AUTOMATED INDICATOR SHARING (AIS) 2.0 SUBMISSION GUIDE

V1.0

Publication: November 2021
Cybersecurity and Infrastructure Security Agency

Table of Contents

1 Overview 3

2 Purpose 3

3 Definitions 3

4 Guidance on Creating STIX Submissions 4

4.1 Requirements for Creating STIX Submissions 4

4.2 Recommendations for Creating STIX Submissions 4

4.2.1 Recommendation 1 4
4.2.2 Recommendation 2 4
4.2.3 Recommendation 3 5
4.2.4 Recommendation 4 6
4.2.5 Recommendation 5 7
4.2.6 Recommendation 6 7
4.2.7 Recommendation 7 7
4.2.8 Recommendation 8 8
4.2.9 Recommendation 9 8
4.2.10 Recommendation 10 8
4.2.11 Recommendation 11 8

5 How to Share Submissions 8

6 Participant Identity Information 8

7 Proprietary Information 9

8 Personally Identifiable Information (PII) 9

9 Protected Critical Infrastructure Information (PCII) 9

10 Modifications of Submissions 10

11 Accidental Disclosure 10

12 CISA Contact and Administration Information 10

13 Appendix A - Acronyms 12

14 Appendix B – AIS Submission Samples 13

14.1 Non-Federal Submission of Malware 13

14.2 Non-Federal Submission of a Sighting 13

14.3 AIS PFTE Sample Data 13

1 Overview

The goal of Automated Indicator Sharing (AIS) is to achieve real-time sharing of cyber threat indicators (CTIs) and defensive measures (DMs) by enabling the Cybersecurity and Infrastructure Security Agency (CISA) to: 1) receive CTIs and DMs submitted by AIS participants and Federal Entities; 2) remove personally identifiable information (PII) that is not directly related to a cybersecurity threat; and 3) disseminate the CTIs and DMs to AIS participants and federal entities, as appropriate. Due to the nature of cyber threats, timely response and timely sharing is extremely important.

2 Purpose

The purpose of this document is to provide guidance for AIS participants when submitting CTIs and DMs in the Structured Threat Information Expression (STIX) format via the Trusted Automated Exchange of Intelligence Information (TAXII).[1]

3 Definitions

AIS Participant - a person, business, organization, non-Federal governmental body, or other non-Federal legal entity, foreign or domestic, that has accepted the *AIS Terms of Use (ToU).*[2]

All definitions from 6 U.S.C. § 1501[3], as applicable, are incorporated by reference. For convenience, the definitions for Cyber Threat Indicators and Defensive Measures from that section are included in full below:

Cyber Threat Indicators - information that is necessary to indicate, describe or identify:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- any combination thereof.

Defensive Measures – (A) Except as provided in subparagraph (B), an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by,

[1] https://oasis-open.github.io/cti-documentation/
[2] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[3] https://www.govinfo.gov/content/pkg/USCODE-2015-title6/html/USCODE-2015-title6-chap6-subchapI-sec1501.htm

or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

For more information, including examples of CTIs and DMs, please see the *Non-Federal Entity Sharing Guidance*.[4]

4 Guidance on Creating STIX Submissions

AIS participants will submit CTIs and DMs to AIS using the STIX format. Note that deviations from this guidance at a minimum could reduce the utility of the information for others and, worst case, may result in rejection of portions or all of the CTIs and DMs. The following subsections provide requirements and recommendations for how submissions should be prepared such that they conform to the STIX Specification and AIS functionality and are shared appropriately with other AIS participants.

The STIX Validator and the AIS Public Facing Test Environment (PFTE) may be used to check submissions for conformance with the STIX specification and AIS Profile, respectively.[5][6] Please see *AIS Public Facing Test Environment* for more information about the PFTE.[7] Examples of STIX submissions are also provided in Appendix B.

4.1 Requirements for Creating STIX Submissions

The set of requirements for STIX submissions to AIS are defined in the *AIS Profile*.[8] These requirements must be followed in all STIX submissions. Failure to follow these requirements will result in portions or all of the CTIs and DMs being rejected.

