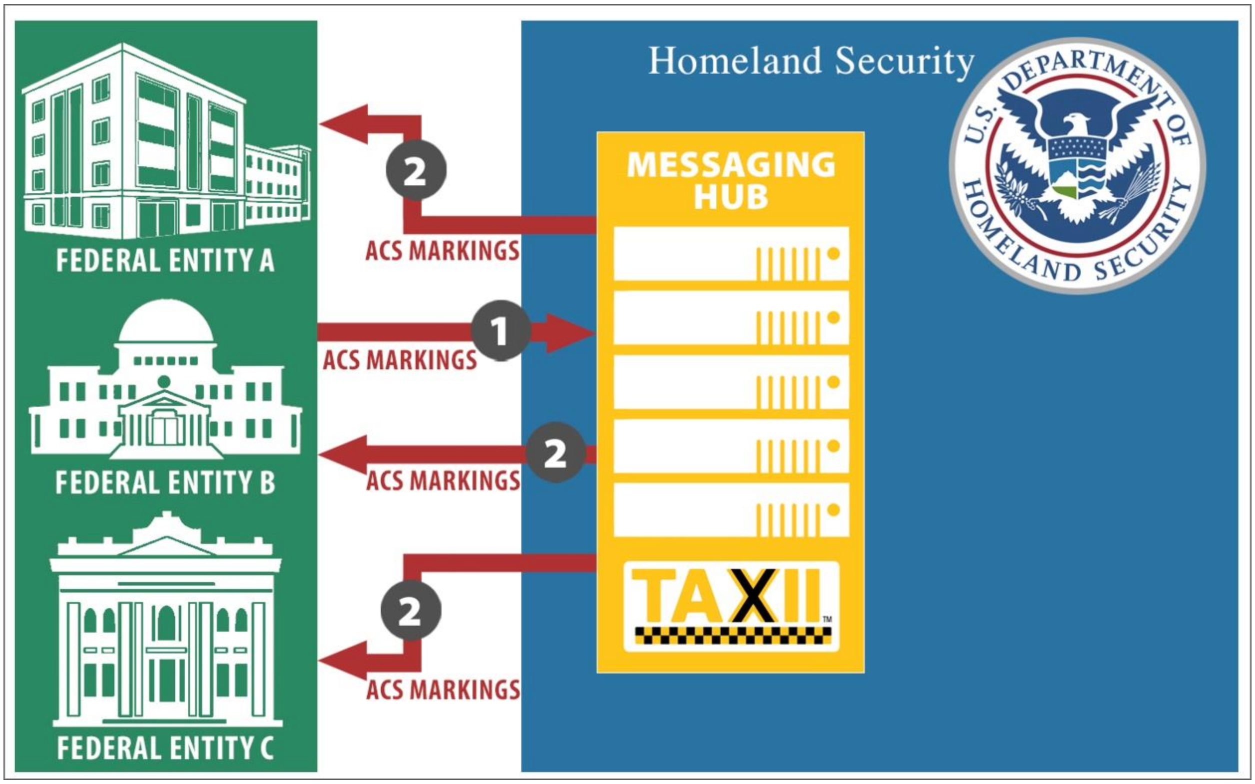


Figure 4: Federal Entity Indicator Sharing with Federal Entity

1. Federal Entity A publishes indicator (with ACS) to DHS-hosted messaging hub.
2. Using a TAXII client, consumers (Federal entities) receive the STIX formatted document with ACS markings for processing.

No processing or marking translations take place at DHS to enable this exchange of information.

In the initial capability, the Messaging hub/TAXII server does not have the capability to enforce ACS markings or provide support for field level markings. Therefore, all information shared by Federal entities must be shareable with all other Federal entities that have been granted access to subscribe to the TAXII server. **No data flows with ACS markings restricting access to a sub-set of Federal entities should be published by Federal entities at this time.** In the future, DHS will update the TAXII capability to process ISA ACS markings either through the TAXII protocol or using additional data flow management strategies.

