



Amendment Approval Form

Contract Between:

Northrop Grumman Systems Corporation

7575 Colshire Drive
McLean, VA 22102-7508

and

The Commonwealth of Virginia

11751 Meadowville Lane
Chester, VA 23836

Contract Number	VA-051114-NG
Amendment Number	103
Description of Contract Change – Provide a brief description of contract change	Enterprise deployment of dual-factor authentication.
Section(s) of CIA Referenced – Identify section(s) of CIA modified, including Attachments and Schedules	<ul style="list-style-type: none">• Appendix 3 to Schedule 3.3 (Security Services SOW)• Addendum 6 to Appendix 3 to Schedule 3.3 (Enterprise VPN Services)• Schedule 10.1 (Fees)

This is Amendment No. 103 to the Comprehensive Infrastructure Agreement between the Commonwealth and Vendor originally dated as of November 14, 2005 and as subsequently amended (hereinafter, "Amendment No. 103"). The Commonwealth and Vendor have agreed to modify the Comprehensive Infrastructure Agreement as set forth below. Except as expressly modified in Amendment No. 103, the terms and conditions of the Agreement shall remain in full force and effect. Capitalized terms used but not defined in Amendment No. 103 shall have the meanings assigned to them in the Agreement.

1. In Appendix 3 to Schedule 3.3 (Security Services SOW), the first sentence of Section 3.1.5.5 is deleted in its entirety and replaced with the following.

"Vendor will provide enterprise-level VPN in accordance with Addendum 6 to Appendix 3 to Schedule 3.3 (hereinafter, "Enterprise VPN")."

2. In Appendix 3 to Schedule 3.3 (Security Services SOW), all references to "key fobs" in Section 3.1.5.5 are changed to "tokens."
3. Addendum 6 to Appendix 3 to Schedule 3.3 (Enterprise VPN Services) is deleted in its entirety and replaced with the attached Exhibit A.
4. In Schedule 10.1 (Fees), a new Section 5.3.19 is added as follows.

"5.3.19 Fees for Enterprise VPN

Vendor will make a one-time bulk purchase of 20,350 soft tokens, seed files, licenses, and license maintenance. The Commonwealth agrees to pay a one-time fee of \$75.00 for each soft token, which amount is non-refundable and payable in full when the soft token container file is deployed. Vendor will initially deploy approximately 17,250 soft token containers to the existing single factor authentication VPN user group. The remaining soft tokens will be deployed upon request by an Eligible Customer through the Work Request process. After such inventory is exhausted, if additional soft tokens are needed in the future, the Parties will agree on the bulk purchase price and quantity prior to such purchase.

5. In Attachment 10.1.3-A to Schedule 10.1 (Definition of Resource Units), the "Enterprise VPN 2-Factor Authentication Service" Resource Unit is deleted in its entirety and replaced with the following (the header row is shown for context only).

Security	Unit	Definition
Enterprise VPN 2-Factor Authentication Service (hard token)	Per hard token issued (One-time)	Assessed for each issuance of a hard token. Fee assessed for initial issuance, refresh, or replacement of a lost, stolen, or damaged hard token. This RU includes hardware, software and support required for the two-factor authentication Service.
Enterprise VPN 2-Factor Authentication Service (soft token)	Per soft token issued (One-time)	Assessed for each issuance of a soft token container file. Fee assessed for initial issuance, refresh, or replacement of a lost or stolen soft token. This RU includes soft token seed files, licenses and license maintenance.

6. In the remaining Attachments to Schedule 10.1 (Fees), all other references to the "Enterprise VPN 2-Factor Authentication Service" Resource Unit are changed to "Enterprise VPN 2-Factor Authentication Service (hard token)."

7. In Attachments 10.1.4-B (Additional Resource Unit Baselines), 10.1.5-A (Post-Transition Phase Fees and Baseline Resource Unit Rates by Service Tower), 10.1.7 (Post-Transition Phase Fees – Additional Resource Charges (ARC) Rates by Service Tower), and 10.1.8 (Post-Transition Phase Fees – Reduced Resource Credits (RCC) Rates by Service Tower) to Schedule 10.1, a new row is inserted after *Enterprise VPN 2-Factor Authentication Service (hard token)* with the title "Enterprise VPN 2-Factor Authentication (soft token)," and the values for the periods prior to Contract Year 8 Stub shall be "N/A," and the values for Contract Years 8 Stub through 13 shall be "TBD."

The Parties have executed this Amendment No. 103 on the dates indicated below.

VITA for the Commonwealth of Virginia	Northrop Grumman Systems Corporation
By: 	By: 
Name: Francine C. Barnes	Name: Roxanne Esch
Contract Manager	Director, Contracts
Date: 	Date: 

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

After July 1, 2014 single-factor authentication will only be available by VITA-granted exception. After the execution of Amendment No. 103, Vendor will begin converting those existing remote access users with single-factor authentication to dual-factor authentication using soft tokens over the time period as specified in the VITA-approved project plan. New Enterprise VPN users will request a token through the Work Request process using a standard form that VITA and Vendor will develop.

Technical Description

Single Factor Authentication – Single factor authentication relies on a user’s login ID and password and synchronization between Active Directory and the DIRSYNC database. A token is not required.

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. An Eligible Customer may request a deviation from the standard configuration, subject to VITA and Vendor approval.

Dual Factor Authentication – Enterprise VPN incorporates the use of dual-factor authentication for network access as well as the use of network appliances that operate in redundant failover mode to support load balancing and load sharing. Enterprise VPN service requires the End-User to use two factors to enable network access. The first of these factors is the ID and password. The second is either a hard token or soft token. The End-User enters a pin and the sequence number that appears on or is provided by the token.

Requirements

- Commonwealth-requested changes to the second authentication factor (e.g., brand of token) may result in additional charges.
 - If a hard token is used, the End-User will meet the minimum requirements for the service, including use of a VITA-approved computing device with a broadband connection (i.e., DSL, Ethernet) and use Vendor’s standard VPN client. If a soft token is used, the connecting computer device must be a Vendor-provided computing device and have a VPN profile, Vendor’s standard VPN client and centrally managed firewall software, and current virus definitions installed.
 - VITA will provide a minimum of two weeks advance notice prior to requesting remote access VPN services for 50 or more End-Users.
 - Tokens have a limited lifespan, not to exceed four years. Upon expiration of a token, the Eligible Customer must request a replacement token through the Work Request process.
 - Vendor will not track Enterprise VPN Services and associated assets or software in any Vendor asset management system, electronic software distribution or electronic inventory system, including Altiris, LANDesk, or the Commonwealth’s TEAMS. However, Vendor will use the RSA server to generate an automated report on the quantity of tokens available for distribution and deliver it to VITA twice per month.
 - Tokens are typically delivered to the End-User two to four weeks from the date VITA approves the Work Request.
 - Vendor and VITA will agree on the threshold at which Vendor will order additional tokens. This will be based on the distribution rate tokens are deployed.
-