4.2 Recommendations for Creating STIX Submissions

In addition to the requirements described in 4.1, there is a set of recommendations that AIS participants should follow for STIX submissions. While failure to follow these recommendations will not result in portions or all of the CTIs and DMs being rejected, AIS participants should follow these recommendations to improve the usefulness of submissions.

4.2.1 Recommendation 1

For STIX object properties that leverage open vocabularies, it is **RECOMMENDED** that only values from the defined open vocabulary are used.

4.2.2 Recommendation 2

All STIX Domain Objects (SDOs), STIX Relationship Objects (SROs), and STIX Meta Objects (SMOs) **SHOULD** have their **created_by_ref** property populated with a reference to a producer Identity SDO. The referenced producer Identity SDO **SHOULD** be included in the submission. If the referenced producer Identity SDO is not included in the submission, the submission will be anonymized according to ais-consent-none. More

[4] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[5] https://github.com/oasis-open/cti-stix-validator
[6] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[7] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[8] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

information about the ais-consent-none label can be found in *AIS Identity Anonymization Process*.[9]

4.2.3 Recommendation 3

The producer Identity SDO **SHOULD** represent the organization creating the content being submitted to AIS. In addition to the required **name** property, the following properties **SHOULD** be filled in.

- **identity_class** with a value from the **identity-class-ov** open vocabulary that represents the class of identity.
- **sectors** with one or more values from the **industry-sector-ov** open vocabulary that describe the industry sector(s) to which that identity belongs.

When populating the **sectors** property, entities that are part of a designated Critical Infrastructure sector can use the table below, which shows the alignment of the defined STIX 2.1 **industry-sector-ov** values mapped to the designated Critical Infrastructure sectors under Presidential Policy Directive (PPD) 21.[10,11]

Submissions that include a **sector** property that is not listed below or is not defined in STIX 2.1 **industry-sector-ov** -- will be categorized as "Other"

Table 1: Sectors Property Mapping between PPD-21 and STIX 2.1 Open Vocabulary

PPD 21	STIX 2.1 industry-sector-ov
Food and Agriculture Sector	agriculture
Chemical Sector	chemical
Commercial Facilities Sector	commercial
	entertainment
	hospitality-leisure
	retail
Communications Sector	communications
	telecommunications
Critical Manufacturing Sector	manufacturing
Defense Industrial Base Sector	defense
Energy Sector	energy
	mining
Financial Services Sector	financial-services
	insurance
Emergency Services Sector	emergency-services
Government Facilities Sector	education

[9] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[10] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_oogrswk3onck
[11] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. See also https://www.cisa.gov/critical-infrastructure-sectors.

	government-local
	government-national
	government-public-services
	government-regional
Healthcare and Public Health Sector	healthcare
	pharmaceuticals
Dams Sector	dams
Nuclear Reactors, Materials, and Waste Sector	nuclear
Water and Wastewater Systems Sector	government-public-services
	water
Information Technology Sector	technology
	telecommunications
Transportation Systems Sector	aerospace
	automotive
	transportation
Other	non-profit

4.2.4 Recommendation 4

The producer Identity SDO **SHOULD** be labeled appropriately with an AIS Consent label. This label controls anonymization and defines the communities, if any, with which identity information will be shared. If no label is assigned, the AIS Consent label will default to ais-consent-none. If multiple labels are assigned, only the most restrictive label will be used. AIS Consent labels found on any STIX object other than an Identity object will be ignored. The possible AIS Consent labels are defined below.

Table 2: AIS Consent Label Options

AIS Consent Label	Description
ais-consent-none (default, most restrictive)	CISA will not disclose the submitter's identity, except as permitted in the AIS Terms of Use.
ais-consent-usg	CISA will only share the submitter's identity with Federal Entities.
ais-consent-everyone-cisa-proprietary	CISA will share the submitter's identity with all AIS participants and with Federal Entities. However, all objects in the submission that reference the Identity SDO are considered proprietary.
ais-consent-everyone (least restrictive)	CISA will share the submitter's identity with all AIS participants and with Federal Entities.