5 Appendix A: Acronyms

Acronym	**Definition**
ACS	Access Control Specification
AIS	Automated Indicator Sharing
CISA	Cybersecurity Information Sharing Act of 2015
CTI	Cybersecurity Threat Indicator
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DM	Defensive Measure
DOD	Department of Defense
ESSA	Enhance Shared Situational Awareness
FBI	Federal Bureau of Investigations
FD	Formal Determination
FE1	Federal Entity 1
ID	Identifiers
ISA	Information Sharing Architecture
MISA	Multi-lateral Information Sharing Agreement
NCCIC	National Cybersecurity and Communications Integration Center
NSA	National Security Agency
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PUBREL	Publicly Releasable
SCP	Shared Capability Provider
STIX™	Structured Threat Information eXpression
TAXII™	Trusted Automated eXchange of Indicator Information
TBD	To Be Determined
TLP	Traffic Light Protocol
USG	United States Government
SD-EDH	Smart Data - Enterprise Data Header

6 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)

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.

7 Appendix C: Hyperlinked References

Document	Purpose	Link
"Information Sharing Architecture (ISA) Use of Structured Threat Information Expression (STIX™) and Profile Description," Version 2.0, May 15, 2015	Defines the ISA community agreed upon usage rules for the STIX data model, describes the ISA STIX profiles, and the application of the ISA Smart Data - Enterprise Data Header (SD-EDH) Cyber profile to STIX documents.	Max.gov
Information Sharing Architecture (ISA) STIX Profiles (numerous documents), May 2015	STIX profiles including the parent, malware, indicator, and incident profiles.	Max.gov
"Information Sharing Architecture (ISA) Access Control Specification," Version 3.0, February 2016	Specification of the data elements required to implement automated access control systems based on the relevant policies governing sharing between Federal entity participants	ISA Access Control Specification (ACS), Version 3.0, February, 2016
"Information Sharing Architecture (ISA) Shared Situational Awareness (SSA) Requirements Document," Version 2.1, October 21, 2013	Defines the enterprise-wide mission, technical, and information requirements to apply to current and future ISA Participants	ISA SSA Requirements Document, Version 2.1, October 21, 2013
"Enhanced Shared Situational Awareness Multilateral Information Sharing Agreement", March 2015	Agreement that establishes cybersecurity information sharing responsibilities for Federal entities	ESSA Multilateral Information Sharing Agreement, March 2015
"U.S. Department of Homeland Security Automated Indicator Sharing Terms of Use"	Terms and conditions for the non-Federal entities governing the use of Cyber Threat Indicators and Defensive Measures and the participation in the DHS AIS initiative	Automated Indicator Sharing Terms of Use
" Consolidated Appropriations Act, 2016, Division N – Cybersecurity Act of 2015, Title I - Cybersecurity Information Sharing," December 2015	Also known as the CISA and starting on page 1728 of the appropriations act, starts the definitions and regulations of cybersecurity information sharing of cyber threat indicators and defensive measures between the Federal and non-Federal entities	Cybersecurity Act of 2015
"Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensice	Co-developed by DHS and the Department of Justice, this document establishes the procedures relating to the receipt of CTIs/DMs by all Federal	Final Procedures Related to the Receipt of Cyber Threat

Document	Purpose	Link
*Measures by the Federal Government", June 15, 2016	entities	Indicators and Defensive Measures by the Federal Government
"Privacy and Civil Liberties Final Guidelines Cybersecurity Information Sharing Act of 2015", June 15, 2016	Co-developed by DHS and the Department of Justice, this document establishes the privacy and civil liberties guidelines governing the receipt, retention, use and dissemination of CTIs by a Federal entity	Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015
"Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with the Federal Government under the Cybersecurity Information Sharing Act 2015", June 15, 2016	Co-developed by DHS and the Department of Justice, this document further assists non-federal entities who elect to share cyber threat indicators with the Federal Government to do so in accordance with the Act	Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with the Federal Government under the Cybersecurity Information Sharing Act 2015
"Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act 2015", February 16, 2016	Co-developed by DHS, the Office of the Director of National Intelligence, the Department of Defense and the Department of Justice, this document describes the mechanisms through which the Federal entities share information with non-Federal entities.	Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015

8 Appendix D: TLP to ACS Markings for Developers

The tables below provide a resource for developers to understand how to apply the translations between the AIS marked STIX files and the required ACS markings.

