

EXHIBIT I to Amendment No. 60
ADDENDUM 6 TO APPENDIX 3 TO SCHEDULE 3.3 TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
ENTERPRISE VPN SERVICES

**ADDENDUM 6 TO APPENDIX 3 TO SCHEDULE 3.3
TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
ENTERPRISE VPN SERVICES**

Overview

IPSec-based VPNs are the remote-access technology that allow secure access to resources by establishing an encrypted tunnel across the Internet which allows Agencies to cost effectively and securely extend the reach of their networks to anyone, anyplace, anytime.

With Enterprise VPN services, The Commonwealth can securely connect remote offices and remote users using cost-effective, third-party Internet access rather than expensive, dedicated WAN links or long-distance remote dial links. WAN bandwidth costs are reduced, while increasing connectivity speeds, by using broadband connectivity such as DSL, Ethernet, or cable and securing it with encrypted IPSec VPN tunnels.

Vendor offers two VPN services to the Commonwealth:

- Enterprise VPN Single Factor Authentication
 - Here the “single factor” is a user ID and password. The single-factor solution allows us to authenticate VPN users to the COV Active Directory domain. This solution has two caveats, the need for a cross-connect and an additional requirement that the user has a COV account in the group that has been configured and mapped for VPN access. This offering is the current Agreement standard provided at no additional charge to the Commonwealth. Use with a Vendor-provided asset is required for this service.
- Enterprise VPN 2-Factor Authentication
 - This service requires the user to use two factors to enable network access. The first of these factors is the ID and password. The second is an RSA key fob or token. This offering is subject to additional charges and the caveat that Vendor will not track Enterprise VPN Services in any Vendor Asset Management System including Altiris or TEAMS. Commonwealth-requested changes to the second authentication factor may result in additional charges (e.g., brand of key fob). Use of a Vendor-provided or VITA-approved computing device is required for this service.

Technical Description

The VPN solution architecture includes ASA 5550s that operate in redundant failover mode to support load balancing and load sharing and is expandable to support the entire customer base. A more detailed technical explanation of each VPN type is outlined below:

- **Single Factor Authentication** – Single factor authentication relies on a user’s login credentials (ID and password), and synchronization between Active Directory and the DIRSYNC database. A key fob is not required.

Use of a Vendor-provided computing device is required for this service. The asset must have installed a VPN profile, Cisco VPN client, centrally managed firewall software, and current virus definitions.

Single-factor VPN clients have limited access to a subset of network resources including Active Directory authentication, DNS, HTTP, HTTPS, file shares and Outlook ports.

Request for deviations from this configuration will be processed and approved by VITA and

may be subject to additional charges. All changes will be coordinated with Vendor to evaluate any financial or operational impact.

- **2-Factor Authentication** – this IPSec authentication mechanism is based on a login credential *and* another factor, such as a key fob. The user enters a pin (personal identification number) and the sequence number that appears on the token. Vendor will supply hard tokens which can be carried on a key chain. COV accounts are not required since the authentication mechanism differs from the one used with the single-factor solution.

The asset must be VITA-approved and have installed a VPN profile, Vendor's standard VPN client, centrally managed firewall software, and current virus definitions. This solution provides enhanced access to network resources.

Technical Assumptions

- End Users will meet the minimum requirements for the service, including use of a VITA-approved computing device with a broadband connection (i.e., DSL, Ethernet, or cable).
 - VITA will provide a minimum of two (2) weeks advanced notice prior to requesting remote access VPN services (either single factor or 2 factor) for large quantities of users (50 or more).
 - Vendor may reassign key fobs and tokens as long as the new End User belongs to the same agency as the previous user.
-