



Australian Government
Department of Defence
Intelligence, Security and
International Policy

Laptop With High Grade Silicon Data Vault Hardening Guide

Defence Signals Directorate

Release Date: March 2009

Table of Contents

Table of Contents	2
Overview	3
Guidance for Laptop Hardening	4
Overview	4
Laptop Recommendations.....	5
Guidance for High Grade Silicon Data Vault Users	7
Overview	7
Guidance for ITSAs	9
Guidance for HGSDV System Administrators.....	10
Guidance for HGSDV Users (incl. System Administrators).....	13

Overview

Introduction This document provides technical guidance on how to harden a laptop containing a High Grade Silicon Data Vault (HGSDV). Included in this document are instructions for configuring the HGSDV, itself, to make it as secure as possible.

Other Documentation Other documentation that should be read in conjunction with this document that relates to the HGSDV includes:

Document	Location
Australian Government ICT Security Manual (ISM) (formerly known as ACSI 33)	Available at: http://www.dsd.gov.au/library/infosec/ism.html
DSD's Consumer Guide: Secure Systems' High Grade Silicon Data Vault	Available at: http://www.dsd.gov.au/library/pdfdocs/cons_guide/HGSDV.pdf
DSD Best Practices Guide: High Grade Silicon Data Vault	Please contact DSD for a copy of this document. Email: assist@dsd.gov.au Phone: (02) 626 50197

Versions This document relates to the following HGSDV version:

Note: nn is the size in gigabytes (GB) of the HGSDV HDD, e.g. 60 GB.

HGSDV Version	Part Number
SDV182A	SDV182A03MW3-nn-0104

Contents This document contains the following sections:

Section	See Page
Guidance for Laptop Hardening	4
Guidance for High Grade Silicon Data Vault Users	7

Guidance for Laptop Hardening

Overview

Introduction

The information in this section is provided to give System Administrators direction with regard to setting up a laptop that will contain a HGSDV to limit the opportunity for classified data to be removed from the laptop by a person not cleared to gain access to that data.

Contents

This chapter contains the following topics:

Topic	See Page
Laptop Recommendations	5

Laptop Recommendations

Seals

Security seals meeting ISM requirements when placed over the hard drive bay, access screws, RAM bay, docking port, and communications ports will ensure that any attempts to modify or tamper with components of the laptop will be evident to users upon inspection.

BIOS Protection

Protecting the laptop BIOS with an ISM compliant password will ensure that changes can not be made to BIOS settings. Coupled with seal usage any attempt to remove the battery to return the BIOS settings to a default state will be evident to users upon inspection.

BIOS Hardening

Changing the boot order to only allow booting from the HGSDV and disabling all communications ports will prevent users from running unauthorised operating systems and using unauthorised communication mediums. Not all laptops provide the ability to modify the boot order and this should be checked prior to laptop purchase.

CD/DVD Burners

Choosing laptops with read only CD/DVD ROMs will prevent users from removing classified information from the laptops. If CD/DVD burners can not be avoided, restrictions should be made on the ability to burn CDs/DVDs.

Example: To disable native CD burning in Windows set the

```
HKEY_CURRENT_USERS\Software\Microsoft\Windows\
CurrentVersion\Policies\Explorer\NoCDBurning
```

value to “1” in the Windows registry.

Continued on next page

USB Mass Storage Devices

Configuring the operating system to prevent write access to USB Mass Storage devices will prevent users from removing classified information from the laptops via the USB port.

Example: To prevent writing to USB Mass Storage devices in Windows create the “WriteProtect” dword attribute with value “1” under the “StorageDevicePolicies” key in the

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
```

path of the Windows registry.

Peripheral Access

Using access control software or operating system controls to control access to peripherals on the laptop will provide a second layer of protection to prevent unauthorised transfer of information from the laptop.

Example: To prevent the installation of USB peripherals in Windows deny SYSTEM permissions on the

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
```

policy group in the Windows registry.

Hardening the Operating System

Using a hardened operating system that restricts user accounts to limited access will prevent users from making changes to the operating system security settings.

