



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 | 104 |
| Description of Contract Change – Provide a brief description of contract change | Enterprise deployment of hard drive encryption. |
| Section(s) of CIA Referenced – Identify section(s) of CIA modified, including Attachments and Schedules | <ul style="list-style-type: none">• Addendum 3 to Appendix 1 to Schedule 3.3 (DSS Shared Services)• Appendix 5 to Schedule 3.3 (Desktop Computing Services SOW)• Addendum 7 to Appendix 5 to Schedule 3.3 (Hard Drive Encryption for Workstations)• Schedule 10.1 (Fees) |

This is Amendment No. 104 to the Comprehensive Infrastructure Agreement between the Commonwealth and Vendor originally dated as of November 14, 2005 and as subsequently amended (hereinafter, "Amendment No. 104"). The Commonwealth and Vendor have agreed to modify the Comprehensive Infrastructure Agreement as set forth below. Except as expressly modified in Amendment No. 104, the terms and conditions of the Agreement shall remain in full force and effect. Capitalized terms used but not defined in Amendment No. 104 shall have the meanings assigned to them in the Agreement.

1. In Addendum 3 to Appendix 1 to Schedule 3.3 (DSS Shared Services), the sentence following the heading "*Hard Drive Encryption for Workstations (HDEW) - DSS Shared Services*" is deleted in its entirety and replaced with the following.

"Vendor will provide enterprise-level hard drive encryption for DSS Workstations in accordance with Section 3.1.9 of Appendix 5 to Schedule 3.3 (Desktop Computing Services) inclusive of on-site support as necessary. The HDEW Resource Unit and the HDEW DSS Shared Services Resource Unit will apply, as well as the Installation for HDEW Resource Unit."

2. Addendum 7 to Appendix 5 to Schedule 3.3 (Hard Drive Encryption for Workstations) is deleted in its entirety and replaced with the attached Exhibit A.
3. In Attachment 10.1.4-B to Schedule 10.1 (Additional Resource Unit Baselines) the values for Contract Years 9 through 13 for the "*Hard Drive Encryption for Workstations (HDEW)*" Resource Unit are deleted in their entirety and replaced with the following (the header row is shown for context only).

| Year 9 | Year 10 | Year 11 | Year 12 | Year 13 |
|--------|---------|---------|---------|---------|
| 16,204 | 16,204 | 16,204 | 16,204 | 16,204 |

4. In Attachment 10.1.5-A to Schedule 10.1 (Post-Transition Phase Fees - Fixed Recurring Fees and Baseline Resource Unit Rates by Service Tower) the values for Contract Years 9 through 13 for the "*Hard Drive Encryption for Workstations (HDEW)*" Resource Unit are deleted in their entirety and replaced with the following (the header row is shown for context only).

| Year 9 | Year 10 | Year 11 | Year 12 | Year 13 |
|--------|---------|---------|---------|---------|
| 3.00 | 3.00 | 3.00 | 3.00 | 3.00 |

5. In Attachment 10.1.7 to Schedule 10.1 (Post-Transition Phase Fees - Additional Resource Charges (ARC) Rates by Service Tower) the values for Contract Years 9 through 13 for the "*Hard Drive Encryption for Workstations (HDEW)*" Resource Unit are deleted in their entirety and replaced with the following (the header row is shown for context only).

| Year 9 | Year 10 | Year 11 | Year 12 | Year 13 |
|--------|---------|---------|---------|---------|
| 3.00 | 3.00 | 3.00 | 3.00 | 3.00 |

6. In Attachment 10.1.8 to Schedule 10.1 (Post-Transition Phase Fees - Reduced Resource Credits (RRC) Rates by Service Tower) the values for Contract Years 9 through 13 for the "*Hard Drive Encryption for Workstations (HDEW)*" Resource Unit are deleted in their entirety and replaced with the following (the header row is shown for context only).

