

**ADDENDUM 13 TO APPENDIX 8 TO SCHEDULE 3.3
TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
ENTERPRISE REMOTE CONNECTION SERVICE
TECHNICAL APPROACH**

Statement of Technical Approach for Enterprise Remote Connection Service

Enterprise Remote Connection Service (ERCS) utilizes secure tunnels across the internet to connect to the Commonwealth network. This technology offering allows the use of common broadband internet services as a means to facilitate private Wide Area Network (WAN) connectivity and achieve connectivity back to the Commonwealth Domain securely. This service implements Dynamic Multipoint Virtual Private Network (DMVPN) technology that creates dynamic Internet Protocol Security (IPSec) tunnels making this service highly scalable. Wi-Fi service can be added as a single non-mobile Access Point (AP) embedded in the router as an additional convenience.

Technical Description for Enterprise Remote Connection Service

ERCS can securely connect End-Users with broadband or wireless internet connectivity to the VITA WAN using dynamic IPSec tunnels that protect data from unauthorized access. ERCS provides the following benefits:

Low cost network connectivity:

- Broadband internet access such as Digital Subscriber Line (DSL) or Cable and 3G wireless internet access can be utilized.
- Reduction in equipment costs have the potential to translate into reduced cost of service as compared to traditional T-1 technology.

Security

- All End-User traffic will traverse encrypted tunnels (IPSec) to the Commonwealth Enterprise Solution Center or other ERCS Eligible Customer Location. No direct access to the internet (split tunneling) is allowed.
- All traffic destined for the internet will flow through the Internet Secure Gateway (ISG) at CESC providing centralized firewall and web filtering protection.
- Authorization of ERCS routers will be controlled by certificates in order to prevent connections by unauthorized devices.

Monitoring

- 24 x 7 equipment monitoring
- Security Intrusion Prevention Services including Network-based Intrusion Detection Service (NIDS), Host-based Intrusion Detection Service (HIDS), and Network / Host-based Intrusion Prevention Services (NIPS/HIPS)

Technical Solution for Enterprise Remote Connection Service

Broadband Service

Eligible Customer Locations will be required to have an existing broadband service (DSL or Cable) or wireless service subscription in place prior to the deployment of this service.

Components

The solution consists of the following components:

- a. Broadband (DSL or Cable) service ordered separately by the Eligible Customer (Eligible Customer responsibility):
 - A standard telephone line over which DSL can be acquired or cable connectivity into the site location via a common cable provider.
 - A DSL bridge or cable modem that is provided by the DSL/Cable provider as part of their service.
 - An Ethernet cable to connect from the bridge/modem to the router provided by Vendor.
- b. Wireless service ordered separately by the Eligible Customer (Eligible Customer responsibility):
 - A wireless card provided by wireless subscription provider that will be embedded in the router provided by Vendor.
- c. Router supplied by Vendor:
 - The Vendor will supply a router capable of accepting Ethernet as its WAN interface. The router will be Virtual Routing and Forwarding (VRF) aware and able to perform DMVPN. All requests for ERCS will be submitted to Vendor in the form of a work request in accordance with the ERCS request instructions contained in the Procedures Manual.
 - As requested by Eligible Customers, Wi-Fi connectivity is available within the router and can provide a single point of Wi-Fi access (Please note: This does not constitute Vendor's Wireless Network Service as described in Appendix 8 to Schedule 3.3 of the CIA). No additional Access Points (AP's) can be installed with this solution.

Architecture

ERCS is suitable for locations that have modest bandwidth needs and do not desire Voice over IP (VoIP) or video services. Figure 1 below shows how the connection flow would work:

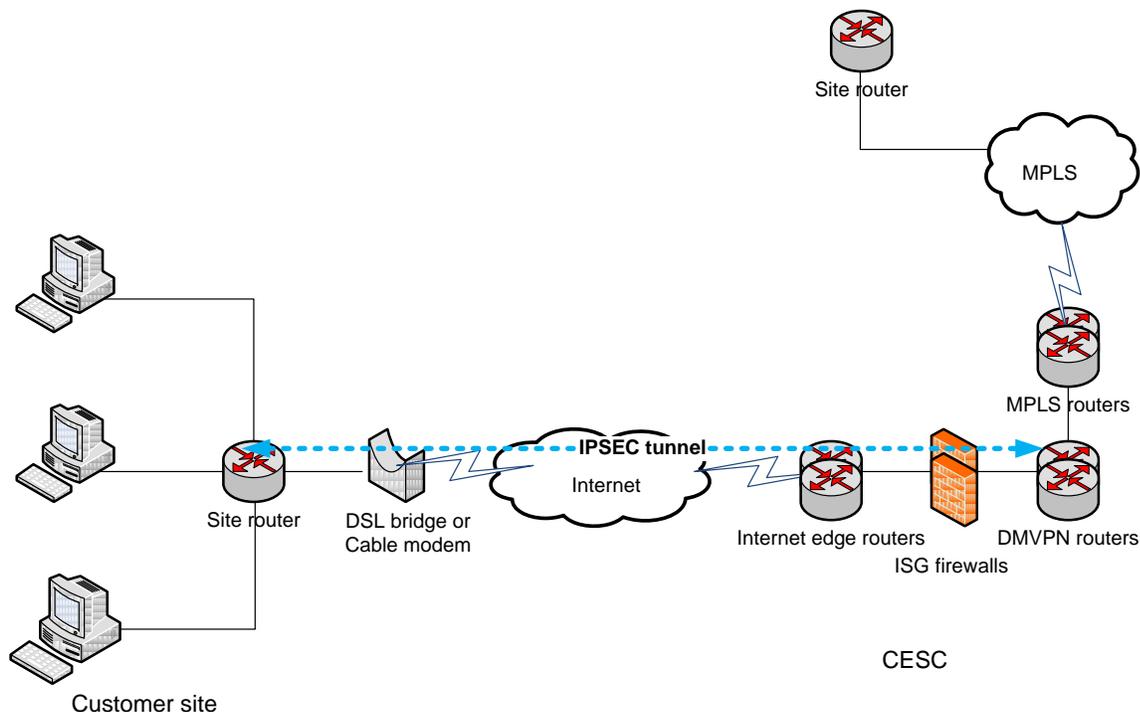


Figure 1 Enterprise Remote Connection Service Diagram

The connection from the customer site to CESC is across the internet broadband through an IPSec tunnel. The initial tunnel setup is done between the site router and the DMVPN hub routers at CESC. If the intended destination of the customer site network traffic is determined by the DMVPN routers to be another ERCS site, an IPSec tunnel is end pointed onto the destination site's router and the DMVPN hub routers then drop out of the traffic pathway. If the destination is the internet or conventional MPLS sites, the traffic will traverse the IPSec tunnel to the CESC hub routers and then follow the standard MPLS paths. Internet traffic will flow through the CESC ISG and back out to the internet to ensure secure firewall and intrusion detection for all internet communications.

Security

The Enterprise Remote Connection Service provides a secure connection method over the internet to both internal and external resources. The solution includes the following security functionality:

- IPSec tunnels using AES 256 encryption
- No ability to split tunnel
- Centralized firewalls with redundancy for all external (internet) communications
- Network-based Intrusion Detection Service (NIDS), Host-based Intrusion Detection Service (HIDS), and Network / Host-based Intrusion Prevention Services (NIPS/HIPS)

Technical Assumptions

Vendor's Enterprise Remote Connection Service includes the following assumptions:

- Broadband or wireless service will be acquired by the Eligible Customer via existing VITA contracts if at all possible and the Eligible Customer will be directly responsible for all costs and maintenance associated with the broadband or wireless service. In the event DSL service is utilized, a standard Plain Old Telephone Service (POTS) line will be required; Eligible Customers will be responsible for acquisition of the telephone line and associated charges.
- Due to technical and security considerations, ERCS is not suitable for site locations requiring high availability and throughput greater than 15Mbps. Prior to implementing an ERCS work request, Vendor will work with the Eligible Customer to determine if throughput, availability or degradation of WAN performance is possible.
- Voice over IP and Video services are not supported at Eligible Customer Locations utilizing the Enterprise Remote Connection Service.
- No direct access to the internet (split tunneling) is allowed.
- Wi-Fi network service offered with Enterprise Remote Connection Service will only be available in 802.11n standard and only allows for a single access point. No additional access points will be available. As the Wi-Fi access emanates from the router, the placement of the router will affect service area coverage.
- Wi-Fi service provisioned with Vendor's ERCS does not constitute Vendor's Wireless Network Service as described in Appendix 8 to Schedule 3.3 of the CIA.
- NOC monitoring will not be available for wireless component of this service.