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

Automated Indicator Sharing Interconnection Agreement

INSTRUCTION ON HOW TO COMPLETE THE INTERCONNECTION AGREEMENT

a. Replace field marked **[EXTERNAL ORGANIZATION]** with the name of the organization connecting with DHS. The external organization name is required to activate the Interconnection Agreement.

b. Provide Participating Organization Point of Contacts equivalent to the DHS Points of Contacts.

c. Return completed form to cyberservices@cisa.dhs.gov.

1.0 Purpose

This Interconnection Agreement is required by Federal and Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) policy and establishes individual and organizational security responsibilities for the protection and handling of unclassified indicators between CISA and _____ **[EXTERNAL ORGANIZATION]** _____, hereafter referred to as the "Participating Organization".

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

CISA Point of Contacts	**Participating Organization Point of Contacts**
Authorizing Official: Robert Costello	
System Owner: David Carroll David.Carroll@cisa.dhs.gov	
Risk Management Compliance Team / Information System Security Officers: CISA.CSD.ME_RMC@cisa.dhs.gov	
Information System Security Managers: CSD_ISSM_Team@cisa.dhs.gov	
Primary POC: AIS Service Team taxiiadmins@mail.cisa.dhs.gov (onboarding) cyberservices@cisa.dhs.gov (general questions)	

2.0 Justification

The goal of the Automated Indicator Sharing (AIS) service 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, and law enforcement purposes, while ensuring appropriate privacy and civil liberties

protections. To do this, 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, CISA has deployed an Automated Indicator Sharing environment to share cyber threat data in the Structured Threat Information Expression (STIX) format.

3.0 Security Considerations

3.1 General Information/ Data Description

The CISA AIS environment is hosted in the Amazon Web Services (AWS) GovCloud region and connects to AIS clients using Transport Layer Security (TLS) 1.2v and 1.3v 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[1].

3.3 Data Sensitivity

The highest level of data that the CISA AIS environment processes is Sensitive but Unclassified. This may include Personally Identifiable Information (PII) that has been determined necessary to understand the cyber threat and For Official Use Only (FOUO) indicators shared amongst CISA and the Participating Organization.

3.4 Services Offered

The information set to be shared will be limited to unclassified STIX 2.1 (JSON) 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 https://ais2.cisa.dhs.gov, port 443 with Federal Bridge certificates to encrypt the messages in transit.

The following AIS feed will be used for submission of indicators: **AIS_INGEST**

The following AIS feed will be used for receiving indictors: **PUBLIC, FEDERAL, CISCP**

3.5 Period of Operation

The connection will only be initiated and active when the external entity connects to the CISA AIS environment to submit a cyber threat indicator or receive the latest cyber threat indicators available to be retrieved. Routine maintenance for the CISA AIS environment 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 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

[1] 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.

perimeter protections required for their respective network as dictated by organization security policies.

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.

CISA and the Participating Organization shall protect the data to maintain confidentiality, integrity, and availability of the data and information systems. To connect to the CISA AIS environment, any external organization must be whitelisted at the AIS environment firewall; therefore, static IP addresses or ranges are to be used by external organizations.

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 AIS 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.

CISA AIS personnel will be notified of any security incident that may have an operational or security on the AIS resources. Likewise, the Participating Organization shall be notified of any security incident that may have an operational or security impact on AIS resources connected to the Participating Organization.

CISA Point of Contacts	**Participating Organization Point of Contacts**
System Owner: David Carroll David.Carroll@cisa.dhs.gov	
CSD/CD Risk Management Compliance Team / Information System Security Officers: CISA.CSD.ME_RMC@cisa.dhs.gov	
Information System Security Managers: CSD_ISSM_Team@cisa.dhs.gov	
AIS Administration Team: taxiiadmins@mail.cisa.dhs.gov	

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.

3.11Security Audit Trail Responsibility

Both parties are responsible for auditing system security events and log data related to this interconnection. Security audit trail activities carried out by CISA will be logged and will contain details such as the event

type, date and time of occurrence, system identification (such as hostname and/or IP address), access attempts' success or failure, and security measures taken by system administrators, security personnel, or automated systems. The Participating Organization should retain logs according to their internal policies.

4.0 Signatory Authority

This Interconnection Agreement 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 agreement.

CISA	**Participating Organization**
Robert J. Costello (CIO)	**Print Name:** **Email:**
Signature (Digital or Physical):	**Signature (Digital or Physical):**
Date (MM/DD/YYYY):	**Date (MM/DD/YYYY):**

Submit

Automated Indicator Sharing (AIS) Interconnection Agreement Privacy Act Statement

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

Purpose: The primary purpose for collection of information is to establish a connection to the Cybersecurity and Infrastructure Security Agency (CISA) Automated Indicator Sharing (AIS) environment. CISA may also use this information to contact you regarding your AIS cyber threat indicator or defensive measure submission.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659 and DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792.

Disclosure: Providing this information is voluntary, however, failure to provide this information will prevent you from establishing a connection to the CISA AIS environment.