| Year 9 | Year 10 | Year 11 | Year 12 | Year 13 |
|--------|---------|---------|---------|---------|
| 1.41 | 1.41 | 1.41 | 1.41 | 1.41 |

The Parties have executed this Amendment No. 104 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 7 TO APPENDIX 5 TO SCHEDULE 3.3
TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
HARD DRIVE ENCRYPTION FOR WORKSTATIONS**

Statement of Technical Approach for Hard Drive Encryption for Workstations Service

Vendor's Hard Drive Encryption for Workstations (HDEW) service offers the Commonwealth hard drive encryption, HDEW product with Single Sign-On (SSO) synchronization capability with the Windows operating system sign-on and features configured for the Commonwealth's enterprise. The scope of Vendor's HDEW solution applies to all desktop, laptop, and tablet workstations managed and operated by the Vendor, whether owned by Vendor or the Commonwealth.

Beginning on July 1, 2014, the Commonwealth requires HDEW on all laptop and tablet Workstations and within 45 days after the execution of Amendment No. 104, Vendor will begin converting all existing unencrypted laptops and tablets to HDEW using remote-silent install, or local install if necessary, at no additional charge. Existing encrypted laptops and tablets will have the existing hardware encryption removed and the HDEW software encryption local-installed on or before January 1, 2015.

Technical Description

HDEW uses a McAfee desktop encryption software product for data on the hard drive of a Microsoft Windows-based Workstation running the minimum Vendor-supported operating system. HDEW is software that operates at the boot sector level and uses a pre-boot password to authenticate users prior to granting access to the Workstation's data. HDEW encrypts all the sectors on a disk and then, in normal operation, loads a device driver that transparently decrypts the sectors as they are needed. Once a correct password is provided by the user, HDEW program operations are performed transparently to the user. HDEW encrypts all of the data, or up to eight partitions, on a computer's hard disk, using the 256-bit Advanced Encryption Standard. If a user attaches files in an email from a hard drive that is encrypted, those file attachments will not be encrypted. The user that receives that email with those file attachments will be able to successfully open the file attachments.

Assumptions

Variance in infrastructure, technology and environmental factors among the Eligible Customers will present need-based requirements. Therefore, the technical approach for this HDEW is based on those environmental characteristics established in the analysis for this solution. Additionally, it is necessary to capture assumptions across all aspects of the implementation and deployment plan that are elemental for this service offering and awareness among stakeholders.

Limitations

The following limitations apply to HDEW.

- HDEW only supports full-disk encryption
- HDEW is only for desktop, laptop, and tablet Workstations configured with a Windows OS
- HDEW supports systems with only a single hard drive; no additional hard drives or attached removable media can be present during installation and encryption
- Workstations with existing hard disk encryption software will need to have the existing encryption software removed prior to installing HDEW
- Changes to the settings for the HDEW standard package based on changes to Commonwealth approved, security standards may be subject to additional costs
- Installation-related activities are defined as the requirements gathering, preparation, backup and recovery (if requested), installation, testing, and End-User orientation.

Addendum 7 to Appendix 5 to Schedule 3.3 to the Comprehensive Infrastructure Agreement
Hard Drive Encryption for Workstations

- After partitions have been encrypted, the partitions must not be modified as modifying the partitions will result in corruption of data or hard disk failure
- Boot-time defragmenters must not be run on encrypted Workstations as it will cause hard disk failure
- Boot sector virus protection must be disabled (BIOS and/or software) prior to installation of HDEW as the HDEW software installation will modify the boot sector. Once HDEW has been installed, boot sector protection can be re-enabled; however other software utilities must not be permitted to modify the boot sector.

