Homeland Security

AUTOMATED INDICATOR SHARING INITIATIVE

The Department of Homeland Security (DHS) Automated Indicator Sharing (AIS) initiative meets the requirements set forth by Congress in the Cybersecurity Act of 2015 to create a mechanism for the real-time sharing of cyber threat indicators and defensive measures with both federal and non-federal entities.

REAL TIME CYBER DATA SHARING

AIS connects participating organizations to a DHS-managed system that allows bi-directional sharing of cybersecurity information, enhancing the ability of the Federal Government, DHS, and its partners to block cyber adversaries before intrusions occur. AIS will not only share government-developed indicators, but also will allow non-federal participants to share threat indicators they have observed in their own network defense efforts.

By sharing unclassified cyber threat indicators, DHS enables the detection, prevention, and mitigation of cyber threats. Sharing cyber threat indicators and defensive measures helps DHS build a more holistic understanding of cyber threat activity occurring across the 16 critical infrastructure sectors, the Internet, and the Federal Government.

AIS leverages DHS-led standards for machine-to-machine communication and lessons learned from existing DHS information sharing programs to build the framework for this capability. DHS will also utilize feedback from participants to strengthen its ongoing implementation.

The Cybersecurity Act also provides targeted liability protection to non-federal entities that share cyber threat information through AIS.

INFORMATION PROTECTION

DHS took careful measures to ensure appropriate privacy, civil liberties, and compliance protections are fully implemented and regularly tested.

DHS published a Privacy Impact Assessment detailing the risks identified with this capability and the mitigations implemented to address them.

What is a Cyber Threat Indicator?

Simply put, a cyber threat indicator is an observation or identified fact, combined with a hypothesis about a threat that can be used to focus cybersecurity measures. To apply a non-cyber metaphor:

- “James is experiencing a fever” is an observation, but not an indicator
- “James is experiencing a fever and probably has the flu” is the observation with a credible hypothesis on the cause – *an indicator* – where the flu is the *threat*.

While James may already have the flu, the threat indicator created about James’ predicament can be shared with the greater community, who can take measures to protect against the *threat* – such as getting a flu shot or stocking up on cold medicine.

When applied in a cyber context, a cyber threat indicator tells an individual about a cyber observable, such as a malicious file or email, and the threat associated with it – like whether it may attempt to hijack your computer.

To ensure personally identifiable information (PII) is protected, AIS has designed processes to:

- Perform automated analyses and technical mitigations to ensure that PII that is not directly related to the cyber threat is deleted before any information is shared;
- Incorporate elements of human review to ensure that automated processes are functioning appropriately;
- Minimize the amount of data included in a cyber threat indicator to information specifically needed to understand a cyber threat;
- Retain information for a limited amount of time, consistent with the need to address cyber threats; and
- Ensure any information collected is explicitly used for only purposes of cybersecurity, except in exceptional (law enforcement) circumstances.

Homeland Security

HOW TO CONNECT

The AIS initiative will be available to partners in critical infrastructure; the private sector; state, local, tribal, and territorial governments; federal departments and agencies; information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs); and foreign partners and companies. Interested organizations will need to agree to a Terms of Use to connect directly to DHS, but will also be able to connect through a participating ISAC or ISAO.

