INTERCONNECTION SECURITY AGREEMENT

between

Your Company Name

and

U.S. CUSTOMS AND BORDER PROTECTION (CBP)

MONTH, YEAR

Full Company Name (including other legal names or d.b.a.* company names)

Department of Homeland Security
Customs and Border Protection

Address
City, State, Zip

Tel #:

Fax #:

Email:

---

* “doing business as”

INTERCONNECTION SECURITY AGREEMENT

The intent of the Interconnection Security Agreement (ISA) is to document and formalize the interconnection agreement between Customs and Border Protection (CBP) and other non-Customs organizations.

1. INTERCONNECTION STATEMENT OF REQUIREMENTS.

a. The requirements for interconnection between the CBP and YOUR COMPANY NAME located at, COMPANY ADDRESS, CITY, STATE, ZIP is for the express purpose of the following:

- Provide your company with VPN tunnel connectivity to CBP for the purpose of allowing your company to send/receive Automated Commercial System (ACS) and/or Automated Export System (AES) data, to/from CBP via MQ Server.

b. No other services are authorized under this agreement. Other than the passing of data stated in paragraph 1a, only communication control signals typical of Transmission Control Protocol/Internet Protocol (TCP/IP) and MQ Server will be permitted.

c. Data transmitted between your designated end-point system and CBP will be protected (encrypted) in accordance with the guidelines of the Privacy Act, Trade Secrets Act (18 U. S. Code 1905), and Unauthorized Access Act (18 U. S. Code 2701 & 2710) while in CBP possession. Transaction data returned to your system remains protected (encrypted) until transmitted through the layer-3 VPN tunnel connected to your system, at which point the data is decrypted (open and unprotected) for final transmission into your system. Your company is responsible for providing any further protection measures for your company data when resident in your computing environment, as necessary.

d. The pertinent details of the connection are:

- Router Access Lists (RAC) and TCP/IP addresses and ports
- Cisco VPN Concentrator or IOS based VPN and IPSEC encryption
- MQSeries server connections, only

2. SYSTEM SECURITY CONSIDERATIONS.

a. The interconnection between YOUR COMPANY NAME and CBP is via a dedicated Multi Protocol Layer Switching (MPLS) Peerless IP (PIP) Virtual Private Network (VPN). Triple Data Encryption System (3DES), or Advanced Encryption Standard (AES) protect a VPN tunnel over a commercially provided native IP backbone network with no connection to the public Internet. The Cisco VPN Concentrator or IOS based VPN hardware on the end point devices provides the cryptographic function. Access is further controlled by a CA-Top Secret profile specific to each approved user. All access is controlled by authentication methods to validate the approved users.

b. The security of the information being passed on this network layer VPN connection uses Cisco VPN Concentrator or IOS based VPN hardware.

c. The CBP system and users are expected to protect this data in accordance with the Privacy Act, Trade Secrets Act (18 U.S. Code 1905), and Unauthorized Access Act (18 U.S. Code 2701 & 2710).

d. The sensitivity of all data filed is Sensitive But Unclassified (SBU).