If the AIS private-sector-originator uses a Proprietary marking (as allowed under the CISA), then the Caveat of CISAProprietary is included, otherwise it is not required.

TLP White to ACS Marking
ACS Default Marking:

```
   <edh2:ControlSet>CLS:U FD:PUBREL FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT[9] </edh2:ControlSet>

   <edh2:PolicyRef>urn:isa:policy:acs:ns:v3.0?privdefault=deny&amp;sharedefault=permit</edh2:PolicyRef>

  <edh2:AuthRef>urn:isa:authority:ais</edh2:AuthRef>

   <edh2:AccessPrivilege>

        <edh2:privilegeAction>CISAUSES</edh2:privilegeAction>

       <edh2:privilegeScope>ALL</edh2:privilegeScope>

       <edh2:ruleEffect>permit</edh2:ruleEffect>

   </edh2:AccessPrivilege>
```

[9] May potentially include CVT:CISAPROPRIETARY if the AIS Private Sector Originator set a Proprietary marking.

TLP White to ACS Marking

ACS Field Level Marking on Source ID:

with Consent=None

The source ID will be removed so no field level marking is required.

with Consent=Everyone

Same as Default so no need for field level marking on source ID

with Consent=USG

Field level marking on source identity will be the Most restrictive:

```
         <edh2:ControlSet>CLS:U ORG:USA.USG FD:INFORMATION-DIRECTLY-RELATED-TO-
CYBERSECURITY-THREAT [10] </edh2:ControlSet>

          <edh2:PolicyRef>urn:isa:policy:acs:ns:v2.1?privdefault=deny&amp;sharedefault=deny</edh2:PolicyRef>

          <edh2:AuthRef>urn:isa:authority:ais</edh2:AuthRef>

         <edh2:AccessPrivilege>

             <edh2:privilegeAction>CISAUSES</edh2:privilegeAction>

            <edh2:privilegeScope>ALL</edh2:privilegeScope>

           <edh2:ruleEffect>permit</edh2:ruleEffect>

   </edh2:AccessPrivilege>

   <edh2:FurtherSharing>

               <edh2:sharingScope>USA.USG</edh2:sharingScope>

               <edh2:ruleEffect>permit</edh2:ruleEffect>

</edh2:FurtherSharing>
```

[10] May potentially include CVT:CISAPROPRIETARY if the AIS Private Sector Originator set a Proprietary marking.

TLP Green to ACS Marking

ACS Default Marking:

```
 <edh2:ControlSet>CLS:U ORG:USA.USG FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT [11] </edh2:ControlSet>

  <edh2:PolicyRef>urn:isa:policy:acs:ns:v2.1?privdefault=deny&ampsharedefault=deny</edh2:PolicyRef>

  <edh2:AuthRef>urn:isa:authority:ais</edh2:AuthRef>

  <edh2:AccessPrivilege>

          <edh2:privilegeAction>CISAUSES</edh2:privilegeAction>

         <edh2:privilegeScope>ALL</edh2:privilegeScope>

        <edh2:ruleEffect>permit</edh2:ruleEffect>

  </edh2:AccessPrivilege>

 <edh2:FurtherSharing>

     <edh2:sharingScope>FOREIGNGOV</edh2:sharingScope>

     <edh2:ruleEffect>permit</edh2:ruleEffect>

  </edh2:FurtherSharing>

  <edh2:FurtherSharing>

     <edh2:sharingScope>SECTOR</edh2:sharingScope>

     <edh2:ruleEffect>permit</edh2:ruleEffect>

  </edh2:FurtherSharing>

  <edh2:FurtherSharing>

     <edh2:sharingScope>USA.USG</edh2:sharingScope>

     <edh2:ruleEffect>permit</edh2:ruleEffect>

  </edh2:FurtherSharing>
```

