INTERCONNECTION SECURITY AGREEMENT

between

Your Company Name

and

U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)/

U.S. CUSTOMS AND BORDER PROTECTION (CBP)

MONTH, YEAR

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

U.S. Department of Homeland Security
U.S. 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 U.S. Customs and Border Protection (CBP) and other non-Customs organizations.

1. INTERCONNECTION STATEMENT OF REQUIREMENTS.

a. The requirements for interconnection between the DHS/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 DHS/CBP for the purpose of allowing your company to send/receive Automated Commercial System (ACS) and/or Automated Export System (AES) data, to/from DHS/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 DHS/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 DHS/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 DHS/CBP is via a dedicated Multi Protocol Layer Switching (MPLS) Peerless IP (PIP) Virtual Private Network (VPN). Advanced Encryption Standard (AES) 256 bit protected 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 DHS/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).

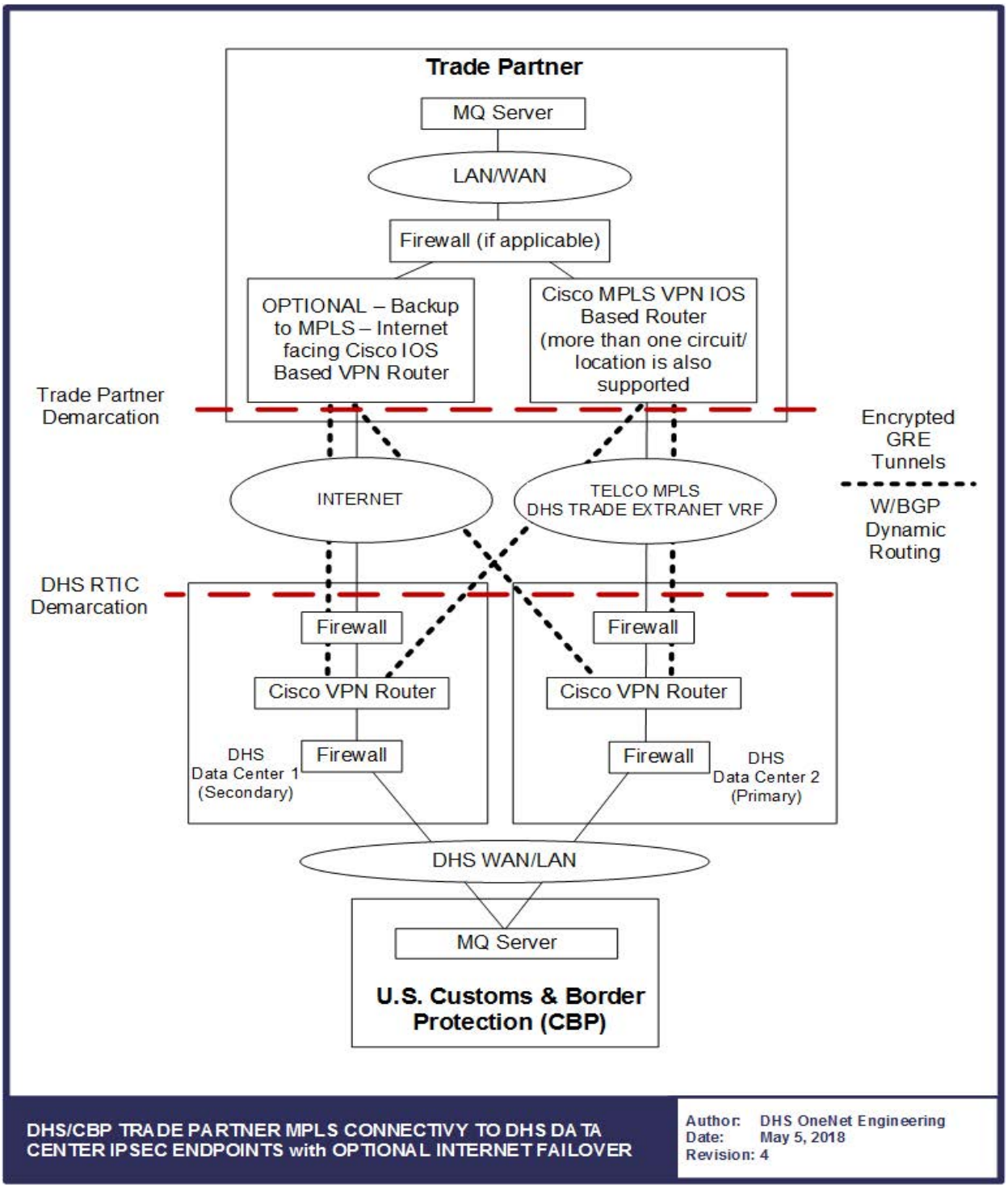
e. All DHS/CBP employees with access to the data are U. S. citizens with a valid and current DHS/CBP Background Investigation.

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. DHS/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 Security Operations Center (CBP SOC) 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:



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 reviewed, validated and stored by CBP. Renewals will be initiated by *your company* every 3 years, or when significant changes occur. 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.

Company Name
Your Name
Your Title

Phone Number

CBP CISO
Alma R. Cole
Chief Information Security Officer
Cyber Security Directorate
Office of Information and Technology
U.S. Customs and Border Protection

DHS RTIC Authorizing Official
Dr. Thresa Lang
Acting Chief Information Security Officer
Information Technology Services Office
Office of the Chief Information Officer
Department of Homeland Security

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.