Homeland Security

AUTOMATED INDICATOR SHARING (AIS)

Q. Does the government want my company to submit cyber threat indicators?

A. Yes. We need you! All companies are encouraged to submit indicators via the Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) capability.

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

A. DHS does not charge any fee for companies to participate in AIS.

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

A. No. Non-U.S. based companies can participate in AIS. The goal is to share indicators as widely as possible so that our adversaries have to change their behaviors, which increases their costs.

Q. If my company participates in AIS, am I required to submit indicators, or can I just receive them?

A. Companies aren't required to submit indicators through AIS: they can just receive them if they prefer. However, we strongly encourage companies to submit indicators.

Q. Why is it important for my company to submit indicators and not just receive them?

A. The cyber threats facing the government can be different than the cyber threats facing the private sector. When both the government and the private sector share the indicators of those threats with each other, everyone is better protected from a wider range of threats.

Q. If my company submits indicators through AIS, who will DHS share them with?

A. The sharing of AIS indicators depends on their markings. For example, Traffic Light Protocol White or Green indicators will be shared with all AIS participants, to include other companies and private sector entities; federal departments and agencies; state, local, tribal, and territorial governments; Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs); and foreign partners and companies. However, only DHS will know who submitted the indicator unless you authorize us to share your identity further.

Q. Will my company be identified as the source of the indicators I submit through AIS?

A. No. Your anonymity is protected: we will not reveal the source of any indicators submitted through AIS, unless you ask us to reveal your name (some companies want credit).

Q. How quickly will DHS share indicators that my company submits through AIS?

A. Cyber threat indicators are composed of multiple fields of information. DHS has chosen a set of indicator fields to share through AIS, a small number of which may require human review to ensure that personally identifiable information (PII) that is not directly related to a cyber threat has not inadvertently been included. When such a field is included in an indicator submitted via AIS, an initial version of that indicator minus the field that requires human review will be shared with AIS participants immediately. As soon as the relevant field has been reviewed and determined not to contain any PII that is not directly related to a cyber threat or once any PII that is not directly related to a cyber threat has been removed, an updated version of the indicator will be shared with AIS participants to include the human-reviewed field. DHS is seeking to further automate this process where practicable.

Q. Are indicators shared through AIS given any type of risk score?

A. DHS assigns an automatically-generated risk score to some types of indicators it shares via AIS. Those indicators have a risk score set either by the submitting entity or by DHS. To start, we're primarily passing along the submitting entity's risk score, but over time, we plan to provide a DHS-derived risk score more often. Those DHS-derived scores will be a combination of the Department's confidence that the indicator is accurate and the severity of the threat.

Q. Is my company required to assign confidence levels to indicators I submit via AIS?

Yes, both Section 4 and Appendix B in the Submission Guidance provides the DHS guidance and standard for assigning the confidence level to indicators or defensive measure submissions.

Q. What type of context does DHS add to the AIS indicators to make them useful and actionable?

A. DHS includes technical context with each indicator with items like timestamps of when the indicator was last seen, the type of indicator, the critical infrastructure it has been reported in, etc. This technical context is meant to be used by tools and systems that can parse the AIS indicator and make decisions on what actions to take based on thresholds and priorities determined by entities receiving the indicators. However, DHS does not include cyber threat intelligence context (are the indicators part of a particular on-going campaign or tied to a potential threat actor) in AIS, but does do additional indicator vetting and sharing of cyber threat context for partners who are a member of our Cyber Information sharing and Collaboration Program (CISP).

Q. Will my company receive any sort of protections for sharing indicators with the government via AIS?

A. Yes. Companies that submit indicators through AIS in accordance with the requirements set forth in the Cybersecurity Act of 2015 receive liability protection. Additionally, indicators submitted via AIS are exempt from federal, state, tribal, and local disclosure laws including the Freedom of Information Act, federal anti-trust laws, and federal and state regulatory use. These requirements and protections are described in detail in the Non-Federal Entity Sharing Guidance, which can be found on:
www.us-cert.gov/ais.

Q. How can my company submit indicators though AIS?

A. In order to submit indicators through AIS, a company must agree to the AIS Terms of Use, acquire their own TAXII client (free open source clients are available) that will communicate with the DHS TAXII server, purchase a PKI certificate, provide its IP address to DHS so it can be whitelisted, and sign an Interconnection Security Agreement.

