Automated Indicator Sharing (AIS) Frequently Asked Questions (FAQs)

V2.0

Publication: November 2021
Cybersecurity and Infrastructure Security Agency

Table of Contents

1 About AIS

1.1 Q. What are the major changes from AIS 1.0 to AIS 2.0?

A. AIS 2.0 includes the following new features:

- Support for Structured Threat Information Expression (STIX) 2.1 and Trusted Automated eXchange of Intelligence Information (TAXII) 2.1. The update to STIX 2.1 changes the format of submissions from the eXtensible Markup Language (XML) to the JavaScript Object Notation (JSON).
- A single ingest point for all STIX submissions. Previously, there were different ingest points for different AIS participants (e.g., federal vs. non-federal entities).
- A new status feature that enables submitters to determine the status of their submission (e.g., Did it validate correctly? Is it undergoing human review?). See FAQ 3.5.
- Instead of assigning a confidence score to participant submissions, CISA will enrich submissions from AIS participants by providing an opinion value score for non-CISA submitted Indicator objects based on the extent to which the submission is confirmed by or consistent with other sources. See FAQ 1.12.
- A filtering capability for participants to identify objects of interest.
- An enriched identity anonymization process that assigns unique anonymized identities to each organization indicating in their submission a request to be anonymous, such that other organizations can track submissions from the same anonymized organization over time. See FAQ 3.3.

1.2 Q. Why is it important for my organization to submit cyber threat indicators (CTIs) and defensive measures (DMs) and not just receive them?

A. The cyber threats facing or identified by the government can be different than the cyber threats facing or identified by the private sector.

When the government and the private sector share CTIs/DMs, everyone is better protected from a wider range of threats. That is, your detection becomes someone else’s prevention. AIS is one of the only programs that aggregates and shares CTIs and DMs observed by both public and private sector organizations. The more organizations can contribute to the collective awareness, the more we can support our collaborative defense effort.

1.3 Q. What will it cost my organization to participate in AIS?

A. CISA does not charge any fee for organizations to participate in AIS; however, there are costs (approximately $200) associated with purchasing a PKI certificate.

1.4 Q. Does my organization have to be based in the U.S. to participate in AIS?

A. No. Non-U.S. based organizations can participate in AIS. The goal is to share CTIs/DMs as widely as possible, so our adversaries have to change their behaviors, which subsequently increases their costs.

Please reach out to cyberservices@cisa.dhs.gov if interested in participating.

1.5 Q. If my organization participates in AIS, am I required to submit CTIs/DMs or can I just receive them?

A. Organizations aren’t required to submit CTIs/DMs through AIS and can only receive them if they prefer. However, CISA strongly encourages organizations to submit CTIs/DMs. See FAQ 1.2 above.

1.6 Q. How do I sign up to participate in AIS?

A. You can email cyberservices@cisa.dhs.gov to receive more information on the steps required to participate in AIS.

1.7 Q. How quickly will CISA share CTIs/DMs that my organization submits through AIS?

A. CISA shares information in real-time, with the exception of CTIs/DMs that require human review to exclude personally identifiable information (PII) not directly related to a cyber threat.

In these cases, the CTIs/DMs will be shared as fast as operationally possible upon completion of the review.

1.8 Q. Would participating in AIS be useful for small and medium-sized businesses?

A. Yes, but CISA recognizes that many small and medium-sized businesses are not in a position to invest in the equipment and technical personnel required to participate in AIS. If participation in AIS is not feasible, CISA encourages small and medium-sized businesses to submit CTIs/DMs to CISA via web form or email or share them with an Information Sharing and Analysis Center (ISAC) or Information Sharing and Analysis Organization (ISAO). Managed security service providers can also participate in AIS and use the CTIs/DMs they receive to protect their small and medium-sized business customers.

1.9 Q. Which versions of STIX and TAXII does AIS support?

A. AIS supports STIX 2.1 (JSON) and TAXII 2.1. While AIS participants transition to STIX/TAXII 2.1, AIS will continue to support STIX 1.1.1 (XML) and TAXII 1.1, to the extent reasonably practicable, through a legacy feed connection. Participants are encouraged to connect to AIS 2.0 and share STIX 2.1 content over TAXII 2.1. CISA will update AIS participants in advance of the legacy feed connection being discontinued. More information about the changes to STIX/TAXII can be found on the STIX/TAXII website.[1]

1.10 Q. What does AIS feed content look like?

A. AIS primarily shares individual, or groups of, CTIs/DMs but may also include full reports

[1] https://oasis-open.github.io/cti-documentation/

that themselves contain CTIs/DMs. At this time, AIS content may include any STIX 2.1 Object with the exception of the Incident object, Artifact object, Extension Definition object (with the exception of Access Control Specification data markings), and Custom Objects and Custom Properties as they are not currently supported.

1.11 Q. How does AIS enrich submissions?

A. AIS preserves all of the submitted data and enriches CTIs with an opinion value indicating if the CTIs could be confirmed with other sources.

