INTERCONNECTION SECURITY AGREEMENT

July 2017

U. S. Department of Homeland Security

U. S. Customs and Border Protection

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 and other non-Customs organizations.

1. *INTERCONNECTION STATEMENT OF REQUIREMENTS.*

a. The requirements for interconnection between the U.S. Customs and Border Protection (CBP) and your company is for the express purpose of the following:

- Provide your company with a Virtual Private Network (VPN) tunnel connectivity to CBP for the purpose of allowing your company to send/receive data, to/from CBP, via Message Queue (MQ) Client/Server.
- If providing Stow Plans or Container Status Messages (CSMs) as part of a Security Filing, then this ISA supports the use of email and Secure File Transport Protocol (SFTP) for Stow Plans as well as SFTP for CSMs sent from your organization to CBP.
- Supports the use of SFTP for Advanced Encryption Standard (AES) Commodity data.

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 Client/Server will be permitted.

- SFTP and email for filing of Stow Plans, AES Commodity and Container Status Messages (CSM) only are supported.

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). 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.

2. *SYSTEM SECURITY CONSIDERATIONS.*

a. **General Information/Data Description.** The interconnection between your company and CBP is via the public Internet, over an FIPS 140-2 Approved Advanced Encryption Standard (AES) 256 bit protected VPN tunnel. Authentication will be via CBP provided user ID and password and/or pre-share keys.

b. **Services Offered.** The security of the information being passed on this layer-3 IPSEC VPN connection uses either Cisco VPN hardware or software.

c. **Data Sensitivity.** The sensitivity of all data filed is Sensitive But Unclassified (SBU).

d. **FIPS-199 Security Categorization**. All associated CBP applications are security categorized as High

e. **User Community.** All CBP employees with access to the data are U.S. Citizens with a valid and current CBP Background investigation

f. **Information Exchange Security.** The connection with CBP is via the public Internet, over an AES 256 bit protected VPN tunnel.

g. **Trusted-Behavior Expectations.** 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).

h. **Formal Security Policy.** Policy documents that govern the protection of the data are U.S. CBP Customs Information Security Handbook (CIS HB) (HB 1400-05D), and Department of Homeland Security (DHS) –4300A Sensitive Systems Policy.

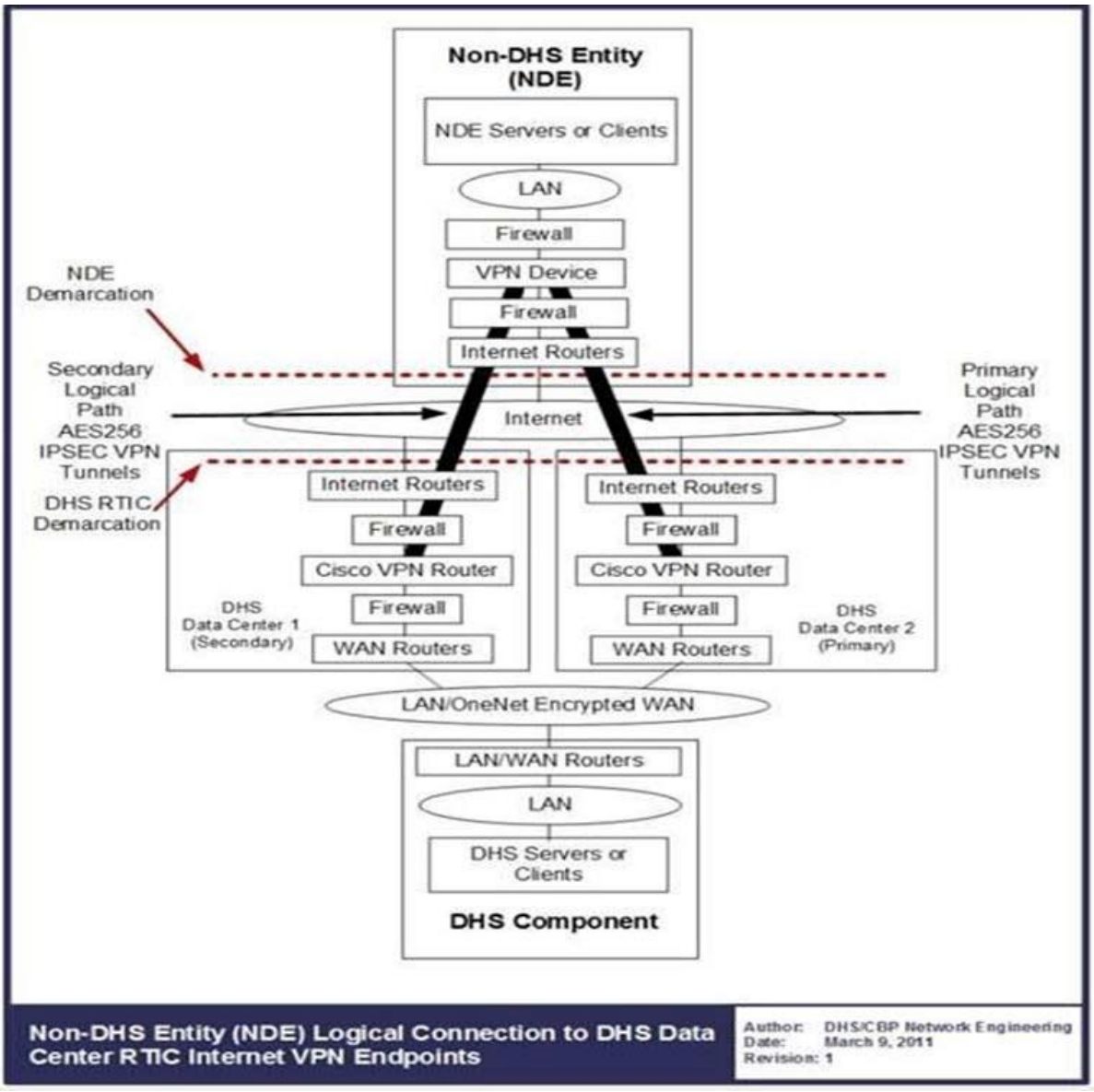
i. **Incident Reporting.** All security incidents that have any effect on the security posture of CBP must be reported to the CBP Computer Security Incident Response Center (CSIRC) located at the CBP NDC (tel: 703-9216507). The policy governing the reporting of security incidents is CIS HB 1400-05D.

j. **Audit Trail Responsibilities.** CBP maintains an audit trail and employs intrusion detection measures to maintain security and system integrity.

3. *TYPOLOGICAL DRAWING*

The two systems are joined via an encrypted VPN tunnel. The CBP NDC facility maintains 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[1]:



[1] Diagram was updated on March 9, 2011 by DHS/CBP Network Engineering Team and verified by CBP ISA Team on 6/9/17 as most current.

4. *SIGNATORY AUTHORITY.*

This ISA is valid upon electronic acknowledgement of receipt of an agreement from your designated corporate approval authority and valid for three (3) years after the date on the acknowledgement email.

The eISA 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.

DOCUMENT SIGNED IN JULY 2017 BY:

Phillip A. Landfried

Assistant Commissioner

Office of Information and Technology U. S. Customs and Border Protection

THE ORIGINAL SIGNATURE MAY NOT BE POSTED ON-LINE, BUT WILL BE MADE AVAILABLE FOR REVIEW UPON REQUEST.