Homeland Security

Interconnection Security Agreement (ISA) for the DHS Trusted Automated Exchange of Indicator Information (TAXII)

Between

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications

And

Department of Energy
Joint Cybersecurity Coordination Center
Cyber Fed Model

June 6, 2016

Version 1.0

Table of Contents

1.0 CAPABILITY PROVIDER SECTION

1.1. OVERVIEW

This Interconnection Security Agreement (ISA) is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for the protection and handling of sensitive but unclassified (SBU) information between the DHS National Protection and Programs Directorate (NPPD) Office of Cybersecurity and Communications (CS&C) Network Security Deployment (NSD) and any External Entity. DHS has developed the capability to automate the exchange of cybersecurity information including indicator and defensive measure data in support of the Automated Indicator Sharing (AIS) initiative's goal of providing near-real time information sharing between the National Cybersecurity and Communications Integration Center (NCCIC) and other AIS participants and additional cybersecurity information sharing between Federal Entities that are signatories to the Multi-lateral Information Sharing Agreement (formerly the ESSA Initiative). Any specific requirements of both signatory organizations are included in this ISA.

This ISA addresses the interconnection of any Federal agency and the NCCIC TAXII server. Additionally, this ISA covers application and/or control data traversing the network.

1.1.1. Enhance Shared Situational Awareness Initiative background

The vision of the Enhance Shared Situational Awareness (ESSA) Initiative is to create real-time cybersecurity situational awareness, to enable integrated operational actions, and to improve the security of the U.S. Government and U.S. critical infrastructure. ESSA lays the foundation to share the right information, in time to make a difference, and in formats that reduce human workload and speed time to action.

1.2. CAPABILITY SYSTEM SECURITY CONSIDERATIONS

- DHS Sensitive Systems Policy Directive 4300A (based on National Institute of Standards and Technology (NIST) Special Publications 800-37 and 800-53) establishes DHS policy for network connectivity. The 4300A section on network connectivity (Section 5.4.3) states in part: Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
- Interconnections between DHS and non-DHS Information Technology (IT) systems shall be established only through controlled interfaces and by

approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements, or interconnection security agreements.

- ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.
- ISAs shall be reviewed and updated as needed as a part of the annual Federal Information Security Management Act (FISMA) self-assessment.
- The NPPD Chief Information Officer (CIO) shall approve all interconnections between NPPD information systems and non-DHS information systems. The NPPD CIO shall ensure that connections with other Federal Government agencies are properly documented. A single ISA may be used for multiple connections if the security accreditation is the same for all connections covered by that ISA.
- Components shall document interconnections between their own and external (Non-DHS) networks with an ISA for each connection.
- DHS OneNet shall provide secure Name/Address resolution service. DNSSec has been designated as the DHS service solution.
- All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.
- The appropriate Change Control Board (CCB) shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.

1.3. CAPABILITY SERVICES OFFERED

The interconnection between the external Federal partner and the DHS TAXII server will be a machine-to-machine Hyper Text Transfer Protocol (HTTP) over Transport Layer Security (TLS) tunnel initiated between a single server and client within each environment. The information sets to be shared will be limited to only unclassified, Structured Threat Information eXpression (STIX) Extensible Markup Language (XML) files that contain cyber threat indicators and defensive measures, which have been approved to be shared through existing programs.

Services and ports that are needed to access the Department systems are listed in Appendix A (Ports, Protocols, and Services). Additional information on STIX can be found at http://stixproject.github.io. Additional information on TAXII can be found at https://taxiiproject.github.io/ . Indicator fields allowable in each XML file sent to AIS are governed by the AIS Profile which is available via https://www.max.gov. Federal users will use, for Federal sharing, the ISA profiles found at https://community.max.gov/display/CrossAgencyExternal/ISA+STIX+Profiles , access requires an OMB Max account.

1.4. CAPABILITY DATA SENSITIVITY

All data generated by the DHS TAXII Server is intended for machine-to-machine communications and is transmitted via XML format.

The highest level of data will be SBU. This may include, but is not limited to: Sensitive Personally Identifiable Information, For Official Use Only (FOUO), Financial, and/or Law Enforcement Sensitive data.

For non-DHS organizations, it is assumed that they, as well, will be using nothing higher than a SBU classification for any/all of the data that they are using. There are no provisions in place to transmit Confidential, or higher, classifications via the TAXII infrastructure.

The DHS TAXII server has been declared a FISMA Moderate/Moderate/Moderate (M/M/M) system for accreditation purposes. The TAXII Server received a three-year Authority to Operate (ATO) on January 19, 2016.