1.12 Q. What is an opinion value?

A. CISA will provide an opinion value on all Indicator objects submitted to AIS. The opinion value is determined using the AIS Scoring Framework, which was developed by CISA based on the Admiralty score and indicates to what extent the Indicator object can be confirmed by or is consistent with other sources of information. For more information about the opinion value, how it is developed, and how it appears in AIS, please see *AIS Scoring Framework Used for Indicator Enrichment*.[2]

2 Connecting to AIS

2.1 Q. How can my organization submit CTIs/DMs though AIS?

A. To submit CTIs/DMs through AIS, an organization must:

- Agree to the AIS Terms of Use.
- Acquire their own TAXII client that will communicate with the CISA TAXII server.
- Purchase a PKI certificate from an approved Federal Bridge Certification Authority provider.
- Provide its IP address if doing an end-to-end connection to CISA so it can be allowlisted.
- Sign an Interconnection Security Agreement.

To get started, please contact cyberservices@cisa.dhs.gov. More information can also be found in the *CISA AIS TAXII Server Connection Guide for AIS 2.0*.[3]

2.2 Q. What does the AIS Terms of Use entail?

A. The *AIS Terms of Use* covers responsibilities for participants on handling and sharing of CTIs and DMs distributed through AIS based on their TLP markings.[4]

2.3 How can my organization acquire a TAXII client?

A. TAXII client functionality is already built into some commercial cybersecurity platforms and

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

free open-source clients exist.[5] CISA also provides a free GUI-based TAXII client.[6]

2.4 Q. How can my organization purchase a PKI certificate?

A. Organizations can purchase a PKI certificate from a commercial provider that is a Federal-Bridge Certification Authority (FBCA). Self-signed certificates are not allowed as there must be a trust agreement between the signing certificate authority and the U.S. Government.

2.5 Q. What does the Interconnection Security Agreement entail?

A. The *Interconnection Security Agreement* (ISA) lays out responsibilities for securing the connected systems and providing security points of contact for both CISA and the external organization so we are able to communicate with each other.[7]

3 Submitting to AIS

3.1 Q. What is the difference between the AIS Public, AIS Federal, and AIS CISCP feeds?

A. AIS is separated into three feeds: one for each trust group (Public, Federal, and CISCP).

- AIS Public is the feed for all AIS participating private sector entities; state, local, tribal, and territorial governments; Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs); and foreign partners and organizations.
- AIS Federal is the feed for federal departments and agencies.
- AIS CISCP is the feed for Cyber Information Sharing and Collaboration Program (CISCP) participating partners across the critical infrastructure sectors. For more information on the CISCP program, see cisa.gov/ciscp.

3.2 Q. If my organization submits information through AIS, with whom will CISA share them?

A. The distribution of AIS submissions from non-federal entities depends on the submitter-provided Traffic Light Protocol (TLP) markings[8] and the trust group with whom the submission is shared. AIS objects marked as TLP: White or Green will be shared with all AIS participants over the AIS Public feed. AIS objects submitted by non-federal participants and marked as TLP: Amber will only be distributed to the Federal feed. See FAQ 3.1. Submissions by federal departments and agencies that are marked for distribution via AIS will be distributed to all AIS participants. The identity of both federal and non-federal submitters, however, may be anonymized in accordance with submitter-provided markings. See FAQ 3.3. The following table captures how CTIs/DMs are shared. Federal partners should also consult the *AIS Brokering Between the Non-Federal Entities Sharing Community*

[5] https://github.com/oasis-open/cti-taxii-client

[6] https://github.com/cisagov/FLAREclient-UI

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

[8] https://www.first.org/tlp/

and the Federal Entities Sharing Community.[9]

	Source	TLP Level Shared	Goes to AIS Public Feed	Goes to Federal Feed
1	Federal Entity[10]	White, Green, Amber	Y	Y
2	Non-Federal Entity (AIS Public)	White, Green	Y	Y
3	Non-Federal Entity (AIS Public)	Amber	N	Y

Table 1: Source and TLP Levels

3.3 Q. Will my organization be identified as the source of the information I submit through AIS?

A. All submitter organizational identities are anonymized by default absent submitter consent to share its identity. CISA will not reveal the source of any AIS submissions unless the submitter requests that CISA reveal its name. For more information on how CISA anonymizes submitters' data or how submitters can control how their identity is shared, please refer to the *AIS Identity Anonymization Process*.[11]

3.4 Q. Should I provide a confidence score?

A. Participants are strongly recommended to share a confidence score associated with the objects they share. Please see *AIS Scoring Framework Used for Indicator Enrichment* for more information on how to apply and interpret a confidence score using this framework.[12]

3.5 Q. How do I get updates on the status of my submission?

A. AIS provides the AIS Status feature, which supports the ability to retrieve the status of a submission via TAXII. You can get information such as whether a submission is undergoing human review or failed validation, among other status updates. Please see the *AIS Status Service* for more information.[13]