While AIS supports the STIX interpretation of an anonymous creator where the **created_by_ref** property is not

required (see Section 3.5 of the *STIX Version 2.1 Specification*), the sharing of identity information is encouraged to further provide value to other AIS participants. In the event that you only want to share your identity with CISA or the United States Government, the process outlined in *AIS Identity Anonymization Process* will be followed.[12]

Organizations should take care to be consistent with their use of AIS Consent labels when sending updates to previously published content. If the AIS Consent labels are inconsistent (e.g., the initial submission anonymized the identity and the follow-up submission did not anonymize the identity), it is possible that the anonymized identity could be exposed to all participants. If this happens, please see Section 11.0 Accidental Disclosure for instructions on how to remediate the situation.

4.2.5 Recommendation 5

The location of the producer Identity SDO **SHOULD** be provided via a Location SDO. The Location SDO **SHOULD** include the following properties:

- **country**: identifies the country associated with the submitter, using a valid International Organization for Standardization (ISO) 3166-1 ALPHA-2 code
- **administrative_area**: identifies the state, province, or other sub-national administrative area associated with the submitter using the ISO 3166-2 format

When a Location SDO is provided, an associated STIX Relationship Object **SHOULD** be provided with the following properties.

- **source_ref** with the STIX identifier of the Identity SDO
- **target_ref** with the STIX identifier of the Location SDO
- **relationship_type** with a value of "located-at"

STIX objects for common locations may be found in the STIX Common Objects repository.[13]

4.2.6 Recommendation 6

For submissions from non-Federal Entities, each SDO, SRO, and STIX Cyber-observable Object (SCO) **SHOULD** be marked with the appropriate Traffic Light Protocol (TLP) marking object as defined in Section 7.2.1.4 of the *STIX Version 2.1 Specification*.[14] Failure to mark submissions with a TLP marking object will default the submission to TLP Green. Note that these TLP marking objects do not need to be included in the submission as they are defined natively in STIX. Also, please note that TLP is the only supported data marking system in AIS for non-Federal Entities to ensure their submissions are shared correctly with other participants. More information about TLP can be found in the *TLP FIRST Standards Definitions and Usage Guidance - Version 1.0*.[15]

4.2.7 Recommendation 7

Each SDO, SRO, and SCO **SHOULD** be provided in English plain text where possible, unless the CTI itself is in a foreign language (e.g., if the text of a phishing email is in a foreign language). If the original CTI was in a foreign language, please note that in the description for the object and CISA will, to the extent the language is supported in AIS, provide a translated version in English using a STIX Language Content Meta Object to accompany the original CTI. For more information on how CTIs are translated, please see *AIS CTI Foreign*

[12] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[13] https://github.com/oasis-open/cti-stix-common-objects
[14] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_yd3ar14ekwrs
[15] https://www.first.org/tlp/

Language Translation Process.[16] In the event that personally identifiable information (PII) is detected in the translated version and is not determined to be directly related to a cybersecurity threat, CISA will not send out the original CTI in the foreign language. Instead, CISA will create a new CTI, in the foreign language, that is based on the English translation of the original CTI with PII removed.

4.2.8 Recommendation 8

It is **RECOMMENDED** that CTIs or DMs are shared as TLP White or Green to maximize the number of AIS participants with whom it can be shared.

4.2.9 Recommendation 9

It is **RECOMMENDED** that no proprietary information be submitted as TLP White, as TLP White information is permitted to be publicly released.

4.2.10 Recommendation 10

AIS participants are responsible for taking the steps necessary to conform with the requirements of the Cybersecurity Information Sharing Act of 2015. For example, prior to submission, AIS participants **SHOULD** remove all PII that is not directly related to a cybersecurity threat from the properties. Some PII may still be included in the submission if it is directly related to a cybersecurity threat (such as the email address of the sender of a phishing email). For further guidance on these requirements, see the *Non-Federal Entity Sharing Guidance*.[17]

Note that CISA will process each submission and, if PII is identified, only PII that is determined by CISA to be directly related to a cybersecurity threat will be retained and shared by CISA. CISA will conduct additional processing to remove PII not directly related to a cybersecurity threat prior to dissemination.