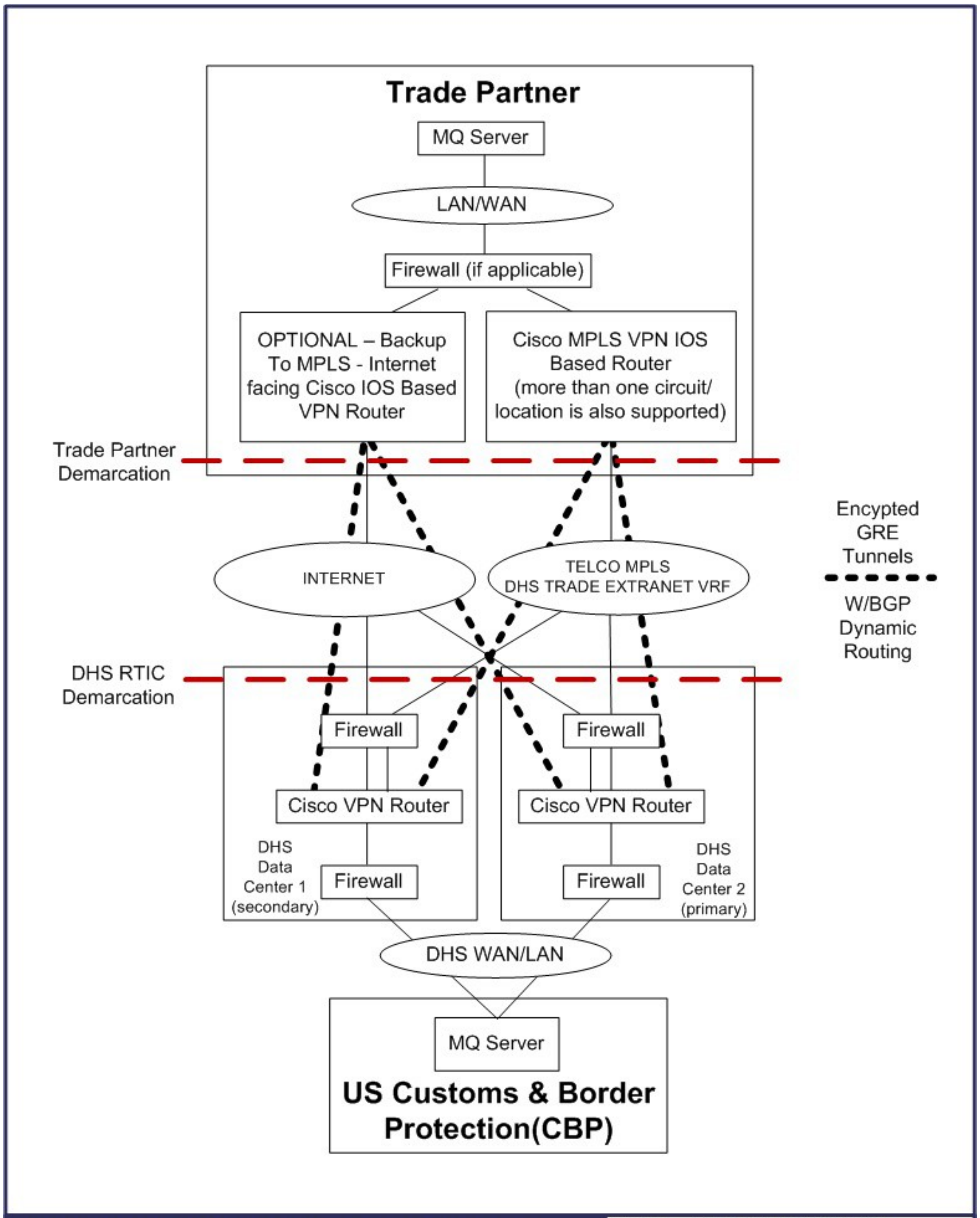
e. All CBP employees with access to the data are U. S. citizens with a valid and current CBP Background Investigation.

f. Policy documents that govern the protection of the data are CBP 1400-05D Security Policy Handbook and Department of Homeland Security 4300A Security Policy Handbook.

g. CBP maintains an audit trail and employs intrusion detection measures to maintain security and system integrity.

h. All security incidents that have any effect on the security posture of CBP must be reported to the CBP Computer Security Incident Response Center (CSIRC) located at the CBP NDC (tel: 703-921-6507). The policy governing the reporting of security incidents is CIS HB 1400-05D.

3. TOPOLOGICAL DRAWING. The two systems are joined via a layer-3 IPSEC VPN tunnel. The DHS/CBP facilities both maintain a 24-hour physically secure facility where access is controlled using restricted access and all visitors are escorted. The lines of demarcation are as illustrated in the following drawing:


Trade Partner
MQ Server
LAN/WAN
Firewall (if applicable)
OPTIONAL – Backup To MPLS - Internet facing Cisco IOS Based VPN Router
Cisco MPLS VPN IOS Based Router (more than one circuit/ location is also supported)
Trade Partner Demarcation
Encypted GRE Tunnels
W/BGP Dynamic Routing
INTERNET
TELCO MPLS DHS TRADE EXTRANET VRF
DHS RTIC Demarcation
Firewall
Firewall
Cisco VPN Router
Cisco VPN Router
DHS Data Center 1 (secondary)
Firewall
Firewall
DHS Data Center 2 (primary)
DHS WAN/LAN
MQ Server
US Customs & Border Protection(CBP)

DHS/CBP TRADE PARTNER MPLS CONNECTIVITY TO DHS DATA CENTER IPSEC ENDPOINTS with OPTIONAL INTERNET FAILOVER

Author: DHS OneNet Engineering
Date: October 18, 2010
Revision: 3

4. SIGNATORY AUTHORITY

This ISA is valid for (3) years after the latest date on either signature below. Approximately 30 days prior to expiration, the ISA will be updated, reviewed, and revalidated. This agreement may be terminated upon 30-days advanced notice by either party or in the event of a security exception that would necessitate an immediate response.

SIGNATURE AUTHORITY NAME AND TITLE	**Donald A. Matheson** **Acting Executive Director** **Enterprise Data Management and Engineering Directorate (EDMED)** **Office of Information & Technology** **U.S. Customs and Border**
--	--
Signature Date	Signature Date
Telephone	
--	
Telephone	

Addendum – Additional Connection / Computer Sites

(*if applicable*)

Please list pertinent identifying information – name (if different/d.b.a.), full address, contact name, contact number, contact facsimile, etc.