

EXHIBIT M to Amendment No. 60
ADDENDUM 7 TO APPENDIX 5 TO SCHEDULE 3.3 TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
HARD DRIVE ENCRYPTION FOR WORKSTATIONS

**ADDENDUM 7 TO APPENDIX 5 TO SCHEDULE 3.3
TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT
Hard Drive Encryption for Workstations**

Statement of Technical Approach for Encryption Hard Drive Encryption for Workstations Service

Vendor's Hard Drive Encryption for Workstation (HDEW) solution offers the Commonwealth hard drive encryption, HDEW product with limited Single Sign-On (SSO) synchronization capability with the Windows operating system sign-on and configurable features 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.

Technical Analysis

Technology Overview

HDEW is a full-disk encryption solution designed to protect all data on the hard drive of a Microsoft Windows-based machine. A pre-boot password authentication ensures that only authorized individuals will have access to the computer's data. HDEW encrypts each sector of the disk drive if desired. It operates at the boot sector level and works on computers that run at minimum Windows XP SP1&2 and Windows 2000 SP4. The software 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 password is provided by an authorized user, program operations are performed transparently to the user. HDEW is designed to encrypt all of the data, or up to eight partitions, on a computer's hard disk, using the 256-bit Advanced Encryption Standard (AES, or the Rijndael algorithm). Since HDEW operates at the pre-DOS level, access is controlled via a logon that is required before Windows starts up. After the initial encryption, HDEW works transparently with other applications to encrypt data as it is created on the hard disk. When the user accesses files, the data is decrypted and then re-encrypted on-the-fly. Encryption on-the-fly should have no impact on a computer's normal operation. All files that are "in use" by the operating system (or software applications) are unencrypted on-the-fly as needed; this means that when data is copied to an external share, external hard drive, burned to a CD or DVD, or files attached within emails, it will not be encrypted. For example, if a hard drive is encrypted and then files from that drive are burned to a CD, the files on the CD will not be encrypted. 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.

Technical Approach Analysis

Each Eligible Customer requesting HDEW services presents a unique set of requirements. To deliver HDEW to desktop, laptop or tablet workstations of various types, resources and application loads, the Vendor has established the following technical approach to accommodate installation requests from any Eligible Customer across the Commonwealth:

Local Install Approach

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 eighty (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 initial encryption is complete.

Remote Silent Install Approach

This approach is similar to the local install approach except this approach does not require the End-User or an administrator to be physically present at a desktop, laptop, or tablet workstation. This approach allows for deployment scenarios with enterprise-grade deployment tools such as Altiris. A standard HDEW package will be created using Vendor's recommended 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 desktop, laptop, or tablet workstations to End-Users. End-Users complete the other elements of the setup after they receive 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 encrypted (any data later written to the drive after the initial encryption process is completed will, of course, be encrypted). This results in an average encryption time of four (4) minutes per GB. For example, a depot install of the package on an eighty (80) GB drive with five (5) GB of data, will take approximately twenty (20) minutes to encrypt.

Assumptions

Variance in infrastructure, technology and environmental factors among the Eligible Customers will present need-based requirements on a case-by-case basis. Therefore, the technical solution as recommended in this document will articulate the mode of HDEW service delivery 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 to this service offering and awareness among the stakeholders.

- HDEW is only for desktop, laptop and tablet workstations configured with a Windows Operating System
- HDEW supports systems with only a single hard drive and no additional hard drives or attached removable media can be present during installation and encryption
- Systems with existing hard disk encryption software will need to have their 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 requirements gathering, preparation, backup and recovery (if requested), installation, testing, and End-User orientation
- 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 desktop, laptop and tablet 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 recommended by Vendor

The standard HDEW enterprise package will use Vendor's recommended 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 system. An outline of the Vendor's recommendations is listed below:

- Five incorrect logon attempts are allowed before the One Time Password feature is enabled
- Two grace restarts are allowed before End-Users are forced to create their HDEW user name and password and complete the initial encryption
- The service will support limited single sign-on (SSO) and will synchronize the HDEW user name and password to match the Windows "short-name" name and password if they are changed. SSO is currently available for all End-User desktop, laptop, or tablet workstations that have not migrated to the Active Directory domain as current application restrictions impede the ability to utilize the Active Directory user sign-on ID naming convention.
- End-Users cannot decrypt the drive once it has been encrypted
- Automatic HDEW account expiration is disabled
- Initial encryption speed is set to "Fast"
- 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 the 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
- Authenti-Check questions have been disabled as One Time Password will be used for password recovery and End-Users will prove authenticity to Helpdesk administrators when requiring password resets

HDEW Support

- VITA enterprise network connectivity is required for all workstations receiving the encryption service. VITA is required to ensure all workstations are connected to the Commonwealth network at least every fourteen (14) business days for a period of time necessary to receive appropriate maintenance in support of security policy and contractual requirements. Vendor recommends a connection for a minimum of one (1) 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 user; the user will then be able to change their password and regain access to their computer).
 - HDEW Installation and troubleshooting
 - Encrypted hard disk recovery
 - Direct End-Users to HDEW Frequently Asked Questions (FAQ) 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.
- An administrator support ID and password will be provided to appropriate Vendor support staff on an individual basis as required. A record of all distributed administrator IDs and passwords will be maintained.
- The passwords associated with the administrator support IDs will be modified on a periodic basis and/or following their distribution, in order to maintain compliance with Commonwealth Security Policies as agreed upon between the Commonwealth and Vendor. Electronic software distribution of the updated configuration file will be the vehicle used for modification. A list of scheduled workstations not receiving the update due to network connectivity issues will be provided to VITA for disposition following the estimated completion date of the deployment.

Communications Plan

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