4.2.11 Recommendation 11

Proprietary information **SHOULD NOT** be included in SCOs because SCOs do not support the **created_by_ref** property and cannot be associated with an Identity object marking them as proprietary. As such, all SCOs submitted to AIS will be considered not proprietary.

5 How to Share Submissions

AIS provides several mechanisms by which you can share CTIs and DMs.

- **AIS STIX Submissions via TAXII:** AIS STIX format and TAXII are the preferred submission method. This requires that you have a TAXII 2.1 client. More information about signing up to connect to AIS can be obtained by contacting cyberservices@cisa.dhs.gov. Please note that TLP Red submissions will not be accepted or processed through AIS and must be submitted to CISA via email.
- **AIS STIX Submissions via Email:** AIS STIX format submissions may be sent via email to central@cisa.gov.
- **AIS Web Portal Submissions:** AIS submissions may be made via the web portal on the CISA website.[18]

6 Participant Identity Information

All submissions to AIS should include the identity of the AIS Participant making the submission. However, the AIS Participant controls how their identity is shared over AIS. AIS participants may specify that their identity is

[16] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[17] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[18] https://us-cert.cisa.gov/forms/share-indicators

not shared with anyone (except as permitted in the AIS ToU), is only shared with Federal Entities, or is shared with all AIS participants and Federal Entities. How to share identity information in STIX submissions is controlled by the ais-consent-none, ais-consent-usg, ais-consent-everyone-cisa-proprietary, and ais-consent-everyone labels defined in Section 4.2.4.

In addition, CISA recommends that where appropriate, the identified author of a STIX Note or Opinion object should be an organizational entity rather than a named individual.[19,20] If the author is a named individual, and that person is someone other than the submitter, the submitter should select ais-consent-usg or ais-consent-everyone only if the named author is aware their name is being submitted and has consented to their name being shared further with Federal Entities and/or all AIS participants, respectively. Selection of ais-consent-none will result in identifying information of the submitter and author (if any) being anonymized. Failure to select a consent label will default to ais-consent-none.

7 Proprietary Information

Consistent with the Cybersecurity Information Sharing Act of 2015 and any other applicable provision of law, a CTI or DM provided by a non-Federal entity to the Federal Government under the Act shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating non-Federal entity. STIX submissions are marked as proprietary via the ais-consent-everyone-cisa-proprietary label defined in Section 4.2.4. Please note that an SDO or SRO in a submission is proprietary if its **created_by_ref** property points to an Identity object that has the ais-consent-everyone-cisa-proprietary label set. Also, SCOs cannot be marked as proprietary because they do not have a **created_by_ref** property.

8 Personally Identifiable Information (PII)

CISA defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information linked or linkable to that individual, regardless of whether the individual is a United States (U.S.) Citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department. Some PII is not sensitive, such as that found on a business card. Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

Examples of PII that should not typically be in a submission include name, email, Social Security number (SSN), credit card number, phone number, or location encoded as latitude/longitude or in the Universal Transverse Mercator (UTM) system.

PII should not be submitted unless it is information that is directly related to a cybersecurity threat. AIS participants should remove all PII that is not directly related to a cybersecurity threat prior to submission of a CTI or DM.

CISA will process all CTIs and DMs shared within the Federal Government or with AIS participants for privacy, civil liberties, and other compliance concerns as otherwise required by law.

9 Protected Critical Infrastructure Information (PCII)

Critical Infrastructure Information (CII), which becomes PCII upon completion of the submission and validation

[19] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_gudodcg1sbb9
[20] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_ht1vtzfbtzda

process, is defined in the CII Act as: Information not customarily in the public domain and related to the security of critical infrastructure or protected systems – (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

At this time, AIS participants should not submit or share PCII through AIS as adequate marking and information protections schemes are not currently implemented; however, future AIS updates may allow for this capability.