[11] May potentially include CVT:CISAPROPRIETARY if the AIS Private Sector Originator set a Proprietary marking.

TLP Green to ACS Marking (Continued)

ACS Field Level Marking on Source ID:

with Consent=Everyone

Same as the Default so no need for field level marking

with Consent=None

Source ID removed so no need for field level marking

with Consent=USG

Field level marking on source identity will be the Most Restrictive:

```
   <edh2:ControlSet>CLS:U ORG:USA.USG FD:INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT [12] </edh2:ControlSet>

   <edh2:PolicyRef>urn:isa:policy:acs:ns:v2.1?privdefault=deny&amp;sharedefault=deny </edh2:PolicyRef>

   <edh2:AuthRef>urn:isa:authority:ais</edh2:AuthRef>

   <edh2:AccessPrivilege>

            <edh2:privilegeAction>CISAUSES</edh2:privilegeAction>

           <edh2:privilegeScope>ALL</edh2:privilegeScope>

          <edh2:ruleEffect>permit</edh2:ruleEffect>

   </edh2:AccessPrivilege>

   <edh2:FurtherSharing>

       <edh2:sharingScope>USA.USG</edh2:sharingScope>

       <edh2:ruleEffect>permit</edh2:ruleEffect>

   </edh2:FurtherSharing>
```

[12] May potentially contain CVT:CISAPROPRIETARY if the AIS Private Sector Originator set a Proprietary marking.

TLP Amber to ACS Marking

The Default is the same as the marking for the source ID so no field level markings are required.

```
   <edh2:ControlSet> CLS:U ORG:USA.USG FD:INFORMATION-DIRECTLY-RELATED-TO-
        CYBERSECURITY-THREAT [13]</edh2:ControlSet>

   <edh2:PolicyRef>urn:isa:policy:acs:ns:v2.1?privdefault=deny&amp;sharedefault=deny</edh2:PolicyRef>

<edh2:AuthRef>urn:isa:authority:ais</edh2:AuthRef>

   <edh2:AccessPrivilege>

     <edh2:privilegeAction>CISAUSES</edh2:privilegeAction>

     <edh2:privilegeScope>ALL </edh2:privilegeScope>

      <edh2:ruleEffect>permit </edh2:ruleEffect>

</edh2:AccessPrivilege>

<edh2:FurtherSharing>

     <edh2:sharingScope>USA.USG</edh2:sharingScope>

     <edh2:ruleEffect>permit</edh2:ruleEffect>

 </edh2:FurtherSharing>
```

[13] May potentially contain CVT:CISAPROPRIETARY if the AIS Private Sector Originator set a Proprietary marking.

9 Appendix E: ACS to TLP Markings for Developers

DHS identifies information for dissemination to AIS from a Federal entity by one of the following ControlSet markings. If the Default Marking contains a formal determination of PUBRELL, DHS disseminates the information via AIS to non-Federal entities as TLP White. If the Default Marking includes a formal determination of For Official Use Only (FD:FOUO) and a Formal Determination of AIS, DHS removes the source information and disseminate the information via AIS to non-Federal entities as TLP Amber.

If the STIX file includes portions that are marked with more restrictive markings than those below, DHS removes those portions prior to dissemination based on the portion marking.