1.5. CAPABILITY USER COMMUNITY

The DHS TAXII external user community is comprised of private sector entities; Information Sharing and Analysis Organizations (ISAOs); Information Sharing and Analysis Centers (ISACs); U.S. Federal Government organizations; State, Local, Tribal, and Territorial (SLTT) entities and International partners.

Internally, the DHS TAXII server administrators and analysts are NPPD employees or contractors with DHS adjudicated suitability background investigations. Additionally, other users may include employees or contract employees of other DHS Components and other Federal agencies.

Under normal conditions, only U.S. Citizens are allowed access to DHS systems and networks, however, at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and

exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the CIO. Attachment J to the DHS 4300A Sensitive Systems Handbook provides an electronic form for requesting exceptions to the U.S. Citizenship requirement. Through the AIS initiative, foreign nationals will have access through the TAXII protocol to the server, but not to the actual network or systems hosting the server.

1.6. CAPABILITY INFORMATION EXCHANGE SECURITY

Information exchanged between the U.S. Federal Government agencies and the DHS TAXII systems occurs using Federal Information Processing Standard (FIPS) 140-2 compliant HTTP over TLS (Transmission Control Protocol (TCP) port 8443) with AES-256 as the minimum standard encryption algorithm. This connection will use the exchange of trusted Public Key Infrastructure (PKI) certificates for the establishment of secure communications. PKI certificates for the TAXII server are issued from the DHS Certificate Authority (CA) or Federal Bridge CAs per DHS Policy for Public Key Enablement. Each Federal entity connecting must provide DHS with PKI certificates for their TAXII instance. Those certificates should either be issued by the Federal entity's CA or purchased from a commercial vendor that issues certs with a Federal Bridge CA relationship.

Each organization will maintain the boundary protections to include firewalls, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), and any other perimeter protections required for their respective network as dictated by organization security policies. All traffic between U.S. Federal agencies and the DHS TAXII server is routed through a managed Trusted Internet Connection (TIC) compliant network interface.

Both organizations will ensure that virus and spyware detection and eradication capabilities are used where appropriate (e.g., workstations, laptops, servers, etc.) and that adequate system access controls are in place and maintained on all components connected to the systems.

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

Currently data for the STIX/TAXII system is not encrypted at rest. However, data is encrypted while being transmitted. In addition, the TAXII database (MySQL) is encrypted by Amazon Web Services.

1.7. CAPABILITY EXPECTATIONS

The requirement for interconnection between the U.S. Federal Government agencies and DHS TAXII is to facilitate the timely and automated exchange of cyber-threat indicators and defensive measures. TAXII is a protocol allowing the import, processing and dissemination of cyber-threat data in STIX format.

The AIS initiative allows for ingest and processing of cybersecurity threat indicators and defensive measures from external entities. The goal of the system is to validate/sanitize ingested data and disseminate data to partner organizations. Partners include private sector entities; ISAOs; ISACs; U.S. Federal Government organizations; SLTT entities and International partners.

The goal of AIS is to provide near real time cyber-threat information through sharing of data with various entities. This in turn allows those entities to bolster perimeter and other defensive measures against cyber-threats. In turn, this is expected to mitigate losses due to cybercrime against Federal, State, and private sector interests.

The ESSA information sharing initiative allows for the sharing of cybersecurity information across the Federal Government. The DHS TAXII capability provides support for publishing and subscribing to this information for Federal Entities.

1.8. INCIDENT REPORTING PROCESS

Any U.S. Federal Government entity discovering a security incident will report it in accordance with the organization's incident reporting procedures. NCCIC TAXII shall report security incidents to the DHS Security Operations Center (SOC).

DHS SOC contact information is:

- DHS OneNET Support: 1-877-DHS1NET or 1-877-347-1638
    - Option 1 = NOC
    - Option 2 = SOC
- DHS SOC Direct Line: (703) 921-6505

Individual U.S. Federal Government agencies will report incidents in accordance with their individual policies concerning incidents.

Timeframes for reporting suspected or confirmed incidents are outlined in the DHS TAXII system incident response procedures and align with DHS 4300A Attachment F, Appendix F3, "Response Guidelines." Each organization will ensure that the other connecting organization is notified when security incidents may have affected the confidentiality, integrity, or availability of the shared data or systems being accessed. Notification for security incidents will be done, at a minimum, to the appropriate SOC and the security point of contacts (POCs) listed in this Interconnection Security Agreement that companies are required to sign.

