



# Automated Indicator Sharing (AIS) Interconnection Agreement

## 1.0 Purpose

This Interconnection Agreement is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for the protection and handling of unclassified indicators between the DHS CISA and

For all issues associated with this agreement, the established points of contact are as follows:

| DHS Points of Contact  | External Organization Points of Contact |
|--|---|
| <b>Authorizing Official:</b> Robert Costello<br><a href="mailto:robert.j.costello@cisa.dhs.gov">robert.j.costello@cisa.dhs.gov</a><br>202-557-5873 |   |
| <b>System Owner:</b> Martin Gross<br><a href="mailto:martin.gross@hq.dhs.gov">martin.gross@hq.dhs.gov</a><br>703-235-2853                          |   |
| <b>ISSO(s) Lead:</b> N. Lopez-Zapata<br><a href="mailto:Nancy.Lopez-Zapata@cisa.dhs.gov">Nancy.Lopez-Zapata@cisa.dhs.gov</a><br>202-494-3496       |   |
| <b>ISSM:</b> MaryJayne Hambright<br><a href="mailto:maryjayne.hambright@cisa.dhs.gov">maryjayne.hambright@cisa.dhs.gov</a><br>850-982-1824         |   |
| <b>Program Manager:</b>  |   |
| <b>Primary POC: Admins</b><br><a href="mailto:taxiadmins@us-cert.gov">taxiadmins@us-cert.gov</a>   |   |

## 2.0 Justification

The goal of the Automated Indicator Sharing (AIS) initiative is to maximize, to the fullest extent possible, the near-real-time dissemination of all relevant and actionable cyber threat indicators among the private sector and Federal Departments and Agencies for cybersecurity purposes and within any statutory limitations, law enforcement purposes, while ensuring appropriate privacy and civil liberties protections. To do this, DHS CISA must be able to receive cyber threat indicators from individual private sector and government entities; filter sensitive information to ensure compliance with law; analyze the information for applicability to the purposes set forth in the legislation; and disseminate cyber threat indicators. To support this automated sharing, DHS CISA has deployed a Trusted Automated Exchange of Indicator Information (TAXII) server to share cyber threat data in the Structured Threat Information Expression (STIX) format.



### 3.0 Security Considerations

#### 3.1 General Information / Data Description

The DHS TAXII server is hosted in the Amazon Web Services (AWS) GovCloud region and connects to TAXII clients using Transport Layer Security (TLS) v1.2 & v1.3 to securely share cyber threat indicators in STIX format.

#### 3.2 Physical Security and Environmental Controls

Both organizations shall provide physical security and system environmental safeguards adequate to provide protection of the system components. Each organization is responsible for the physical security and environmental controls at their respective locations<sup>1</sup>.

#### 3.3 Data Sensitivity

The highest level of data that the DHS TAXII server processes is Sensitive but Unclassified. This may include Personally Identifiable Information (PII) that has been determined is necessary to understand the cyber threat and For Official Use Only indicators shared amongst DHS CISA and [EXTERNAL].

#### 3.4 Services Offered

The information set to be shared will be limited to unclassified STIX XML files that contain cyber threat indicators which have been approved to be shared and are properly marked with information handling controls. All communication is with **taxii.dhs.gov** over port **8443** using TLS v1.2 & v1.3 and Federal Bridge certificates to encrypt the messages in transit. The following TAXII feed will be used for submission of indicators: **AIS\_INGEST**. The following TAXII feed will be used for receiving indicators: **AIS**. Federal Departments and [EXTERNAL] will have separate TAXII publication and subscription feeds.

#### 3.5 Period of Operation

The connection will only be initiated and active when the external entity connects to the DHS TAXII server to submit a cyber threat indicator or receive the latest cyber threat indicators available to be retrieved. Routine maintenance for the DHS TAXII server will be coordinated ahead of time to ensure no loss of data or unwarranted disruption of service occurs. Any suspected deviation from expected, normal operations will be reported in a timely manner to the technical POC of the adjacent organization for verification, troubleshooting, or incident reporting.

#### 3.6 User Community

The external stakeholders of AIS may include Federal Departments and Agencies, foreign CERTs, and private sector companies. To participate in AIS, private sector and foreign CERTs must sign a Terms of Use agreement. Federal Departments and Agencies must sign the Enhance Shared Situational Awareness (ESSA) Multi-lateral Information Sharing Agreement (MISA).

#### 3.7 Information Exchange Security

Each organization will maintain the boundary protections to include firewalls, IDS/IPS, and any other perimeter protections required for their respective network as dictated by organization security policies.

---

<sup>1</sup> Physical and environmental safeguards of DHS-hosted components are fulfilled by AWS and have been independently audited to the Federal Risk and Authorization Management Program (FedRAMP) requirements.



