Automated Indicator Sharing (AIS) Profile: Requirements for STIX Submissions

V1.0

Publication: October 2021
Cybersecurity and Infrastructure Security Agency

Contents

Overview 3

Purpose 3

Definitions 3

Requirements for STIX Submissions to AIS 4

Requirement 1 4

Requirement 2 4

Requirement 3 4

Requirement 4 4

Requirement 5 5

Requirement 6 5

Submission of Proprietary Information 5

Appendix A - Acronyms 6

OVERVIEW

The goal of Automated Indicator Sharing (AIS) is to achieve real-time sharing of cyber threat indicators (CTIs) and defensive measures (DMs) between non-Federal entities and Federal entities. By doing so, organizations are able to leverage the CTIs and DMs, known by other organizations, to proactively protect their networks against cyber threats.

PURPOSE

The purpose of this document is to define the formal set of submission requirements for AIS Participants when submitting CTIs and DMs to AIS using the Structured Threat Information Expression (STIX) format via the Trusted Automated Exchange of Intelligence Information (TAXII).[1] Note that previous versions were called *STIX Profile*; however, because STIX 2.1 has no concept of a "profile", the requirements that apply to AIS submissions are now referred to as the *AIS Profile*.

The set of requirements for AIS submissions defined in this document will be updated as needed. The AIS Profile Change Control Board will assess any changes to the requirements in this document.

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.

[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

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, 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]

REQUIREMENTS FOR STIX SUBMISSIONS TO AIS

The following sections define the requirements that AIS Participants must follow when submitting CTIs and DMs to AIS using the STIX format. Failure to follow these requirements will result in the rejection of portions or all of the CTIs and DMs in a submission.

Requirement 1

All STIX submissions **MUST** conform to the *STIX Version 2.1 Specification*.[5] If a STIX submission does not conform to the specification, it will be rejected.

Requirement 2

Submissions **MUST NOT** exceed 100 megabytes (MB). Submissions that exceed 100 MB will be rejected. Please note that if you have a large data set that you would like to share with the community (greater than 100 MB), please contact the TAXII Administrator taxiiadmins@us-cert.gov before publishing. This will allow us to plan accordingly for operational scaling, timing and support during the data load.

Requirement 3

For submissions from Federal entities, objects **MUST** be marked with an Access Control Specification (ACS) marking object as defined in the *ACS Marking Definition Version 3.0a for STIX™ Version 2.1* document.[6] Please note that ACS is the only supported data marking system in AIS for Federal Entities to ensure their submissions are shared correctly with other participants.

Requirement 4

STIX custom objects/properties and extensions **MUST NOT** be used in STIX submissions by non-federal entities, and should only be submitted by Federal entities (or those acting on behalf of federal entities) to support ACS data markings. If received, custom and extension objects will be rejected, and custom and extension properties will be stripped from the applicable objects in the submission. Extensions from Federal entities to support ACS markings, which **MUST** be used for submissions by Federal Entities (or those acting on behalf of Federal entities), are retained. If you would like for AIS to consider supporting additional extensions, please contact cyberservices@cisa.dhs.gov.

[4] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[5] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
[6] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

Requirement 5

The Incident STIX Domain Object (SDO) **MUST NOT** be used in STIX submissions as it is not currently supported in AIS. If received, Incident SDOs will be rejected. Support for the Incident SDO in AIS may be included at a later time, at which time the AIS Profile will be revised to reflect this update.

Requirement 6

The Artifact STIX Cyber-observable Object (SCO) **MUST NOT** be used in STIX submissions as it is not currently supported in AIS. If received, Artifact SCOs will be rejected. Support for the Artifact SCO in AIS may be included at a later time, at which time the AIS Profile will be revised to reflect this update.

SUBMISSION OF PROPRIETARY INFORMATION

For all submissions where the submitter intends to designate the information as commercial, financial, and proprietary in accordance with the Cybersecurity Information Sharing Act of 2015[7] (referred to as "CISA Proprietary"), such designation can only be indicated via inclusion of an Identity object in the submission with the ais-consent-everyone-cisa-proprietary label and where the applicable objects reference that Identity object with the **created_by_ref** property. Note that the CISA Proprietary information **SHOULD NOT** be submitted as SCOs, which do not have the **created_by_ref** property. Because SCOs cannot be designated as CISA Proprietary, CISA will not treat SCOs as CISA Proprietary. More information about the ais-consent-everyone-cisa-proprietary label can be found in *AIS Identity Anonymization Process*.[8]

[7] 6 U.S.C. § 1504(d)(2).
[8] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

APPENDIX A - ACRONYMS

Table 1: Acronyms

ACS	Access Control Specification
AIS	Automated Indicator Sharing
CTI	Cyber Threat Indicator
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DM	Defensive Measure
MB	Megabyte
SCO	STIX Cyber-observable Object
SDO	STIX Domain Object
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
ToU	Terms of Use
U.S.C.	United States Code