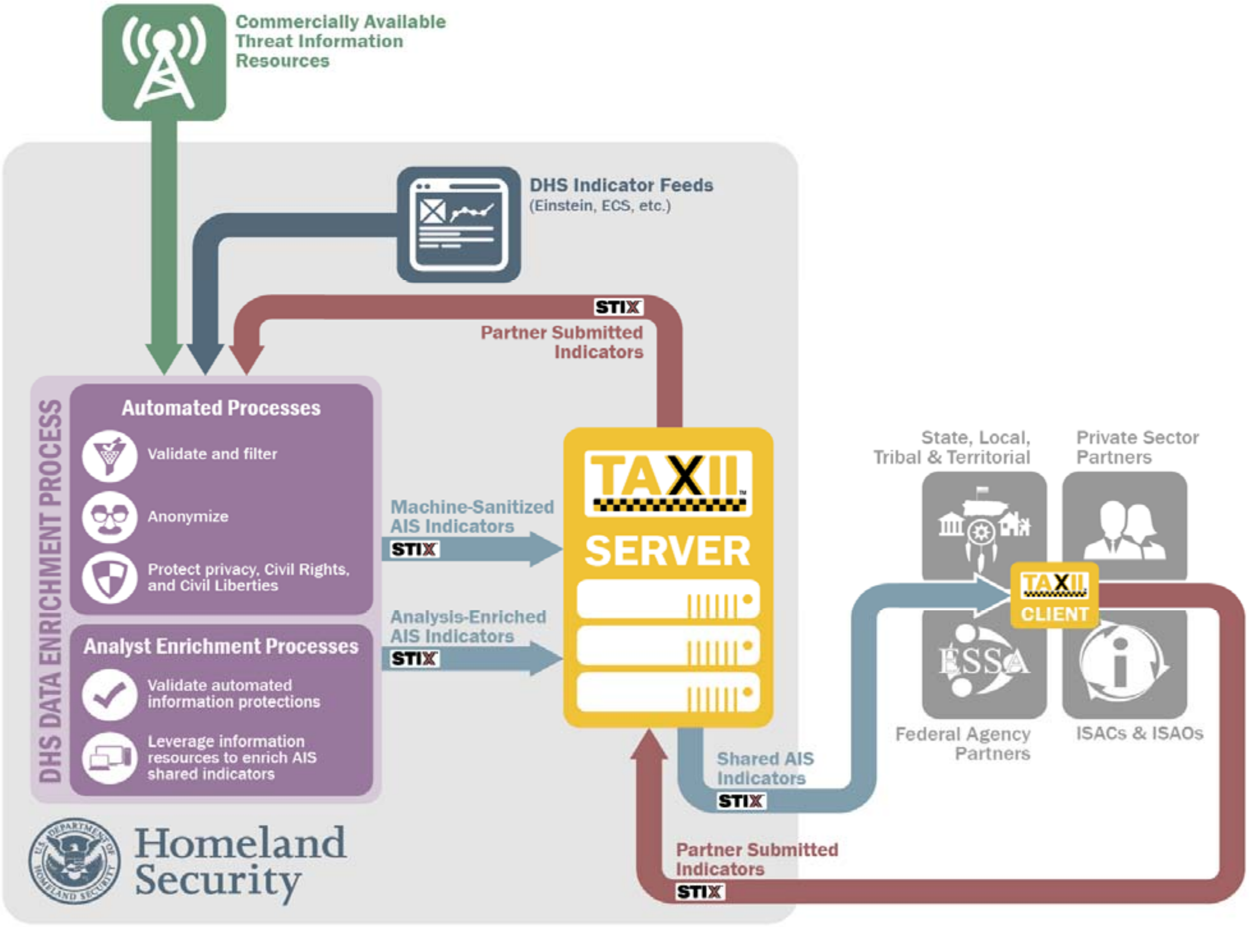
For more information, please visit www.us-cert.gov/ais.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information, please visit www.dhs.gov/cyber.

To view the DHS Privacy Impact Assessment, please visit www.dhs.gov/privacy.


Commercially Available Threat Information Resources
DHS Indicator Feeds
(Einstein, ECS, etc.)
STIX
Partner Submitted Indicators
DHS DATA ENRICHMENT PROCESS
Automated Processes
Validate and filter
Anonymize
Protect privacy, Civil Rights, and Civil Liberties
Analyst Enrichment Processes
Validate automated information protections
Leverage information resources to enrich AIS shared indicators
Machine-Sanitized AIS Indicators
STIX
Analysis-Enriched AIS Indicators
STIX
TAXII
SERVER
State, Local, Tribal & Territorial
Private Sector Partners
TAXII
CLIENT
ESSA
Federal Agency Partners
ISACs & ISAOs
Shared AIS Indicators
STIX
Partner Submitted Indicators
STIX
Homeland Security