Both organizations will ensure that (where appropriate) virus and spyware detection and eradication capabilities are used and that adequate system access controls (i.e., NIST 800-53) are in place and maintained on all components connected to the systems.

DHS CISA and the [EXTERNAL] shall protect the data in order to maintain confidentiality, integrity, and availability of the data and information systems. In order to connect to the DHS TAXII server, any external organization must be white-listed at the TAXII server firewall; therefore, static IP addresses or ranges are to be used by external organizations.

Specific protocols and ports that are needed to support this interconnection are provided in attachment A: Ports and protocols not specifically defined in Attachment A will be approved by DHS firewall change control procedures.

### 3.8 Trusted Behavior / Rules of Behavior

All users, to include system administrators, are expected to protect data in accordance with the policies, standards, and regulations specified for their respective system and programs and in accordance with the AIS Terms of Use or ESSA MISA.

### 3.9 Incident Reporting

Each organization will report any discovered security or privacy incidents regarding their TAXII connectivity in accordance with their own incident reporting procedures. The organization discovering a security incident will report it in accordance with the organization's incident reporting procedures and ensure that the other connecting organization is notified.

DHS TAXII personnel will be notified of any security incident that may have an operational or security impact on the AIS resources. Likewise, the [EXTERNAL] shall be notified of any security incident that may have an operational or security impact on the DHS CISA connected to [EXTERNAL].

| DHS Incident Reporting POCs  | External Org. Incident Reporting POCs |
|--|---------------------------------------|
| Martin Gross<br><a href="mailto:martin.gross@hq.dhs.gov">martin.gross@hq.dhs.gov</a><br>703-235-2853                                   |                                       |
| N.Lopez-Zapata<br><a href="mailto:Nancy.Lopez-Zapata@cisa.dhs.gov">Nancy.Lopez-Zapata@cisa.dhs.gov</a><br>202-494-3496                 |                                       |
| ISSM: MaryJayne<br>Hambright<br><a href="mailto:maryjayne.hambright@cisa.dhs.gov">maryjayne.hambright@cisa.dhs.gov</a><br>850-982-1824 |                                       |
| TAXII Administration Team<br><a href="mailto:Taxiiadmins@us-cert.gov">Taxiiadmins@us-cert.gov</a>                                      |                                       |



### 3.10 System Monitoring

Each organization is responsible for system monitoring of their own network and systems, in accordance with the policy and guidance prescribed through their own security processes.

### 3.11 Security Audit Trail Responsibility

Both parties are responsible for auditing system security events and log data related to this interconnection. At minimum, activities that should be recorded in logs will include: event type, date and time of event, system identification (e.g. hostname and/or IP address), success or failure of any access attempts and security actions taken by system administrators, security personnel, or automated systems. Organizations should retain logs according to their internal policies. Audit logs will be retained for 90 days online, and audit trail records shall be preserved for a period of at least seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.

### 4.0 Signatory Authority

This ISA is valid for three (3) years after the latest date on either signature listed below, if the technology documented herein does not change or if there are no other intervening requirements for updates. At that time, it must be reviewed, updated, and reauthorized. Either party may terminate this agreement with thirty days' advanced notice. Noncompliance on the part of either organization or its users or contractors with regards to security policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

**I agree to the above.**

|   |   |
|---|---|
| <b>DHS CISA</b>   |   |
| Robert Costello<br><a href="mailto:robert.j.costello@cisa.dhs.gov">robert.j.costello@cisa.dhs.gov</a> | <b>Print Name:</b>                      |
| <b>Signature (Digital or Physical):</b>   | <b>Signature (Digital or Physical):</b> |
|   |   |
| <b>Date (MM/DD/YYYY):</b>   | <b>Date (MM/DD/YYYY):</b>               |
|   |   |

**Submit**



**U.S. Department of Homeland Security**  
Cybersecurity & Infrastructure Security Agency  
*Cybersecurity Division (CSD)*  
Washington, DC 20528

## **Privacy Act Statement**

**Authority:** 44 U.S.C. § 3101 and 44 U.S.C. § 3534 authorize the collection of this information.

**Purpose:** DHS will use this information to establish a connection to the DHS Trusted Automated Exchange of Indicator Information (TAXII) Server and to maintain and share—with consent—contact information for you or your organization, should further correspondence be required regarding your cyber threat indicator submission through the Automated Indicator Sharing (AIS) initiative.

**Routine Uses:** This information may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70,792. Unless legally required, contact information will not be further disclosed without the express consent of the submitter. DHS will disclose to Federal law enforcement entities information provided through AIS that relates to threats or acts of terrorism, abuse of minors including sexual exploitation, and threats to physical safety, serious bodily harm, loss of life, or an attempt or conspiracy to commit any of the offenses just described.

**Disclosure:** Providing this information is voluntary, however, failure to provide this information will prevent you from establishing a connection with the DHS CISA TAXII.