Technical Solution

HDEW Settings

The standard HDEW enterprise package will use Vendor's HDEW settings to meet the Commonwealth then-current security standards. Using a standard enterprise package will allow computer support personnel to use the same tools to access or repair a desktop, laptop, or tablet workstation. An outline of Vendor's HDEW settings is listed below:

- Two grace restarts are allowed before an End-User is forced to create a HDEW password and complete the initial encryption
- HDEW will support single sign-on (SSO), if available
- An End-User cannot decrypt the drive once it has been encrypted
- All disk space on the designated hard-drive will be encrypted by default during initial encryption. If the /depot switch is used (only to be used by distribution centers for deployment of new machines), then only disk space that contains data will be encrypted during initial encryption.
- "Recovery After Power Loss" is enabled by default during initial encryption. If the /depot switch is used (only to be used by distribution centers for the deployment of new machines), then this option is disabled.
- An End-User will prove authenticity to Helpdesk administrators when requiring password resets

Technical Approach Analysis

Technical Approach

Each Eligible Customer requesting HDEW services presents a unique set of requirements therefore, to deliver HDEW to desktop, laptop, or tablets of various types, resources and applications loads, the Vendor has established the following technical approach to accommodate installation requests from any Eligible Customer across the Commonwealth. Vendor will deploy HDEW as either a local install or remote-silent install as specified below.

Local Install

Local installation requires the End-User or an administrator to be physically present at the desktop, laptop, or tablet Workstation to initiate the installation and restart the desktop, laptop, or tablet Workstation. During initial encryption, the HDEW product uses a redundant algorithm to protect data loss in case of a power outage and encrypts the entire hard drive, whether there is data present or not. This results in an average initial encryption time of one (1) hour per Gigabyte (GB). For example, installing the package on an eighty (80) GB drive will take about (80 hours) to encrypt. During this time, an End-User may continue to use their desktop, laptop or tablet workstation as normal (including

shutting down and restarting), however, there may be noticeable degradation in performance until the encryption is complete. This will be the primary install approach for all DSS Shared Support Sites and instances where Vendor's automated software deployment tools do not work.

Remote-Silent Install

Unlike the local-install approach, the remote-silent install approach does not require the End-User or an administrator to be physically present at a desktop, laptop, or tablet Workstation. Remote-silent install uses Vendor's enterprise-level automated software deployment tools. A standard HDEW package will be created using Vendor's settings. Using an enterprise package can standardize the install across the enterprise and allow computer support personnel to use the same tools to access or repair a system.

Pre-encrypted Desktop, Laptop, or Tablet Workstation Distribution (Depot) Approach

Pre-encryption requires using the bundled HDEW user program with a command line that temporarily assigns a default account. This allows an administrator to pre-encrypt the hard drive (all partitions will be encrypted) before distributing a desktop, laptop, or tablet Workstation to End-User. End-User completes the other elements of the setup after he or she receives the desktop, laptop, or tablet Workstation. When HDEW is installed with the depot option, the redundancy algorithm is not used. Also, only the data currently on the hard drive is encryption (any data later encrypted). This results in an average encryption time of four minutes per GB. For example, a depot install of the package on an eighty GB drive with five GB of data, will take approximately twenty minutes to encrypt.

HDEW Support

VITA enterprise network connectivity is required for all Workstations receiving the encryption service. VITA will encourage agencies to ensure all Workstations are connected to the Commonwealth network at least every fourteen Business Days for a period of time necessary in order to receive appropriate maintenance in support of security policy and contractual requirements. Vendor recommends a connection for a minimum of one Business Day.

All support for HDEW will be handled by the Helpdesk. The Helpdesk will be trained to provide End-User assistance with:

- End-User password recovery using a challenge response format (e.g., End-User provides a set of numbers to the technician, who then generates a one-time password key and returns it to the End-User; the End-User will then be able to change the password and regain access to the computer).
- HDEW installation and troubleshooting
- Encrypted hard disk recovery
- Direct End-User to HDEW FAQs and procedural information accessible via web-browser

Service Delivery staff will provide general desk-side support of HDEW for End-Users as required and determined by Helpdesk support.

Communications Plan

A communications plan will be executed for the Helpdesk, Service Delivery technical support and End-Users as applicable or required. Communications include product availability, benefit, End-User orientation, installation and support procedures, and FAQs.