ACS Marking to TLP White
Default Marking must be: <edh2:ControlSet>CLS:U FD:PUBREL[14]</edh2:ControlSet>

ACS Marking to TLP Amber
Default Marking must be: <edh2:ControlSet> CLS:U FD:FOUO FD:AIS[15] </edh2:ControlSet>

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

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

10 Appendix F: CUST and ORIG values

Custodian Accepted Values	
USA.CIA	USA.DOD.USCYBERCOM-JOC
USA.CTIIC	USA.DOD.USMC
USA.DIA	USA.DOD.USN
USA.DHS	USA.DOD.USSTRATCOM
USA.DHS.CBP	USA.DOE
USA.DHS.ICE	USA.DOJ
USA.DHS.NCCIC	USA.DOJ.DEA
USA.DHS.NCSC	USA.DOJ.FBI
USA.DHS.TSA	USA.DOS
USA.DHS.USCG	USA.DOT
USA.DHS.US-CERT	USA.DOT.FAA
USA.DHS.USSS	USA.ED
USA.DISA	USA.EOP
USA.DNI	USA.GSA
USA.DNI.IC-SCC	USA.HHS
USA.DOC	USA.HUD
USA.DOC.NIST	USA.NASA
USA.DOD	USA.NCIJTF
USA.DOD.AFCYBER	USA.NGA
USA.DOD.ARCYBER	USA.NRO
USA.DOD.C10F	USA.NSA
USA.DOD.DC3	USA.NSA.NTOC
USA.DOD.MARFORCYBER	USA.SSA
USA.DOD.USA	USA.TREAS
USA.DOD.USAF	USA.USDA
USA.DOD.USCYBERCOM	USA.USG

Originator Accepted Values	
USA.CIA	USA.DOE
USA.CTIIC	USA.DOJ
USA.DIA	USA.DOJ.DEA
USA.DHS	USA.DOJ.FBI
USA.DHS.CBP	USA.DOS
USA.DHS.ICE	USA.DOT
USA.DHS.NCCIC	USA.DOT.FAA
USA.DHS.NCSC	USA.ED
USA.DHS.TSA	USA.EOP
USA.DHS.USCG	USA.GSA
USA.DHS.US-CERT	USA.HHS
USA.DHS.USSS	USA.HUD
USA.DISA	USA.NASA
USA.DNI	USA.NCIJTF
USA.DNI.IC-SCC	USA.NGA
USA.DOC	USA.NRO
USA.DOC.NIST	USA.NSA
USA.DOD	USA.NSA.NTOC
USA.DOD.AFCYBER	USA.SSA
USA.DOD.ARCYBER	USA.TREAS
USA.DOD.C10F	USA.USDA
USA.DOD.DC3	USA.USG
USA.DOD.MARFORCYBER	USA.AL
USA.DOD.USA	USA.AK
USA.DOD.USAF	USA.AZ
USA.DOD.USCYBERCOM	USA.AR
USA.DOD.USCYBERCOM-JOC	USA.CA
USA.DOD.USMC	USA.CO
USA.DOD.USN	USA.CT
USA.DOD.USSTRATCOM	USA.DC

Originator Accepted Values	
USA.DE	USA.PA
USA.FL	USA.RI
USA.GA	USA.SC
USA.HI	USA.SD
USA.ID	USA.TN
USA.IL	USA.TX
USA.IN	USA.UT
USA.IA	USA.VT
USA.KS	USA.VA
USA.KY	USA.WA
USA.LA	USA.WV
USA.ME	USA.WI
USA.MD	USA.WY
USA.MA	USA.AS
USA.MI	USA.GU
USA.MN	USA.MP
USA.MS	USA.PR
USA.MO	USA.SLTT
USA.MT	USA.STA
USA.NE	USA.TER
USA.NV	USA.TRB
USA.NH	USA.SLTT.FUSION
USA.NJ	CDC
USA.NM	CIKR
USA.NY	DIB
USA.NC	FIN
USA.ND	ISAC
USA.OH	NONFED
USA.OK	PRIVATESECTOR
USA.OR	