3.6 Q. Is there any way for my organization to share CTIs/DMs with the government if I don't have a TAXII client?

A. Yes. You can share CTIs/DMs with CISA via web form (https://us-cert.cisa.gov/forms/share-indicators) or email (central@cisa.dhs.gov). See FAQs 3.7 and 3.8. However, CISA strongly recommends setting up a TAXII client and submitting CTIs/DMs through AIS so they can be shared in real time rather than having to be processed by

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

[10] Federal entities use Access Control Specification (ACS) data markings which are then shared out as TLP equivalents. More information can be found in *ACS Marking Definition Version 3.0a for STIX Version 2.1* and Table 7 of the *AIS Combined Brokering Document* (https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation).

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

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

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

human analysts. Organizations can also share CTIs/DMs with CISA though an ISAC or an ISAO that participates in AIS.

3.7 Q. Where is the web form used to submit CTIs/DMs located?

A. The web form is located at https://us-cert.cisa.gov/forms/share-indicators. However, CISA strongly recommends setting up a TAXII client and submitting CTIs/DMs through AIS rather than via web form so they can be shared in real time rather than having to be processed by human analysts.

3.8 Q. How can I email CTIs/DMs to CISA?

A. CTIs/DMs can be emailed to CISA Central at central@cisa.dhs.gov. However, CISA strongly recommends setting up a TAXII client and submitting CTIs/DMs through AIS rather than via email so they can be shared in real time rather than having to be processed by human analysts. If providing by email, please provide the following information: title; type (indicator or defensive measure); valid time of observation or knowledge of topic; tactics, techniques, and procedures (TTP); and a confidence score regarding the level of confidence in the value of the indicator (high, medium, or low).

4 Troubleshooting

4.1 Q. Who should I contact if I have problems receiving or sending CTIs/DMs through AIS?

A. You should email cyberservices@cisa.dhs.gov for engagement-related questions or taxiiadmins@us-cert.gov for technical and onboarding questions.

5 Participant Protections (Cybersecurity Information Sharing Act of 2015)

5.1 Q. Will my organization receive any sort of protections for sharing CTIs/DMs with the government via AIS?

A. Yes, provided sharing is conducted in accordance with all requirements set forth in the Cybersecurity Information Sharing Act of 2015 (CISA 2015). CISA 2015 grants liability protection, privacy protections, and other protections to organizations that share CTIs and DMs through AIS in accordance with CISA 2015's requirements. These requirements and protections are described in detail in the *Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015*.

5.2 Q. Will my organization receive liability protection and the other protections in CISA 2015 if I submit indictors via the CISA web form or email?

A. Yes, provided sharing is conducted in accordance with all requirements set forth in CISA 2015. For more details, see the *Non-Federal Entity Sharing Guidance under the*

Cybersecurity Information Sharing Act of 2015.[14]

5.3 Q. Will my organization receive liability protection and the other protections in CISA 2015 if I submit CTIs/DMs to an ISAC or an ISAO and they share them with CISA?

A. Both your sharing with an ISAC/ISAO and an ISAC/ISAO sharing with CISA are covered by liability protection and CISA 2015's other protections when done in accordance with the requirements set forth in CISA 2015. For more details, see the *Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015*.[15]

6 Further Sharing of the AIS Data

The following questions apply to companies that have signed the AIS TOU and provide cybersecurity services, including managed security service providers, antivirus vendors, other companies that protect customers' networks from cybersecurity threats, and cyber threat providers that share CTIs/DMs with customers as bulletins or within portals.

6.1 Q. I signed the AIS Terms of Use (TOU) and receive CTIs/DMs from CISA. Do all of my customers need to sign the TOU to use the CTIs/DMs?

A. No, they do not, with one exception. By signing the TOU, you are able to receive CTIs/DMs and provide them to your customers with the understanding that they must be handled in accordance with the information handling markings. The exception relates to your customers that are member-based organizations, such as ISAOs. These organizations, which will be re-disseminating information shared with the AIS Public feed, need to sign the TOU.

6.2 Q. Can I include AIS CTIs/DMs in one of my threat feeds? What about premium threat feeds or services?

A. You can either incorporate CTIs/DMs you receive through AIS into one of your product's threat feeds or explicitly label the feed as AIS and originating from CISA. However, in either case, you may not remove the AIS markings (to include TLP and whether the CTI/DM should be considered proprietary under CISA 2015). While you can bundle AIS CTIs/DMs as part of a premium threat feed or service, you cannot impose a monetary charge that is solely and specifically associated with the receipt of U.S. government-provided data. However, you can impose a monetary charge if you add value to the data.

6.3 Q. Can users of my platform or threat feed re-share AIS CTIs/DMs?

A. Re-sharing AIS CTIs/DMs depends on their markings. For example, CTIs/DMs marked as TLP:Amber cannot be further re-distributed, whereas those marked as TLP:White can be re-shared freely.

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

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