Examples:

- Preventing access to registry editing tools.
- Preventing access to the command line interface.
- Restricting access to install programs.
- Disabling any nonessential services.
- Locking the screen after a set period of inactivity.
- Preventing access to Ethernet, Bluetooth, infrared, serial, parallel, firewire, and wireless communication mediums.
- Using strong passwords.
- Using Anti-Virus software.

Additional advice on hardening an operating system can be found within the ISM.

Guidance for High Grade Silicon Data Vault Users

Overview

Introduction During the evaluation of the HGSDV, DSD identified a number of instructions that users of the HGSDV should be aware of that will ensure the integrity of the HGSDV product throughout its lifetime of use. The instructions are provided below.

Definitions The following definitions will be used throughout the *Guidance for High Grade Silicon Data Vault Users* section of this hardening guide.

ITSA: Information Technology Security Adviser – the person who will be responsible for the receipt of a delivery of a HGSDV.

User: any person who can authenticate and use a HGSDV, including System Administrators.

System Administrator: a User who is responsible for initialising and managing the HGSDV.

CTU: CD Token Utility – a software application provided by Secure Systems to create and manage CD Tokens that are used in conjunction with the HGSDV.

Reading this Guidance This document is written in the style of the ISM, whereby the terms MUST, MUST NOT, SHOULD and SHOULD NOT are interpreted in the following way:

Key Word	Interpretation
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reason to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS	DSD's recommendation or suggestion.

Continued on next page

Overview, Continued

Contents

This chapter contains the following topics:

Topic	See Page
Guidance for ITSAs	9
Guidance for System Administrators	10
Guidance for Users (including System Administrators)	13

Guidance for ITSAs

Guidance for ITSAs Regarding Delivery of an HGSDV

Instruction 1 ITSAs **MUST** follow the HGSDV delivery procedures, as specified by the manufacturer of the HGSDV, Secure Systems, when receiving a delivery of a HGSDV.

Guidance for ITSAs Regarding the CD Token Utility

Instruction 2 If an ITSA is provided with the CTU (CD Token Utility) software to burn CD Tokens for Users the ITSA **MUST** abide by the following guidelines:

- The random data used during token creation **MUST** be sourced from DSD.
- Tokens **MUST** be burnt in an appropriate facility and environment commensurate with the classification of the data that is to be stored on the laptop that will make use of the tokens that are burnt.

Example: An ITSA creating tokens to protect SECRET data on a laptop could burn the tokens on a stand alone laptop inside a facility that has been accredited to store information classified SECRET.

Note: Depending on the circumstances surrounding the acquisition of the HGSDV, the CTU may not be provided to the ITSA. If the CTU is not provided to the ITSA, DSD will provide CD Tokens as required.

Note: To arrange the delivery of random data or CD tokens from DSD use the following contacts:

email: assist@dsd.gov.au
phone: (02) 626 50197

Instruction 3 Before an ITSA makes use of the CTU public key option DSD **MUST** be contacted to ensure the correct implementation of this feature.

Guidance for HGSDV System Administrators

Instruction 4 The host laptop containing the HGSDV **MUST** be tamper sealed after the HGSDV has been inserted into the laptop.

Once the HGSDV has been fitted appropriately into the host laptop, seals will have to be applied to the laptop to prevent unauthorised access to both the HGSDV and the internals of the laptop.

Instruction 5 Host laptop BIOS **MUST** be password protected.

The BIOS of the laptop containing the HGSDV must be password protected in order to provide protection against tampering with the BIOS settings of the laptop.

Instruction 6 Host laptop BIOS update/flash feature **MUST** be disabled.

The BIOS of laptops may be able to be updated or flashed by users that do not have access to the BIOS. To prevent this, the System Administrator who does have access to the BIOS must disable the update/flash BIOS feature.

Instruction 7 Host laptop BIOS **MUST** be configured to boot only from the hard drive.

The BIOS of laptops may be able to be updated or flashed by users that do not have access to the BIOS. To prevent this, the System Administrator who does have access to the BIOS must disable the update/flash BIOS feature.