Q. What does the AIS Terms of Use entail?

A. The AIS Terms of Use covers responsibilities for participants on handling and sharing of indicators based on their markings (Traffic Light Protocol).

Q. How can my company acquire a TAXII client?

A. Companies that do not already have a TAXII capability can use the specification documentation to build their own, use the open-source DHS TAXII client available on GitHub, or purchase a commercial capability.

Q. How can my company purchase a commercial TAXII capability?

A. Some endpoint devices and products support TAXII natively, so companies can connect through those if they're already in their enterprise. Companies can also use a generic threat platform available through commercial vendors.

Q. How can my company purchase a PKI certificate?

A. Companies can purchase a PKI certificate from a commercial provider. No self-signed certificates are allowed.

Q. What does the Interconnection Security Agreement entail?

A. The Interconnection Security Agreement lays out responsibilities for securing the connected systems and providing security points of contact.

Q. Is there any way for my company to share indicators with the government if I don't have a TAXII client?

A. Yes. You can share indicators with DHS via web form and email. However, we strongly recommend setting up a TAXII client and submitting indicators through AIS. Companies can also share indicators with DHS though an Information Sharing and Analysis Center (ISAC) or an Information Sharing and Analysis Organization (ISAO).

Q. Where is the web form located?

A. The web form is located at **www.us-cert.gov/forms/share-indicators**. However, we strongly recommend setting up a TAXII client and submitting indicators through AIS rather than via web form.

Q. How can I email indicators to DHS?

A. Indicators can be emailed to the National Cybersecurity and Communications Integration Center (NCCIC) Customer Service Desk at **ncciccustomerservice@hq.dhs.gov**.

Please provide the following information: title; type (indicator or defensive measure); valid time of incident 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). However, we strongly recommend setting up a TAXII client and submitting indicators through AIS rather than via email.

Q. Will my company receive liability protection and would the other protections apply if I submit indictors via the DHS web form or via email?

A. Yes. For more details, see the Non-Federal Entity Sharing Guidance, which can be found on: **www.us-cert.gov/ais.**

Q. Would my company receive liability protection and would the other protections apply if I submit indicators to an ISAC or an ISAO and they share those indicators with DHS?

A. Both your sharing with an ISAC/ISAO and an ISAC/ISAO sharing with DHS are covered by liability protection when done in accordance with the requirements set forth in the Cybersecurity Act of 2015. For more details, see the Non-Federal Entity Sharing Guidance, which can be found on: **www.us-cert.gov/ais**.

Q. What is the preferred method of submitting indicators to DHS?

A. Submitting indicators through AIS rather than via web form or email is preferred as indicators can be shared immediately rather than having to be processed by human analysts.

Q. How many companies are expected to eventually participate in AIS?

A. AIS is starting off with a few trusted partners and will be slowly expanding over the next year or so. Eventually, the goal is to have hundreds of companies as well as ISACs and ISAOs sharing indicators.

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

A. Yes, but we recognize 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. However, we encourage small and medium-sized businesses to submit indicators to DHS via web form or email, or share them with an ISAC or ISAO. Managed security service providers can also participate in AIS and utilize the indicators they receive to protect their small and medium-sized business customers.

Q. Should my company participate in AIS instead of DHS's Cyber Information Sharing and Collaboration Program (CISCP), or vice versa?

A. We encourage companies to participate in both AIS and CISCP. AIS is machine-to-machine indicator sharing, whereas CISCP focuses on analyst-to-analyst collaboration. CISCP will add context to the indicators companies receive through AIS.

Q. What is the process for foreign partners to join AIS and connect to the DHS TAXII server?

A. Foreign partners' identities must first be verified before they can join AIS. Foreign partners will need to contact the Consular Notary at the U.S. Embassy in their home country to have their identity information verified. If the embassy does not have Consular Notary services, foreign partners will need to work with DHS to verify their identity. Once identity verification has been established and submitted to DHS, guidance to connect to the DHS TAXII server will be provided.

Q. Is it possible to relate the indicators shared in the AIS feed to a DHS product published on the US-CERT.gov website?

A. The original report or product might be conveyed using the package Title or Description. DHS generated reports place the original report or product name in either the STIX Package Title or Description, however, not all indicators shared through AIS or the TAXII server are contained in a report. And for content shared into AIS through external entities, it is up to that submitting organization on what they'd like to convey in the Title or Description.