1.9. TECHNICAL SUPPORT CONTACT INFORMATION

For issues relating to TAXII hub status, network outages, and connection issues you may contact the following:

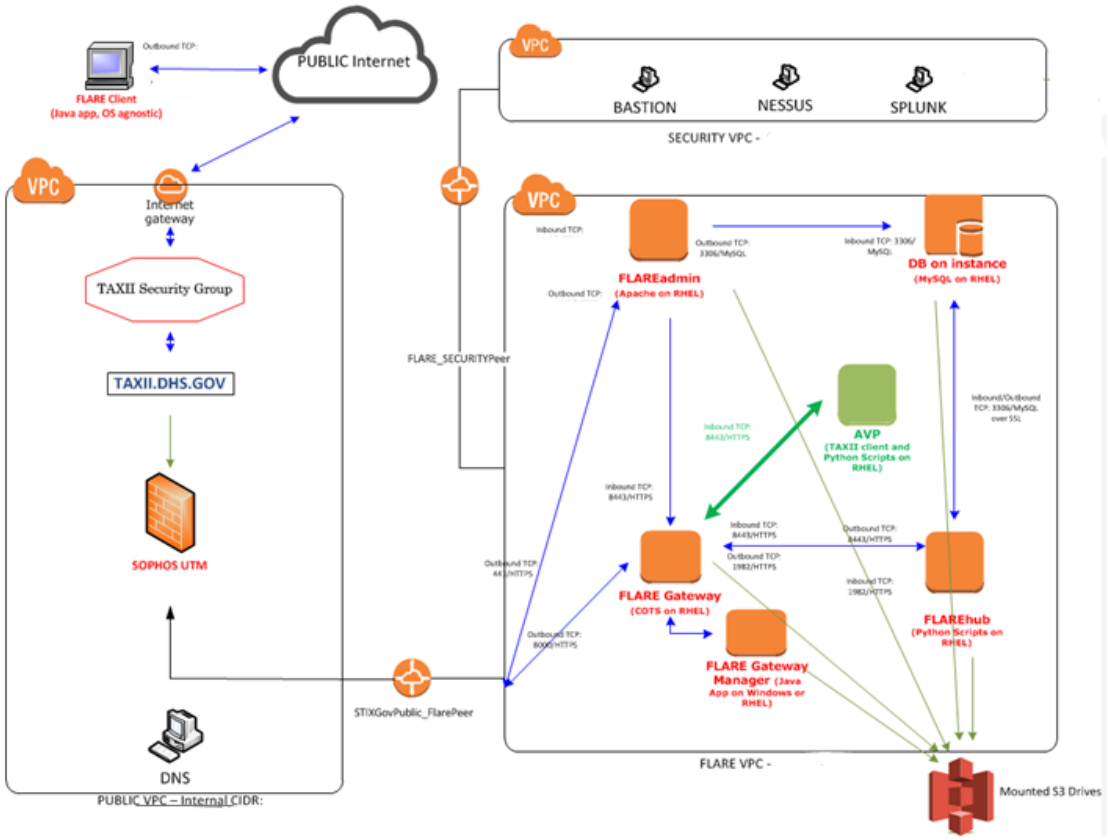
DHS TAXII Admin:

taxiiadmins@us-cert.gov

1.10. CAPABILITY FORMAL SECURITY POLICY

The interconnection between the U.S. Federal Government agencies and the DHS TAXII server will be a machine-to-machine HTTP over TLS tunnel initiated between a single server and client within each environment. The information sets to be shared will be limited to only unclassified, STIX XML files that contain cyber-threat indicators and defensive measures, which have been approved to be shared through existing programs. Services and ports that are needed to access the Department systems are listed in Appendix A (Ports, Protocols, and Services).

1.11. TAXII TOPOLOGICAL DRAWING



1.12. 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. The security controls for this interconnection will be

reviewed at least annually or whenever a significant change occurs. Either party may terminate this agreement with thirty days advanced notice. Noncompliance on the part of either organization or its users or contractors concerning security policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

1.13. CAPABILITY PROVIDER SIGNATORY AUTHORITY

DHS TAXII System Owner W. Preston Werntz	
	Signature & Date

DHS TAXII Information System Security Officer (ISSO) Stephen Tumbarello	
	Signature & Date

DHS TAXII Authorizing Official (AO) David Epperson	
	Signature & Date

2.0 CONNECTING ORGANIZATION SECTION

2.1 CONNECTING ORGANIZATION SUMMARY

The Department of Energy (DOE) is a Cabinet level Federal Government department with a broad array of energy-related missions. As a sector specific agency, DOE maintains substantial cybersecurity outreach programs with the Energy Sector.