Instruction 8 If the System Administrator chooses to write down the Recovery Key to aid in the recovery of an HGSDV that fails the System Administrator **MUST NOT** store the Recovery Key with the laptop containing the HGSDV.

The Recovery Key may enable malicious users to gain access to protected data stored on the HGSDV hard drive and as a result must not be stored with laptop.

Continued on next page

Guidance for HGSDV System Administrators, Continued

Instruction 9 The GateKeeper (GK) and Encrypted Backup Utility (EBU) add-on product modules **MUST NOT** be enabled or used.

GateKeeper (GK) and Encrypted Backup Utility (EBU) are add-on product modules offered by Secure Systems Limited to be used in conjunction with the SDV range of products. HGSDV System Administrators must not make use of GK and EBU as they were out of the scope of the high grade evaluation process undertaken by DSD on the HGSDV.

Instruction 10 The System Administrator **MUST NOT** login to the HGSDV via the “Authentication Application” interface.

If a person wants to act as a System Administrator and a regular User for a given HGSDV that person must create for themselves two separate accounts – one System Administrator account to administer the HGSDV and one regular User account for normal use of the HGSDV. By separating the roles of System Administrator and regular User through the creation of different accounts, the risk of inadvertent compromise of the data protected by the HGSDV is significantly reduced.

Continued on next page

Guidance for HGSDV System Administrators, Continued

Instruction 11 Classified data **SHOULD NOT** be written to the hard drive in the clear

HGSDV encryption can be enabled in two ways:

1. Data can be placed on the hard drive in the clear (unencrypted form), then the encryption can be turned “on” and the entire contents of the hard disk will be encrypted.
2. Encryption can be turned on prior to data being written to the hard disk and then later when data is written to the hard disk it is encrypted as it is written to the hard disk.

If HGSDV encryption is enabled by a System Administrator as for the first scenario detailed above and the data that was initially written to disk was classified, then despite the fact that the data is subsequently encrypted the handling classification of that data will not be reduced.

Example: If CONFIDENTIAL information is written to the hard disk, then encryption is turned on and that data is subsequently encrypted, then the classification of the data and therefore the hard disk will remain at the CONFIDENTIAL classification.

Note: If classified data is written to the hard disk inadvertently, the hard disk could subsequently be sanitised using the appropriate method(s) outlined in the ISM to reduce its classification to such a point that it could be re-used. Alternatively the hard-disk could be destroyed and replaced, as long as the HGSDV seals are also replaced.

Instruction 12 The HGSDV internal partitioning tool **SHOULD** be used to partition the HGSDV hard disk.

The HGSDV internal partitioning tool (available from the System Administration Utility) provides a simple mechanism to partition the HGSDV hard disk according to the specifications of the product. System Administrators may partition the hard disk without using the HGSDV internal partitioning tool. System Administrators who do choose to partition the disk themselves should be aware that if they use a non-standard partitioning scheme for the HDD the HGSDV may be unusable.

Continued on next page

Guidance for HGSDV Users (incl. System Administrators)

Instruction 13 CD Tokens **MUST NOT** be stored with the laptop containing the HGSDV.

The CD Token used by a User or System Administrator to authenticate to the HGSDV is an integral part of the security of the HGSDV. As a result, the CD Token must be stored away from the HGSDV once a successful authentication has been achieved to ensure the security of the HGSDV remains as strong as possible. Furthermore the CD Token must only be used for authentication purposes.

Instruction 14 User and System Administrator passwords **MUST NOT** be written down and stored with the laptop containing the HGSDV.

The password (also known as the passphrase) used by a User or System Administrator to authenticate to the HGSDV is an integral part of the security of the HGSDV. As a result, the password must not be written down and stored with the HGSDV to ensure the security of the HGSDV remains as strong as possible.

Instruction 15 DSD **RECOMMENDS** that Users select passwords that are at least 12 characters long.

The length and complexity of a password governs how difficult it will be to guess. DSD recommends that people select passwords that are at least 12 characters with the requirement that the characters be drawn from upper case letters, lower case letters, numbers and punctuation characters.