Q. Can I find every Indicator Bulletin (IB) and Malware Initial Findings Report (MIFR) in either the AIS or CISCP feed?

A. All IBs and MIFRs should be in either the AIS or CISCP feed; however, AIS does not accept Traffic Light Protocol Red submissions. Any submissions marked Traffic Light Protocol Red will not be found in the AIS feed. Any submission from a Federal Entity, including US-CERT, marked Traffic Light Protocol White, Green, or Amber are shared via AIS TAXII feed. Any submission from a Non-Federal Entity, including AIS companies, CISCP organizations and international partner, marked Traffic Light Protocol White or Green will be shared via AIS TAXII feed.

Q. Is there overlap between the AIS and CISCP feeds?

A. There is possible overlap between AIS and CISCP feeds; however, CISCP maintains a human analytical process which AIS does not. Also, AIS contains community submissions, which might not get incorporated into CISCP.

Q. Who should I contact if I have problems receiving or sending indicators through AIS?

A. You should first email **ncciccustomerservice@hq.dhs.gov**. If they can't resolve your issue, email **taxiiadmins@us-cert.gov.**

The following questions apply to companies that have signed the AIS Terms of Use and provide cybersecurity services, including managed security service providers and antivirus companies and other companies that protect customers' networks from cybersecurity threats, as well as cyber threat providers that shares indicators with customers as bulletins or within portals.

Q. I signed the AIS Terms of Use and receive indicators (and defensive measures) from DHS. Do all of my customers need to sign the Terms of Use in order to use the indicators (and defensive measures)?

A. No, they do not, with one exception. By signing the Terms of Use, you are able to receive AIS indicators 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 member-based organizations, such as Information Sharing and Analysis Organizations. Such organizations, which will be re-disseminating the DHS AIS feed, need to sign the Terms of Use.

Q. Can I include AIS indicators in one of my threat feeds, or can I explicitly call the feed something like "DHS AIS Indicators?"

A. You can either incorporate indictors you receive through AIS into one of your product's threat feeds or explicitly label the feed as AIS and originating from DHS. However, in either case, you may not remove the AIS markings (to include Traffic Light Protocol and whether the indicator should be considered proprietary under the Cybersecurity Act of 2015) or any other fields defined in the AIS profile.

Q. Can I bundle AIS indicators as part of a premium threat feed or service?

A. Yes, but you cannot impose a monetary charge that is solely and specifically associated with the receipt of U.S. Government-provided data.

Q. Can users of my platform or threat feed re-share AIS indicators?

A. Re-sharing of AIS indicators depends on their markings. For example, Traffic Light Protocol Amber indicators cannot be further re-distributed.

Q. Some of the DHS indicators state "Under NCCIC Review", what does that mean?

A. Indicators with fields marked "Under NCCIC Review" are currently undergoing a review to determine 1) if there is PII or other sensitive information not directly related to the cyber threat that should be removed or 2) if there are any invalid values or formatting characters that do not meet the requirements for that specific field. Once the indicators have undergone this manual review, an updated indicator will be published using the same indicator ID and the "Under NCCIC Review" will be removed and replaced with the modified or sanitized information.

Q. What do the different values in the STIX document title mean?

A. DHS provides DHS generated content in AIS, while AIS contributors provide their own generated content. The only requirement is that all content must be restricted to the AIS STIX Profile (https://www.us-cert.gov/sites/default/files/ais_files/AIS_Submission_Guidance_Appendix_A.pdf). It is up to the submitting organization as to what they convey in the Title as long as the submission is in accordance with the AIS STIX Profile.

Following are some examples of the products and reports generated by DHS:
Indicator Bulletins (IBs) - (IB-YY-XXXX-Description)
Joint IBs (JIBs) - (JIB-YY-XXXXX-CC INC XXXXX) The CC may or may not be used.
Analysis Reports (ARs) - (AR-XX-XXXXX)
Joint ARs (JARs) - (JAR-XX-XXXXX – Description)
Malware ARs (MARs) - (MAR-XXXXXX)
Malware Initial Findings Reports (MIFRs) - (XXXXXX)
Technical Alerts (TAs) - (TA-XX-XXXX)