CISA AIS
TAXII Server Connection Guide

Version 1.0

September 2021

Cybersecurity and Infrastructure Security Agency
Office of Cybersecurity and Communications
Capacity Building (CB) Division

Contents

Table of Figures

1 Purpose

The purpose of this guide is to document the formal requirements needed to successfully connect to the Cybersecurity and Infrastructure Security Agency (CISA Automated Indicator Sharing (AIS) Trusted Automated Exchange of Intelligence Information (TAXII) server. In addition, common questions and best practices are also provided to help support customers in successfully connecting to the TAXII server and enable polling of AIS Structured Threat Information Expression (STIX) Cyber Threat Indicators (CTI) and Defensive Measures (DM) content.

2 Preliminary Steps – Customer Requirements

CISA AIS TAXII server operates as a server/client relationship with end-users. In order to connect to the CISA AIS TAXII Server, customers will need to identify, and acquire, the following two core items: 1)TAXII 1.1 Compliant Client or Data Aggregator Commercial Service and 2) a "Medium Device Assurance Level" Client Certificate from an Approved Federal Bridge Certification Authority (FBCA) (not required if using a Data Aggregator commercial service).

2.1 Obtain a TAXII 1.1 Compliant Client or Data Aggregator Commercial Service

Customers will need a compliant TAXII client that can send valid TAXII "Poll_Request" messages to the AIS TAXII Server to pull AIS feed content. The client must also be able to authenticate the TAXII server connection using a Subscription ID and a SSL/TLS client public certificate provided by the customer.

2.1.1 Standalone TAXII 1.1 Compliant Client

Customers could implement a client within their internal infrastructure. (See *Appendix A for a List of Compatible TAXII Clients --)*

NOTE: Customers using any of the Compatible TAXII Clients will still need to obtain a PKI/TLS-medium certificate and provide CISA with static IP addresses that they will be using to connect to the TAXII Server

2.1.2 Data Aggregator Commercial Service

Customers could subscribe to a Data Aggregator Commercial Service to access the AIS feed content based on the community membership granted to that customer. For example: AIS PUBLIC, FEDGOV, and/or CISCP feeds. (See *Appendix B for a List of Data Aggregator Commercial Services* that are currently supporting access to the CISA AIS TAXII Server)

NOTE: Customers using a Data Aggregator Commercial Service to access the AIS TAXII Server to pull AIS feed content do not need to obtain a PKI/TLS-medium certificate or provide CISA with static IP addresses that they will be using to connect to the TAXII Server, as these are provided by the commercial service infrastructure. However, customers must still complete the AIS Terms of Use (TOU) document and return it to cyberservices@cisa.dhs.gov.

2.1.3 Data Aggregator Commercial Service with Associated Direct Client

Customers could subscribe to a Data Aggregator Commercial Service that allows the customer to directly access the AIS TAXII Server through the Data Aggregator Commercial Service infrastructure to pull AIS feed content. (See *Appendix B for a List of Data Aggregator Commercial Services*, with associated direct client, that are currently supporting access to the CISA AIS TAXII Server)

NOTE: Customers using a Data Aggregator Commercial Service – with associated client – to access the AIS TAXII Server to pull AIS feed content will need to obtain a PKI/TLS-medium certificate and complete the AIS Terms of Use (TOU) document. However, they will not need to provide CISA with the static IP addresses they will be using to connect to the TAXII Server.

2.1.4 Via an Available ISAC Member Data Aggregator Feed

Many ISACs provide AIS data to their members. Some ISACs provide both AIS Public and CISCP feed data in their data aggregator indicator feeds. Organizations who are members of an ISAC can request access to the AIS feeds if available.

2.2 Obtain a "Medium Device Assurance Level" Client Certificate from an Approved Federal Bridge Certification Authority (FBCA)

A FBCA approved client certificate is required for your TAXII Client to authenticate with the CISA AIS TAXII server. (See *Appendix C for a List of CISA Approved FBCA Vendors*)

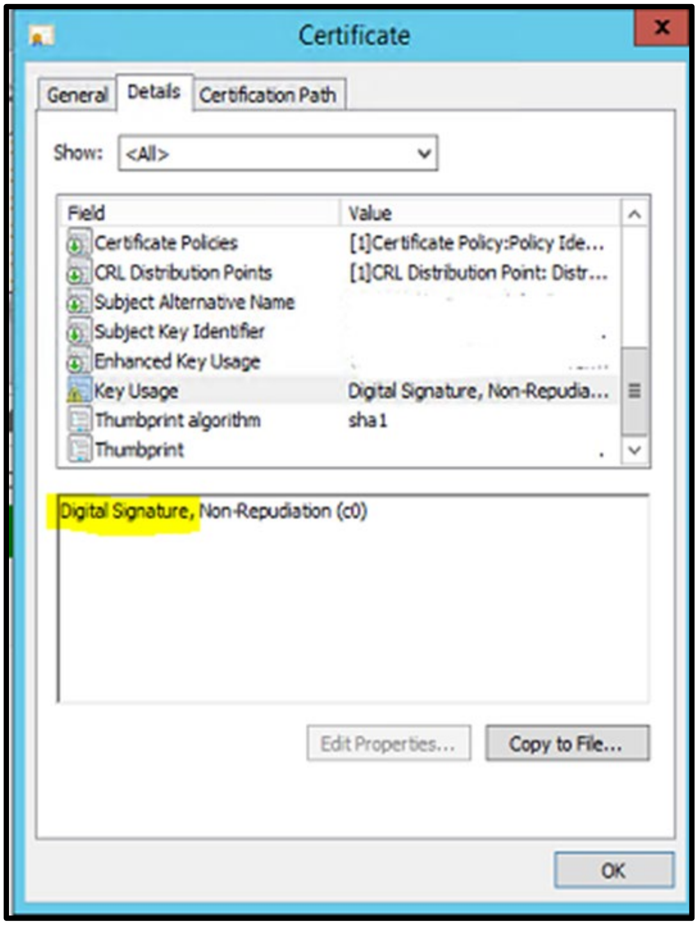
2.2.1 High Level Overview

A (very) high level overview of obtaining a "Medium Device Assurance Level" client certificate from an approved FBCA vendor:

- Select approved FBCA vendor
- Generate the Certificate Signing Request (CSR)
- Complete the online request
- Provide the vendor proof of your identity
- Download the issued certificate

2.2.2 Digital Signature

Once you receive your client certificate from an approved FBCA – please ensure that the certificate has "digital signature" enabled in the "Details" tab:



Show: <All>

Field	Value
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Subject Alternative Name	
Subject Key Identifier	
Enhanced Key Usage	
Key Usage	Digital Signature, Non-Repudia...
Thumbprint algorithm	sha1
Thumbprint	

Digital Signature, Non-Repudiation (c0)

Figure 1: Client Certificate – Digital Signature Enabled

3 Customer Requirements for Successful Connection to AIS TAXII Server

The following items are required by CISA to ensure a customer will successfully be able to connect to the AIS TAXII Server.

3.1 Customer IP Address(es) for TAXII Server Connection

CISA will need the explicit IP address(es) you will be using to connect (poll) the AIS TAXII Server to ensure your addresses are listed in our ALLOW list.

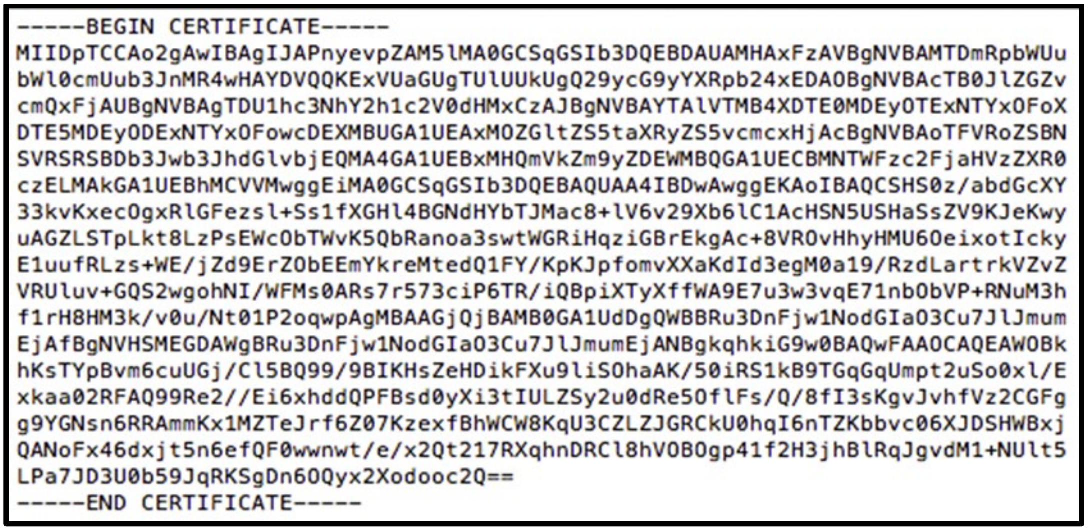
CISA recommends customers limit these to a maximum of 8 specific IP addresses.

Please do not provide IP CIDR ranges (such as: /16, /24, etc.) as we need the specific IP address(es) you will be connecting from within your network.

3.2 Customer SSL/TLS Client Public Certificate

CISA will need your SSL/TLS Client Public Certificate to ensure successful secure connection can be established with the AIS TAXII Server.

The SSL/TLS Client Public Certificate file should be in a ".PEM" or ".txt" format and only include the certificate itself.



```
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIJAPnyevpZAM5lMA0GCSqGSIb3DQEBDAUAMHAxFzAVBgNVBAMTDmRpbWUu
bWl0cmUub3JnMR4wHAYDVQQKExVUaGUgTUlUUkUgQ29ycG9yYXRpb24xEDAOBgNVBAcTB0JlZGZv
cmQxFjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxCzAJBgNVBAYTAlVTMB4XDTE0MDEyOTExNTYxOFoX
DTE5MDEyODExNTYxOFowcDEXMBUGA1UEAxMOZGltZS5taXRyZS5vcmcxHjAcBgNVBAoTFVRoZSBN
SVRSRSBDb3Jwb3JhdGlvbjEQMA4GA1UEBxMHQmVkZm9yZDEWMBQGA1UECBMNTWFzc2FjaHVzZXR0
czELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCSHS0z/abdGcXY
33kvKxecOgxRlGFezsl+Ss1fXGHl4BGNdHYbTJMac8+lV6v29Xb6lC1AcHSN5USHaSsZV9KJeKwy
uAGZLSTpLkt8LzPsEWcObTWvK5QbRanoa3swtWGRiHqziGBrEkgAc+8VROvHhyHMU6OeixotIcky
E1uufRLzs+WE/jZd9ErZObEEmYkreMtedQ1FY/KpKJpfomvXXaKdId3egM0a19/RzdLartrkVZvZ
VRUluv+GQS2wgohNI/WFMs0ARs7r573ciP6TR/iQBpiXTyXffWA9E7u3w3vqE71nbObVP+RNuM3h
f1rH8HM3k/v0u/Nt01P2oqwpAgMBAAGjQjBAMB0GA1UdDgQWBBRu3DnFjw1NodGIaO3Cu7JlJmum
EjAfBgNVHSMEGDAWgBRu3DnFjw1NodGIaO3Cu7JlJmumEjANBgkqhkiG9w0BAQwFAAOCAQEAWOBk
hKsTYpBvm6cuUGj/Cl5BQ99/9BIKHsZeHDikFXu9liSOhaAK/50iRS1kB9TGqGqUmpt2uSo0xl/E
xkaa02RFAQ99Re2//Ei6xhddQPFBsd0yXi3tIULZSy2u0dRe5OflFs/Q/8fI3sKgvJvhfVz2CGFg
g9YGNsn6RRAmmKx1MZTeJrf6Z07KzexfBhWCW8KqU3CZLZJGRCkU0hqI6nTZKbbvc06XJDSHWBxj
QANoFx46dxjt5n6efQF0wwnwt/e/x2Qt217RXqhnDRCl8hVOBOgp41f2H3jhBlRqJgvdM1+NUlt5
LPa7JD3U0b59JqRKSgDn6OQyx2Xodooc2Q==
-----END CERTIFICATE-----
```

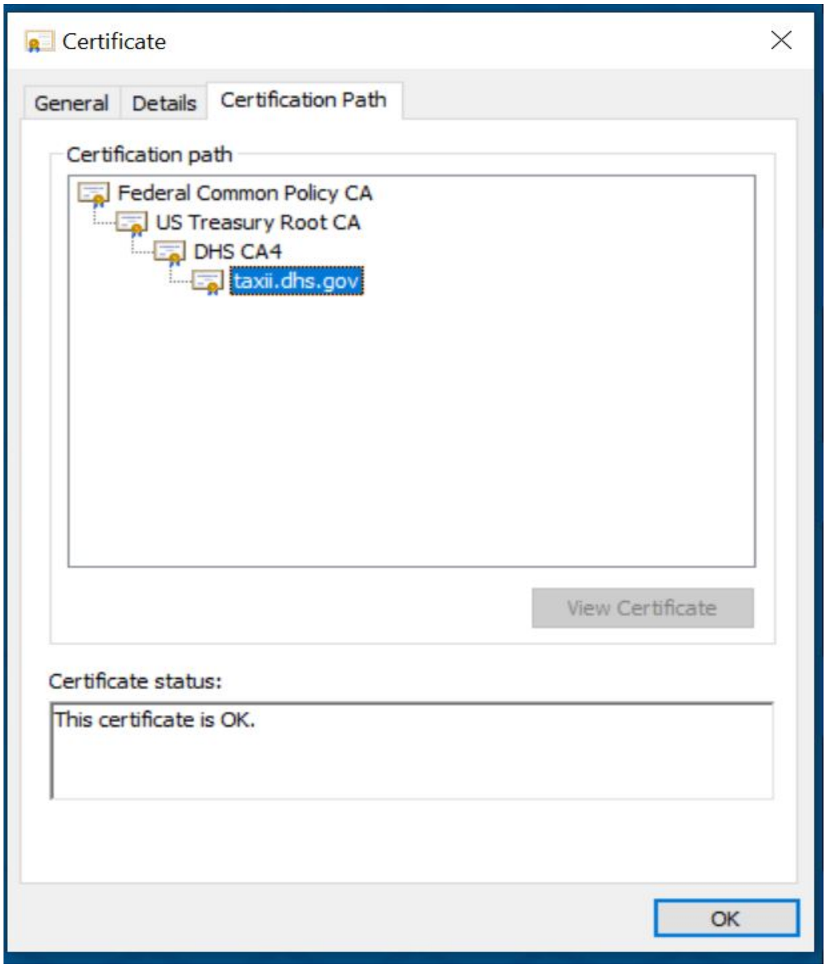
Figure 2: SSL/TLS Client Public Certificate PEM Format Example

3.3 Customer Certificate Authority (CA) Certificate and any Intermediate Certificates for your Client Certificate

CISA will need your Certificate Authority (CA) Certificate and any Intermediate Certificates associated with your FBCA vendor supplied SSL/TLS Client Public Certificate to ensure successful secure connection can be established with the AIS TAXII Server.

There may be one or more intermediate certificates associated with the client SSL/TLS certificate supplied by your selected FBCA CA vendor.

Use the same “. PEM” – or “.txt” – format as you used when sending your SSL/TLS Client Public Certificate to CISA.



Federal Common Policy CA
US Treasury Root CA
DHS CA4
taxii.dhs.gov

Certificate status:

This certificate is OK.

Figure 3: Certificate Authority (CA) and any Intermediate Certificates Example

3.4 Signed Interconnection Agreement

To ensure you and CISA have the proper security Points of Contacts (POCs) -- a completed and signed Interconnection Agreement is needed. (Please see *Appendix D Interconnection Agreement Template*)

3.5 Customer TAXII Client Implementation

If you are connecting directly to the AIS TAXII Server – this is the TAXII Client, you will be using to connect to the AIS TAXII Server. Please see *Appendix A for a List of Compatible TAXII Clients* – that we are aware of at the time of publication.

For Customer implemented TAXII Clients that CISA has not connected previously to the AIS TAXII Server -- additional interoperability testing may be necessary for successful connection.

4 CISA Provided Requirements for Successful Connection to AIS TAXII Server

The following items are provided by CISA to ensure a customer will successfully be able to connect and successfully authenticate to the AIS TAXII Server.

4.1 CISA AIS TAXII Server SSL/TLS Certificates

CISA will provide the AIS TAXII Server public SSL/TLS certificate (taxii.dhs.gov) and associated CA certificates.

4.2 TAXII Connection Authentication/ CISA AIS TAXII Server Data Feed(s) Subscription ID

CISA will provide the AIS TAXII Server Data Feed(s) Subscription Identification (ID) -- the subscription ID is associated with the specific AIS data feed. The subscription ID must be present in all TAXII Server "Poll_Requests" as the value of the "subscription_id" attribute.

An example AIS TAXII Server poll request is below:

```
<? Xml version=“1.0” encoding=“UTF-8” ?>

<taxii:Poll_Request xmlns:taxii=“http://taxii.dhs.gov/messages/taxii_xml_binding-1”message_id=“111111111” feed_name=“feedName” subscription_id=“01234567-89ab-cdef-0123-456789abcdef”>

</taxii:Poll_Request>
```

Note: TAXII Administrators will provide the Data Feed Subscription ID after receiving the customer's requirements from Section 2.3

4.3 CISA Estimated Timelines

Common CISA tasks have the following estimated timelines for implementation:

- CISA needs at least 2 business days to install customer Client SSL/TLS certificates in order to generate and present TAXII login credentials (subscription ID) back to the customer.
- CISA needs up to 2 weeks to implement customer infrastructure IP addresses into our ALLOW lists -- the sooner you can provide your infrastructure specific IP addresses, it will facilitate inclusion in the ALLOW lists.
- Listing of customer infrastructure IP addresses is done by the CISA Trusted Internet Connection (TIC) team and in accordance with TIC requirements.

5 MISP Users

Malware Information Sharing Project (MISP) platform users can analyze AIS cyber threat indicators within a MISP database using an additional conversion tool. MISP doesn't have a built-in TAXII client so an intermediary is used to poll the TAXII server and convert from AIS STIX 1.1 format into the MISP Data event format.

CISA has built an open source tool called FLARE MISP Client to facilitate polling and sending of AIS data to the designated MISP server. (CISA supported open source intermediary tool designed to poll and send AIS STIX data into any MISP database) https://github.com/cisagov/flare-misp-service

Users can obtain AIS TAXII credentials from CISA and configure the FLARE MISP client per instructions on GitHub. CISA can offer additional troubleshooting support with the FLARE-MISP service initial setup, as needed.

6 List of ISAC Providers Sharing AIS Data

Many sector-based Information Sharing and Analysis Centers (ISACs) provide AIS data to their members. Some ISACs provide both AIS Public and CISCP feed data in their cyber threat indicator feeds. Organizations, who are members of one of the ISACs , can inquire as to whether access to the feeds are available and confirm they are also receiving AIS data. For a current list of ISAC providers please refer to the AIS website: https://www.cisa.gov/ais

7 TAXII Production Feeds

7.1 Production Feed

The AIS TAXII Server has three (3) production receive (poll) AIS data feeds:

- AIS (PUBLIC) -- feed that shares data from federal and non-federal participants to include State, Local, Tribal and Territorial (SLTT), international and industry to the broader private sector community
- FEDGOV – Federal bi-directional feed that contains all data.

The AIS TAXII Server has a single (1) production submission feed:

- ➢ AIS INGEST – Submission feed to submit data to the AIS environment

Production Feed Poll Addresses and Poll Timeframes: To access the CISA AIS data feeds use the following TAXII 1.1 production feed address:

- o For feed polling (if using Subscription ID): https://taxii.dhs.gov:8443/flare/taxii11/poll
- o For feed discovery: *https://taxii.dhs.gov:8443/flare/taxii11/discovery*
  - ▪ No subscription ID is needed for Discovery
  - ▪ **IMPORTANT**: Port 8443 must be open inbound and outbound. Bi-directional traffic is required for SSL/TLS secured connection.

- CISCP – CISCP member community feed, contains more enriched data for non-federal entities. Access is authorized by signed CISCA Agreement

7.1.1 AIS PUBLIC and FEDGOV Feeds Recommended Poll Timeframes

There is a limitation associated with attempts to send Poll Requests for archive data and current date for the AIS Public and FEDGOV feeds. Poll requests must to be limited to four (4) hour time periods. This action needs to occur since Poll Responses with too much content in the requested time period are dropped due to HTTPS timeouts.

7.1.2 CISCP Feed Poll Timeframe

The Poll Request for the CISCP feed are limited to a 90-day request time period since the historical guideline for this content reflects that it is shared less frequently on this feed, making searches that result in HTTPS timeouts less common.

8 Frequently Asked Questions (FAQs)

8.1 Why do I need to provide my client SSL/TLS certificate?

This is a 2-way SSL/TLS encrypted communication. In order to complete a 2-way SSL/TLS

8.2 How often should I poll?

That is up to each customer. CTIs/DMs are published throughout the day (everyday) so you may want to check several times a day. Given the volume of data, we recommend you specify start and end dates when polling to narrow down results. Best practice is to poll in four-hour (or less) windows for the AIS Public and FEDGOV feeds.

8.3 Are there usernames and passwords associated with TAXII?

No. TAXII authenticates via PKI certificates using machine-to-machine communications without the need for usernames or passwords.

8.4 Why is my query hung?

If your query is hung, it is possibly related to you not supplying start/end dates and the query is timing out. Once a date range (please see FAQ 8.2) has been added, you should be able to pull data successfully.

8.5 Why am I seeing a TAXII response with status_type="UNSUPPORTED_PROTOCOL"?

Either you are not using HTTPS (TLS/SSL) or you aren't presenting a valid CA certificate. Check the URL you are hitting and confirm the request is using your client certificate. Also, ensure you are using the TAXII Server Public certificate provided to you from CISA.

8.6 Why am I seeing a TAXII response with status_type= "UNAUTHORIZED"?

You have successfully made it past the 2-way SSL/TLS handshake with the AIS TAXII Server, but you are not being recognized as a fully registered user on the CISA AIS system. This is likely an issue requiring additional support to resolve. Please contact taxiiadmins@us-cert.gov to determine if you and your client SSL/TLS certificates have been properly registered on the system.

8.7 Why am I seeing a TAXII response with status_type= "BAD_MESSAGE"?

You have been authenticated and authorized on the AIS TAXII Server however, your request is not a valid TAXII 1.1 message. Check the body of your POST request to ensure that it complies with TAXII specifications. You need to properly specify certain HTTP Headers, in addition to having a valid TAXII 1.1 payload.

8.8 Why am I seeing a TAXII response with status_type= "FAILURE"?

You were authenticated and authorized on the AIS TAXII Server and your message was validated against the TAXII 1.1 specification however, some other generic failure has occurred.

- Please contact taxiiadmins@us-cert.gov for assistance.

8.9 Why am I not able to connect to the TAXII server and receive a "Validation Schema Error" during a Polling request?

Ensure that the Key Usage entry is populated with the Digital Signature – see Section 2.2.2 Digital Signature.

9 Other Items/Best Practices:

- The connection to the CISA AIS TAXII Server should be documented according to your organization's security requirements. CISA can help ensure all parties understand what to do in the event of a cyber incident involving the AIS TAXII Server.
- As CISA continues to ramp up the production of indicators you will continue to see an increase in feed content.
- Indicators may be updated over time with new information -- so understanding STIX sightings and versioning is important.
- It is possible to request indicators shared within AIS to be redacted by contacting taxiiadmins@us-cert.gov with details of the target indicator (Package ID, Indicator ID, and/or Indicator Content (e.g. IP Address or Domain Name)). After a redact request is verified and approved, future Poll Requests for that data will not include the redacted content in responses.
- We recommend customers configure their clients to poll using Coordinated Universal Time (UTC) -- not local time
- Polling time period restrictions are detailed in section 7.1
- It can take between 7 and 14 days for a SSL/TLS certificate to be issued after you have notarized your paperwork and submitted it to the approved ECS vendor.
- All customers must keep their SSL/TLS certificate current. If your SSL/TLS certificate expires you will not be able to authenticate to the CISA AIS TAXII Server.
- For assistance please reach out to the TAXII Admin team at taxiiadmins@us-cert.gov

10 Acronyms

AIS	Automated Indicator Sharing
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing
CISA	Cybersecurity and Infrastructure Security Agency
CISCA	Cyber Information Sharing and Collaboration Agreement
CISCP	Cyber Information Sharing and Collaboration Program
CTI	Cyber Threat Indicator
CTIS	Cyber Threat Information Sharing
DM	Defensive Measure
FAQ	Frequently Asked Questions
FBCA	Federal Bridge Certification Authority
ID	Identification
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
MISP	Malware Information Sharing Project
POC	Point of Contact
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TIC	Trusted Internet Connection
TOU	Terms of Use
UTC	Coordinated Universal Time

11 Appendix A - List of Compatible TAXII Clients

This list of TAXII implementations are interoperable with the CISA TAXII server. There are other TAXII options available which may work with the CISA server, but we would need to conduct additional testing first. This list will be updated as CISA conducts additional interoperability testing:

- **CISA TAXII Client** (Called "FLARE Client" internally and available free of charge)
  - https://github.com/bcmc/oss
  - This is the preferred client to use for complex/problematic troubleshooting when difficult-to-solve polling or publishing issues occur.
  - Note: Polls beginning or ending during the 59th second of any minute will fail. This will be corrected in a future version of FLARE (2019)
- **LibTAXII** (Open source Python library)
- **Cabby Client** (Open source and available free of charge)
- **EclecticIQ/OpenTAXII** (Open source and commercial options)
- **Anomali STAXX** (Commercial product)
- **Analyst1** (Illuminate) (Commercial product)
- **Celerium/NC4 CTX/Soltra** (Commercial product)
- **IBM QRadar** (Commercial product)
- **Palo Alto MineMeld** (Commercial product)
- **Splunk Enterprise** (Commercial product)

NOTE: Customers using any of these clients will still need to obtain a PKI-medium certification and provide CISA with static IP addresses that they will be using to connect to the TAXII Server.

12 Appendix B - List of Data Aggregator Commercial Threat Intelligence Platforms Currently Supporting Access to the CISA AIS TAXII Server

If interested in a Data Aggregator commercial Threat Intelligence Platform that providers AIS data to existing subscribers at no extra cost – please refer to the AIS website: https://www.cisa.gov/ais

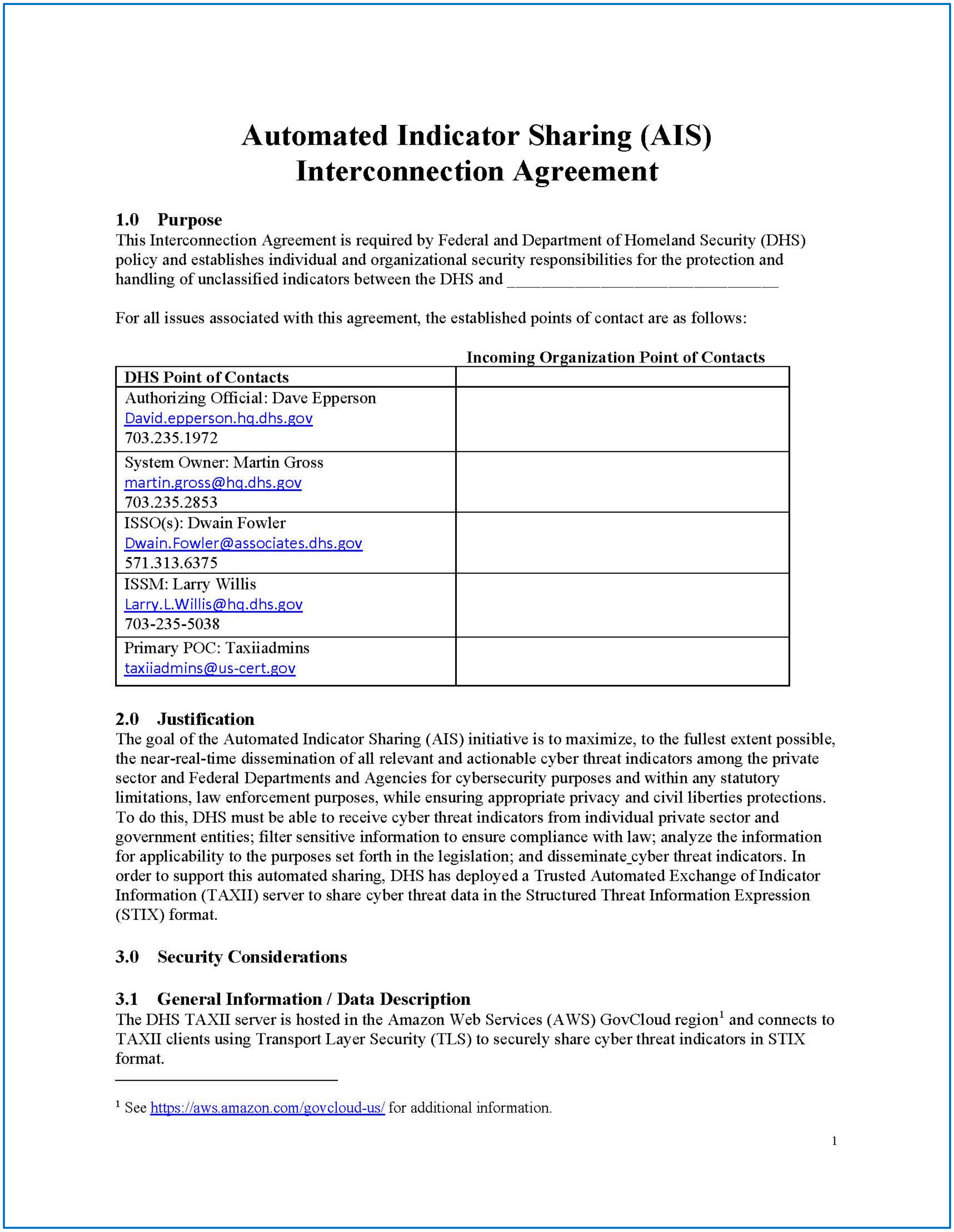
Customers must still complete the AIS Terms of Use (TOU) document and return it to cyberservices@cisa.dhs.gov

13 Appendix C - List of CISA Approved FBCA Vendors

CISA approved FBCA vendors: https://www.cisa.gov/dhs-approved-vendors-offer-ais-taxii-client-compatible-certificates

14 Appendix D - Interconnection Agreement Template

-



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 and ________________________________

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

	Incoming Organization Point of Contacts
DHS Point of Contacts	
Authorizing Official: Dave Epperson David.epperson.hq.dhs.gov 703.235.1972	
System Owner: Martin Gross martin.gross@hq.dhs.gov 703.235.2853	
ISSO(s): Dwain Fowler Dwain.Fowler@associates.dhs.gov 571.313.6375	
ISSM: Larry Willis Larry.L.Willis@hq.dhs.gov 703-235-5038	
Primary POC: Taxiiadmins taxiiadmins@us-cert.gov	

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 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. In order to support this automated sharing, DHS has deployed a Trusted Automated Exchange of Indicator Information (TAXII) server to share cyber threat data in the Structured Threat Information Expression (STIX) format.

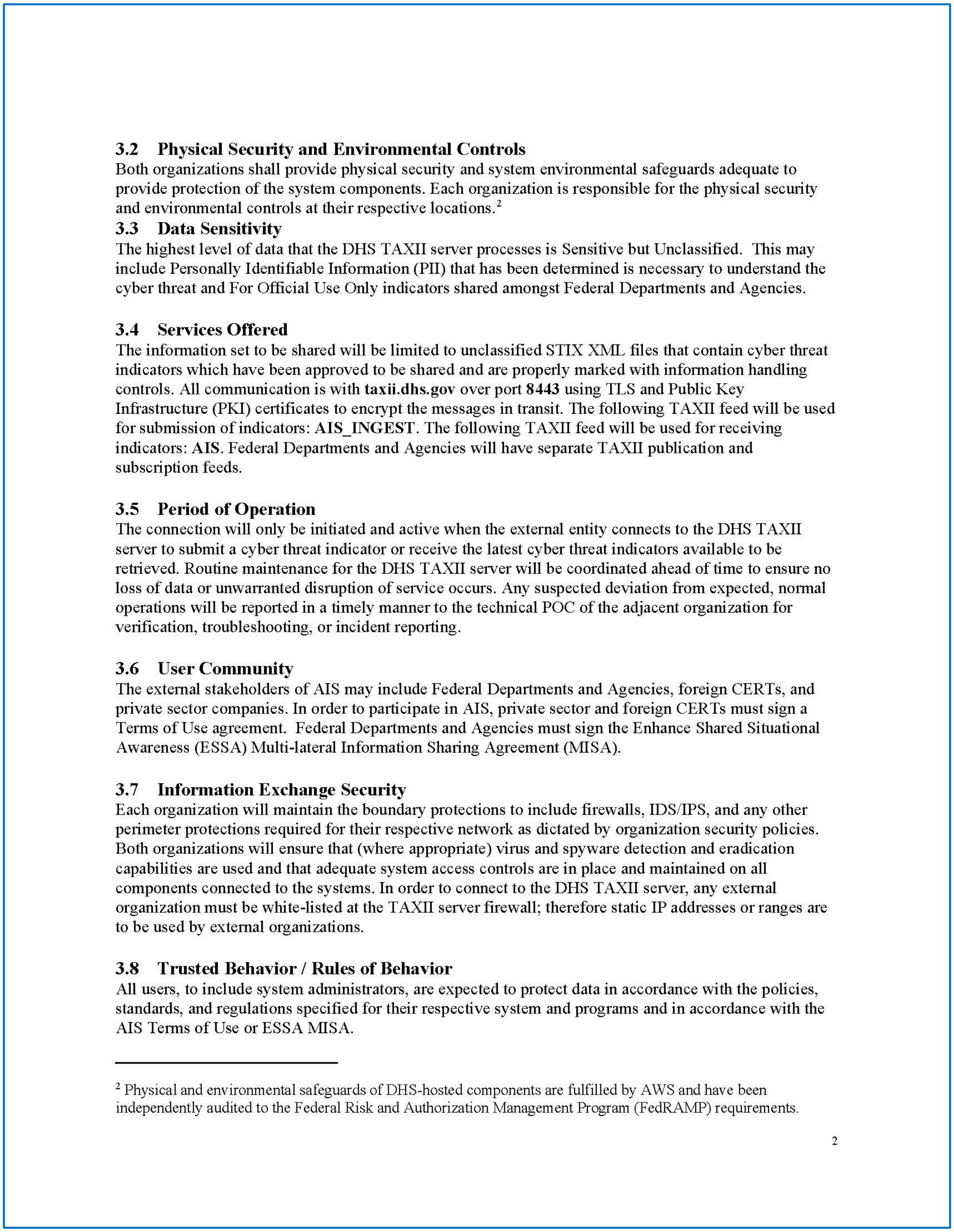
3.0 Security Considerations

3.1 General Information / Data Description

The DHS TAXII server is hosted in the Amazon Web Services (AWS) GovCloud region[1] and connects to TAXII clients using Transport Layer Security (TLS) to securely share cyber threat indicators in STIX format.

[1] See https://aws.amazon.com/govcloud-us/ for additional information.

1



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.[2]

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 Federal Departments and Agencies.

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 and Public Key Infrastructure (PKI) 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 Agencies 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. In order 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).