The DOE Cyber Fed Model (CFM) provides machine-to-machine sharing of cyber data and information; it serves the whole of the Department, and is interconnected under separate agreements with other cybersecurity systems and services operated by DOE, other Federal Government agencies, and the Energy Sector.

Of particular note, agreements required for the operation of the DOE Cybersecurity Risk Information Sharing Program (CRISP), which provides for exchange of actionable cybersecurity information with the Energy Sector ISACs and asset owners, are maintained separately from this agreement. The CRISP program maintains a robust data sharing matrix appropriate to the Energy Sector, ISAC, and the Department.

2.2 CONNECTING ORGANIZATION SERVICES OFFERED

The interconnection between DOE CFM and the DHS TAXII server will be a machine-to-machine HTTP over TLS tunnel initiated between a single server and client within each environment.

The information sets to be shared will be limited to unclassified, STIX XML files that contain cyber-threat indicators and defensive measures that have been approved to be shared through existing programs.

2.3 CONNECTING ORGANIZATION DATA SENSITIVITY

The highest level of data will be SBU. This may include, but is not limited to Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), FOUO, Financial, or Law Enforcement Sensitive data.

2.4 TECHNICAL SUPPORT CONTACT INFORMATION

For issues relating to DOE CFM status, network outages, and connection issues you may contact the following:

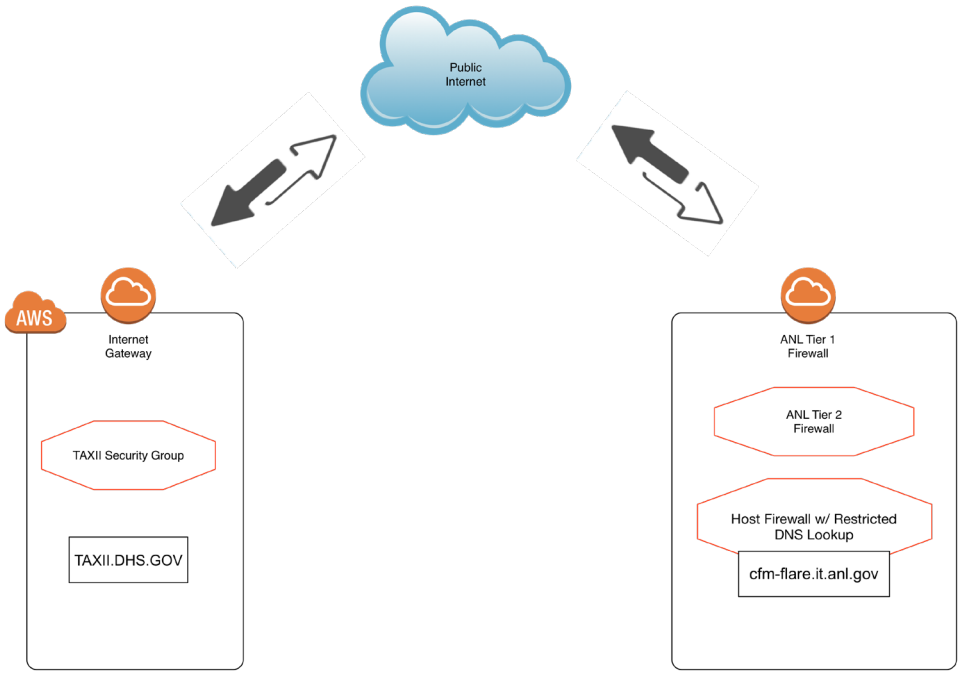
Cyber Fed Model Admin:

cfmteam@anl.gov

2.4. CONNECTING ORGANIZATION FORMAL SECURITY POLICY

DOE's formal security policy is established as DOE Order Number 205.1B, change 3.

2.5 CONNECTING ORGANIZATION TOPOLOGICAL DRAWINGS



2.6 CONNECTING ORGANIZATION SIGNATORY AUTHORITY

System Owner	
	Signature & Date

Information System Security Officer (ISSO)	
	Signature & Date

Authorizing Official (AO)	
	Signature & Date

APPENDIX A: Ports, Protocols and Services

The following ports, protocols, and services are allowed on the DHS TAXII server Security Domains by default.

Ports, Protocols, and Services Chart		
	Connecting Organization	**DHS TAXII**
Port Number (Server / Destination)		8443
Internet Protocol (IP) Protocol (TCP/UDP)		TCP
Software Application		Flare Suite
Data Type / Purpose		Structured cyber threat data (STIX format)
PII Data?		Yes
Financial Data?		No
Encryption used		TLS v1.1/AES 256