Homeland Security

AUTOMATED INDICATOR SHARING (AIS)

The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).

AIS is a part of the Department's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks. While AIS won't eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks. Ultimately, the goal is to commoditize cyber threat indicators through AIS so that tactical indicators are shared broadly among the public and private sector, enabling everyone to be better protected against cyber attacks.

WE NEED YOU!

The Federal Government is sharing indicators through AIS—but we always need more private sector companies to join to receive indicators and also to share indicators back with us!

HOW AIS WORKS

AIS participants connect to a DHS-managed system in the Department's National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber threat indicators. Each partner requires a technical capability (which can be built or bought from a number of commercial vendors) to allow them to exchange indicators with the NCCIC.

Participants will not only receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share back out to all AIS participants.

Participants who share indicators through AIS will not be identified as the source of those indicators to other participants unless they affirmatively consent to the disclosure of their identity. In other words, you are anonymous unless you want us to share your name.

Indicators are not validated by DHS as the emphasis is on velocity and volume: our partners tell us they will vet the indicators they receive through AIS, so the Department's goal is to share as many indicators as possible as quickly as possible. However, when the government has useful information about an indicator, we will assign a reputation score.

AIS leverages industry standards for machine-to-machine communication called STIX and TAXII. DHS initiated the development of these standards in 2012 and licensed them to the OASIS standards body in 2015 for their future continued evolution.

As you give us feedback about AIS, we will update it to make it even more useful to you.

THE CYBERSECURITY ACT OF 2015

AIS is available for free through the Department's NCCIC, a 24/7 cyber situational awareness, incident response, and management center which was designated as the central hub for the sharing of cyber threat indicators between the private sector and the Federal Government by the Cybersecurity Act of 2015. This legislation also grants liability protection and other protections to companies that share indicators through AIS.

As mandated by the Cybersecurity Act of 2015, the Department certified the operability of AIS in March 2016 and released guidance to help private sector entities share cyber threat indicators with the Federal Government. This guidance document can be found on www.us-cert.gov/ais.

Homeland Security

PRIVACY PROTECTIONS

DHS has taken careful measures to ensure appropriate privacy and civil liberties protections are fully implemented in AIS and are regularly tested. The Department has published a Privacy Impact Assessment of AIS, which can be found on www.us-cert.gov/ais.

To ensure that personally identifiable information (PII) is protected, AIS has processes which:

- Perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat;
- Incorporate elements of human review on select fields of certain indicators to ensure that automated processes are functioning appropriately;
- Minimize the amount of data included in a cyber threat indicator to the information that is directly related to a cyber threat;
- Retain only information needed to address cyber threats; and
- Ensure any information collected is used only for network defense or limited law enforcement purposes.

HOW TO PARTICIPATE IN AIS

AIS is available for free to all 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.

Steps:

1. Agree to a short Terms of Use.
2. Set up a TAXII client: build your own, use the open source DHS TAXII client, or purchase a commercial solution.
3. Technical connectivity activities: purchase a PKI certificate from a commercial provider, provide your IP address to DHS, and sign an Interconnection Security Agreement.
4. Connect directly to the DHS-managed system.

You can also share and receive indicators with DHS through a participating ISAC or ISAO or via a number of commercial products currently participating in AIS.

To get started right away, please visit www.us-cert.gov/ais.