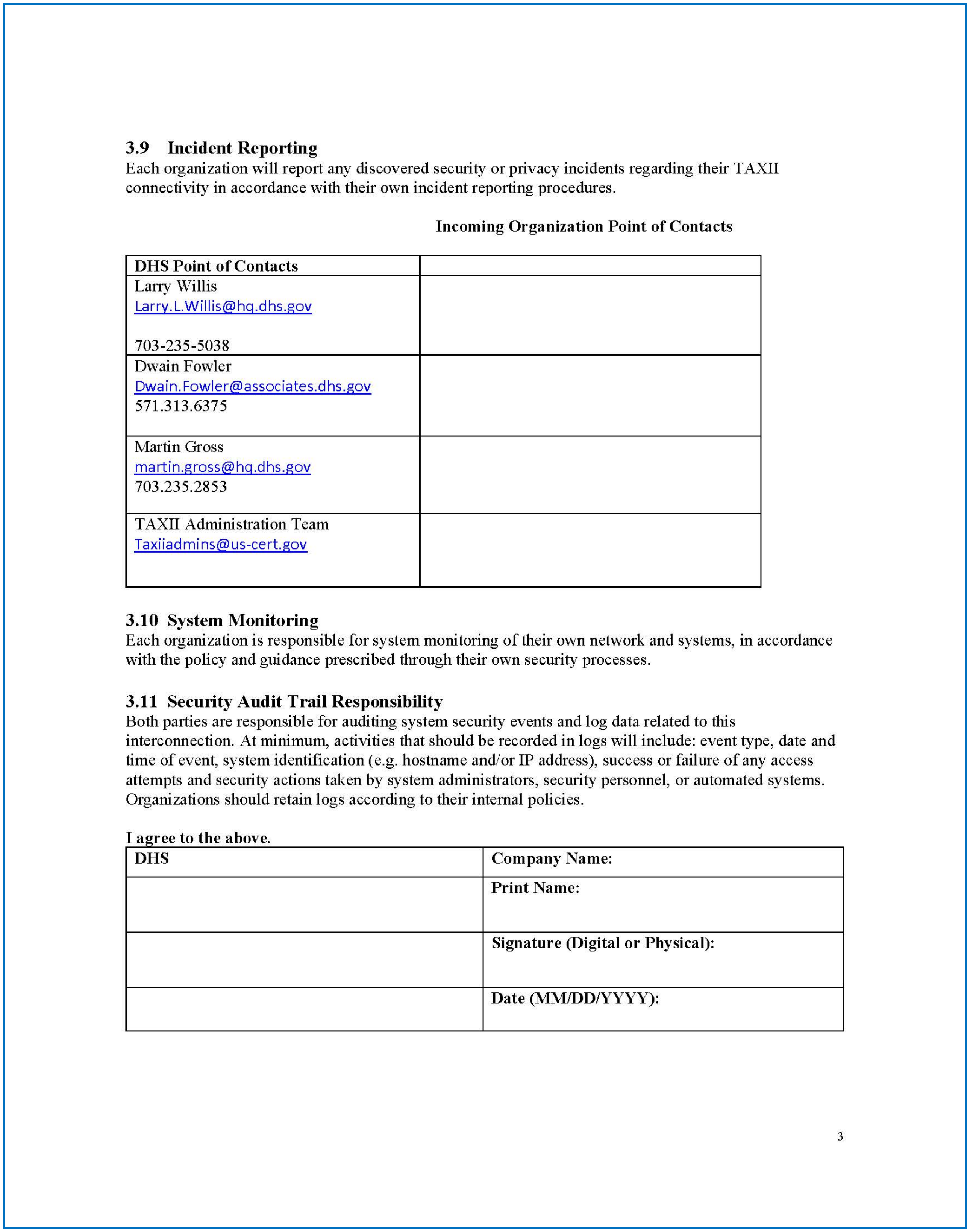
3.7 Information Exchange Security

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. Both organizations will ensure that (where appropriate) virus and spyware detection and eradication capabilities are used and that adequate system access controls are in place and maintained on all components connected to the 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.

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.

[2] 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.



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.

Incoming Organization Point of Contacts

DHS Point of Contacts	
Larry Willis Larry.L.Willis@hq.dhs.gov 703-235-5038	
Dwain Fowler Dwain.Fowler@associates.dhs.gov 571.313.6375	
Martin Gross martin.gross@hq.dhs.gov 703.235.2853	
TAXII Administration Team Taxiiadmins@us-cert.gov	

3.10 System Monitoring

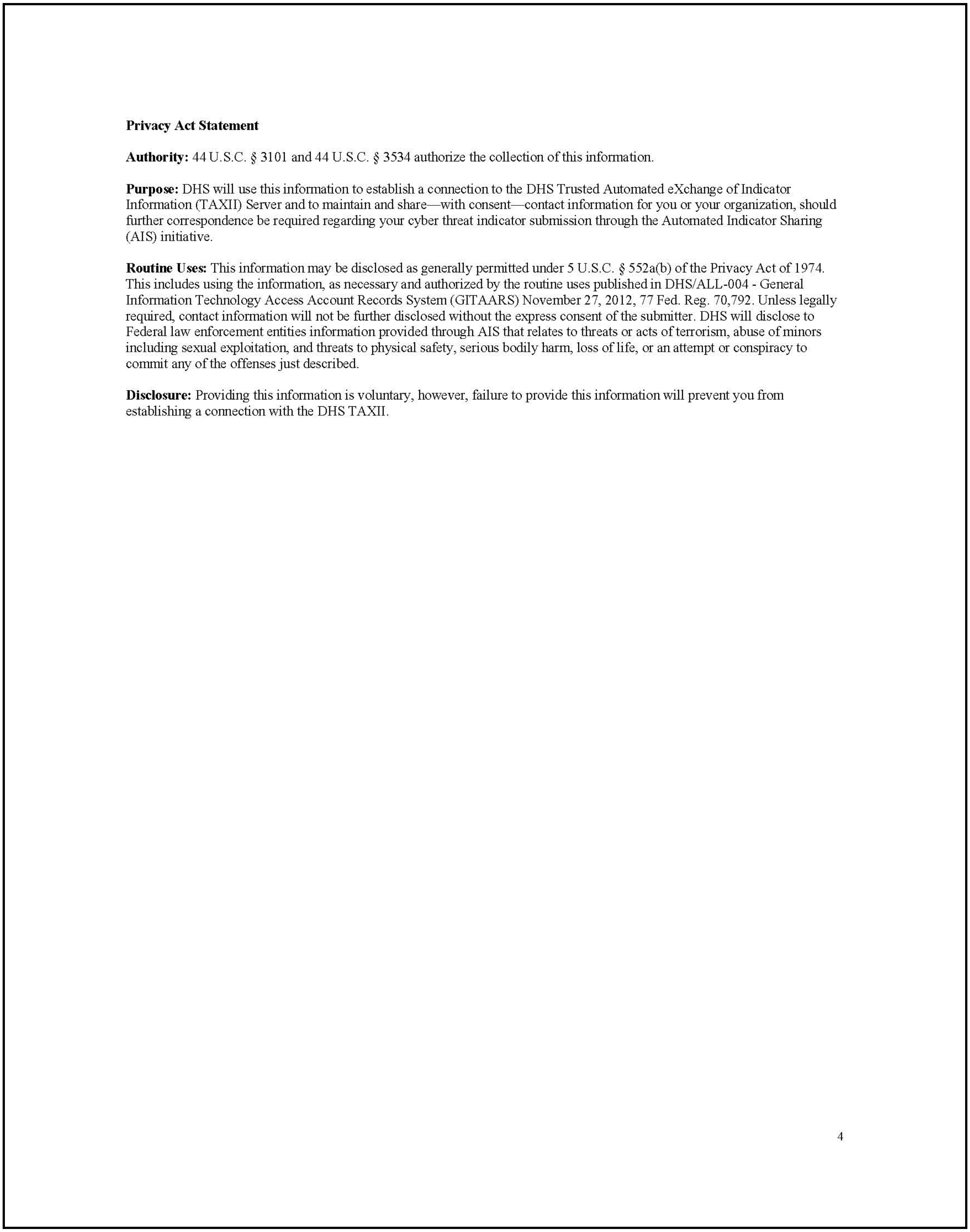
Each organization is responsible for system monitoring of their own network and systems, in accordance with the policy and guidance prescribed through their own security processes.

3.11 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.

I agree to the above.

DHS	**Company Name:**
	Print Name:
	Signature (Digital or Physical):
	Date (MM/DD/YYYY):



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 TAXII.