AIS is not a mechanism to share PCII. If an AIS Participant has PCII (or CII that it wishes to have validated as PCII) to share, it may submit that information to the PCII Program Office or through a partnering federal agency. Please see the CISA website for additional information.[21]

10 Modifications of Submissions

All submissions to AIS are subject to modifications by CISA to ensure the proper sharing of CTIs/DMs as well as the protection of participant identity information and personally identifiable information.

When sharing between non-Federal and Federal entities, markings/labels (e.g., TLP and AIS Consent label) will be converted from TLP used by non-Federal entities to Access Control Specification (ACS) markings used by Federal Entities and vice versa. This also includes applying a TLP Green marking to objects submitted without a TLP marking.

11 Accidental Disclosure

In the event CTIs or DMs are disclosed by mistake, such as in error, or with an incorrect TLP marking, or if an anonymized identity has been exposed, CISA should be notified immediately at toll free 1-888-282-0870 or cyberservices@cisa.dhs.gov. All reasonable steps to mitigate, including sending a versioning update, will take place as soon as practicable, as stated in the ToU.

In the event personal information, which pertains to a U.S. person, has been shared by any government agency in violation of Cybersecurity Information Sharing Act of 2015, CISA should be notified immediately at toll free 1-888-282-0870 or cyberservices@cisa.dhs.gov. All reasonable steps to mitigate, including sending a versioning update, will take place as soon as practicable. Agencies should notify the affected person in a timely manner in accordance with their breach/incident response plan. For more information on how CISA identifies and reports privacy incidents, please reference the *CISA Privacy Incident Handling Guidance*.[22]

12 CISA Contact and Administration Information

If you have any questions concerning the submission or dissemination of CTIs or DMs, please send your

[21] https://www.cisa.gov/submit-cii-pcii-protection

[22] http://www.dhs.gov/sites/default/files/publications/privacy-incidence-handling-guide.pdf

questions using one of the following methods; email: cyberservices@cisa.dhs.gov or toll free 1-888-282-0870.

Changes to the Submission Guidance may be made without notice; however, AIS participants will receive updated copies as they are published.

For additional AIS information, please visit the AIS website.[23]

[23] https://www.cisa.gov/ais

13 Appendix A - Acronyms

Table 3: Acronyms

ACS	Access Control Specification
AIS	Automated Indicator Sharing
CII	Critical Infrastructure Information
CTI	Cyber Threat Indicator
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DM	Defensive Measure
IP	Internet Protocol
ISO	International Organization for Standardization
PCII	Protected Critical Infrastructure Information
PFTE	Public Facing Test Environment
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
SCO	STIX Cyber-observable Object
SDO	STIX Domain Object
SMO	STIX Meta Object
SRO	STIX Relationship Object
SSN	Social Security Number
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TLP	Traffic Light Protocol
ToU	Terms of Use
URL	Uniform Resource Locator
U.S.	United States
U.S.C.	United States Code
UTM	Universal Transverse Mercator

14 Appendix B – AIS Submission Samples

Below are sample AIS Submissions. Note that the TLP Marking Definition objects are defined in Section 7.2.1.4 of the *STIX Version 2.1 Specification*; therefore, they do not need to be included in the samples.[24]

14.1 Non-Federal Submission of Malware

Sample: Malware with known Internet Protocol (IP) address indicator ("192.168.101.52") and reference file. Malware communicates with a Uniform Resource Locator (URL) ("http://example.com/archive.bin") and an IP address ("192.168.100.54").

For the STIX content, please see the CISA website.[25]

14.2 Non-Federal Submission of a Sighting

Sample: Sighting of malware on the network with observed registry key data ("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MalK3y").

For the STIX content, please see the CISA website.[26]

14.3 AIS PFTE Sample Data

In addition to the above, there is also sample data in the PFTE that provides examples of different objects, relationships, and data markings, as well as what might be seen on the non-federal and federal feeds. More information about the PFTE can be found in the *AIS Public Facing Test Environment White Paper*.[27]

[24] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_yd3ar14ekwrs
[25] https://cisa.gov/publication/ais-stix-21-samples
[26] https://cisa.gov/publication/ais-stix-21-samples
[27] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation