Communications Security Establishment
Centre de la sécurité des télécommunications

IT Security Guidance

CLEARING AND DECLASSIFYING ELECTRONIC DATA STORAGE DEVICES

JULY 2006

ITSG-06

Canada

This page intentionally left blank.

Foreword

The *Clearing and Declassifying Electronic Data Storage Devices (ITSG-06)* is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

Requests for additional copies or changes in distribution should be directed to your Client Services Representative at CSE.

For further information, please contact CSE's ITS Client Services area by e-mail at client.svcs@cse-cst.gc.ca or call (613) 991-7600.

Effective Date

This publication takes effect on July 2006.

Sue Greaves
Director, IT Security Mission Management

This page intentionally left blank.

Table of Contents

List of Tables

1 Introduction

1.1 General

This guideline is intended to assist Government of Canada IT authorities in the selection of suitable methods to prepare Electronic Data Storage Devices (EDSD) for declassification, reuse or disposal. This guideline outlines the baseline standards approved by the RCMP and CSE for clearing and sanitizing different types of EDSD, and describes a range of methods to meet those standards. Methods are recommended based on specified levels of data sensitivity within a range of typical GoC operating environments.

1.2 COMSEC Exceptions

This guideline does not apply to Communications Security (COMSEC) equipment and/or key materiel. Refer to relevant Canadian Cryptographic Doctrine (CCD) manuals for COMSEC handling instructions.

1.3 Government Security Policy

The Government of Canada Security Policy (GSP) requires that federal departments and agencies establish and implement a security program that covers organizational, physical and personnel security as well as information technology security. While the GSP is supported by operational and technical security standards that define baseline security requirements, the GSP makes departments and agencies responsible for detailed implementation. In addition, departments and agencies must conduct their own Threat and Risk Assessments (TRA) to determine the need for safeguards above baseline levels specified in the standards.

The GSP requires departments and agencies to conduct active monitoring and assessments of their security program. In order to assess policy compliance and to provide feedback on the effectiveness of the policy, departments are required to provide reports to the Treasury Board Secretariat on the results of these internal assessments or audits. It is crucial that departments understand the security requirements for the handling of information processing and storage devices that contain Protected or Classified information. The minimum requirements for the clearing, sanitization and destruction of EDSDs, as described in this document, have been approved by the Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP).

The Access to Information Act and the Privacy Act (ATIP) should be read, along with the GSP and its supporting Operational Standards, for a more detailed discussion on the classification and handling of Protected and Classified information.

1.4 Departmental Requirements & Considerations

Departments and agencies are required to perform TRAs to consider the unique circumstances of each user group in light of the complex nature of the threat environment and the rapid rate of change in electronic data storage technology.

To ensure that sensitive information is not compromised or exposed, proper control of sensitive EDSDs must be maintained at all times by users and managers. Departmental security policies should address the requirement for procedures for labelling, storing, declassifying/downgrading, destruction and/or erasure of sensitive materiel.

1.5 Data Retention and Audit Requirements

Departments must address legal and policy requirements for data retention periods and audit, etc, before approving media for erasure or destruction. This includes:

- legal requirements under the Access to Information and Privacy Acts (ATIP) regarding retention of public records;
- policy requirements under relevant TBS information management policies regarding the keeping of government records;
- security audit requirements for data retention that could be required as evidence in investigative or legal proceedings; and
- security audit requirements to maintain complete records of destruction and disposal of government records, information and equipment.

1.6 Sensitivity Labels

EDSDs that are used to store sensitive information should be appropriately labelled in accordance with relevant GSP Operational Standards. The labels should be retained until the sensitive information is declassified, downgraded or erased by trustworthy means – or until a point in time immediately preceding the physical destruction of the media.

1.7 Structure of the ITSG-06

This guideline is divided into four (4) sections:

1. ***Introduction*** - This section provides background information pertaining to the proper disposal and/or re-use of information processing devices.
2. ***Clearing, Sanitization, and Destruction Methods*** – This section introduces the various methods for destruction of data and/or devices.
3. ***Handbook of Clearing, Sanitization, and Destruction Methods*** – This section describes RCMP/CSE approved destruction standards for all types of storage devices, separated into the three overall categories of magnetic, optical, and miniature storage media. For each type, the approved standard of destruction is based on the assessed sensitivity of the stored data.
4. ***Annexes*** - The Annexes provide detailed explanations of various aspects of device re-use, clearing, or sanitization.

This page intentionally left blank.

2 Clearing and Sanitization

Many security methods are used to protect sensitive data during handling and storage on IT systems. However, would-be attackers may be able to recover sensitive information from discarded storage media. This guideline addresses security issues related to the change of use or disposal of electronic data storage devices (EDSD), and the methods for properly destroying stored data to reduce or eliminate the threat of unauthorized access.

2.1 Clearing

Clearing is the process of erasing an EDSD in a manner that allows it to be re-used within an equivalent or higher security environment.

Clearing must be adequate to prevent data recovery using tools normally available on the Information System. Simply deleting or erasing the files or formatting a disk does not clear the media, because commands such as undelete or unformat may permit the recovery of the data. The clearing process is not expected to be proof against "hands-on" recovery methods using specialized IT utilities or laboratory techniques. For this reason, cleared media must be retained within security environments appropriate to the highest level of data the media once contained, and cannot be considered for declassification.

2.2 Sanitizing

Sanitizing is the process of erasing or destroying an EDSD in a manner that precludes any reasonable hope* of recovery of the data – i.e., the risk of compromise following sanitization is low or non-existent. In addition to destroying the data, the sanitization process includes the manual removal of external indications that the device once contained sensitive data. EDSDs that have been sanitized may be declassified and disposed of as unclassified waste or as surplus equipment for sale or recycling.

> **Reasonable hope: if a threat agent with opportunity, motivation and capability believes the presumed value of the data is worth the time and cost to attempt to recover it.*

2.3 Clearing and Sanitization Methods

2.3.1 Encryption

Encryption of the entire media (not just files and folders) over the life cycle of the media – using encryption products that have been approved by CSE for that particular application and for the level of

sensitivity of the data being stored, may be considered "equivalent to sanitizing" prior to end-of-life disposal of the media. In the case of a laptop, for example, the encryption provides some assurance of protection of the data even in the event of loss or theft of the device. For routine disposal, however, the encryption should be supplemented by an approved overwrite process to preclude any possibility that an attacker could recover the decryption key from the hard drive.

The effectiveness of encryption in providing ongoing protection of the data depends on three factors: the strength of the cryptographic protection scheme as implemented by the vendor; the management of the encryption key by the user organization; and the avoidance of attack motivators. Given opportunity and time, a capable adversary may recover the data if sufficiently motivated to make the effort. Approved* encryption methods are a deterrent because they ensure that the level of effort involved in recovery will exceed the expected value of the data to be recovered.

> **Commercial products often have serious weaknesses in their underlying encryption schemes. CSE validation ensures that such weaknesses are found - and the vendor is notified to correct the problem – prior to approval for Government use.*

2.3.2 Overwriting

Overwriting is the removal or erasure of information from a storage device by writing "1" and/or "0" data bits to all storage areas of the device, thus replacing any existing intelligence bits.

The effectiveness of this method depends on the number of overwrite cycles (to overcome the track-edge phenomenon1), the skill and knowledge of the person conducting the overwrite process, and overwrite software verification features (if any) to help ensure that overwrite is accomplished over the entire accessible storage area of the media.

Triple Overwrite. Triple overwrite is a process involving three passes of the overwrite software. In accordance with RCMP overwrite criteria, the first pass must write all 1s or all 0s to the media, the second pass must write the complement (or opposite) of the first pass, and the third pass must be a pseudo-random pattern that the human operator can read back to verify results.

1 Track-Edge Phenomenon: Data remnants can remain at track boundaries (edges). The read-write heads do not always pass concentrically over the exact centre of the original bit pattern - mostly due to mechanical and electrical variables and tolerances. The result is that residual "track edges" of the original bit patterns are left on the disk platter even though the bulk of the track will have been overwritten.

Secure Erase. Since about 2001, all ATA IDE and SATA hard drive manufacturer designs include support for the "Secure Erase" standard2. However, SCSI and Fibre Channel hard drives do not support the Secure Erase standard and can be overwritten only by using third-party software products.

- *RCMP overwriting standards*: choose a software product that meets RCMP overwrite criteria3 and that has undergone an independent laboratory analysis, e.g., tested to a relevant profile under the Common Criteria.
- *Verification features*: ensure the product has software features that help the operator to determine whether or not the overwrite software is able to access (and has accessed) the entire known storage area of the disk.

Overwriting as a Stand-Alone Method. For magnetic storage media such as hard disks and tape, etc, triple overwrite is recognized as a stand-alone method for destruction of data at the level of Protected B and below, and may be deemed suitable for Confidential as well.

Overwriting in Combination with Other Destructive Methods. For magnetic storage media that contains Protected C or Classified information higher than Confidential, triple overwrite is not suitable as a stand-alone data destruction method. However, in combination with other incomplete destruction procedures such as disintegration or shredding, a triple overwrite may provide additional assurance that information is destroyed beyond reasonable hope of recovery.

2.3.3 Degaussing

Degaussing is the application of magnetic force of sufficient power to erase all data on a given magnetic data storage device. The effectiveness of this method depends on the relative strength of the magnetic force available in the degausser product and the magnetic retention properties of the data storage device. Degausser products4.must be properly maintained and operated to be effective.

---

2 Secure Erase: a standard developed by the University of California San Diego (UCSD) Center for Magnetic Recording Research (CMRR) and subsequently adopted by hard drive manufacturers to enable user organization security staff to effect sure and simple erasure of all accessible parts of the hard-drive prior to disposal. See Annex B and Annex H.

3 RCMP criteria for disk overwrite: Sanitize a drive via triple overwrite using the RCMP DSX utility software or third-party equivalent (or "Secure Erase" if the hard drive supports the Secure Erase standard). In general, overwrite software must make three passes - the first two write binary 0s; the second to write binary 1s; and the third to write an ASCII text pattern that the operator can later verify.. For example, the text pattern could comprise the name of the overwrite software product, along with the version number and current timestamp.

4 Degaussing: When using a degausser, the operator must be aware of the strength of the degaussing device versus the actual magnetic retentivity (or "coercivity" as measured in Oersteds) of the magnetic media. The operator must ensure that the

2.3.4 Physical Deformation

Physical deformation involves the use of tools such as sledge hammer, nail gun, vice, etc, to cause extreme physical damage to a storage device in order to delay, impede, or discourage an attacker from attempting to recover data from it. In the case of magnetic disks, the effectiveness of this method depends on the amount of damage inflicted on the surface of each platter (including warping of the flat surface) to make it very difficult to do a laboratory analysis – plus the obscurity provided by ensuring that remnants of sensitive disks are indistinguishable from remnants of other destroyed media. See Annex B for acceptable physical deformation techniques.

2.3.5 Shredding and Disintegration

Shredders. Shredding is a form of destruction that is accomplished by reducing the media to small pieces of uniform size and shape. The use of shredders is typically limited to sheet stock or thin media such as CDs and DVDs. Shredders are approved on the basis of the size and shape of the resulting strips or particles that the cutters produce.

Disintegrators. Disintegration is accomplished by a non-uniform cutting or shredding mechanism (e.g., rotating blades within a closed container) that reduces the media to pieces of random size and shape. Disintegrators are suitable for a variety of media of almost any size. A screen is utilized on the output side to catch oversize pieces, which are returned for more shredding. The RCMP approves disintegrators - on the basis of screen size - for various types of EDSDs and for various levels of sensitivity,.

Machine Requirements. If considering an external destruction service, Departments should contact the RCMP for advice. To qualify as valid destruction, the disintegration or shredding must reduce the media to pieces that meet the maximum acceptable size as determined by a particle filter. The particle filter would be selected to catch oversized pieces -and return them for more shredding - while allowing smaller pieces to pass for disposal.

Procedural Requirements. Prior to destruction, security staff must remove all external labels, stickers, and other indicators denoting the present or former classification of the media contents. In all cases, Departmental security staff must witness the destruction.

selected degausser is approved for the coercivity of the media to be degaussed. Failure to do so may result in incomplete destruction of the data on the media.

2.3.6 Materiel/Molecular Separation by High-Speed Centrifuge

This is a new recycling technology available in Canada. Its potential for media destruction and disposal is under investigation.

2.3.7 Grinding and Hammer-milling

Grinding involves using a machine to grind the EDSD into small pieces.

CD Surface Grinders. Specialized CD grinders are capable of reducing the data-bearing layer of an optical disk to fine powder, while leaving the disk itself intact for recycling or disposal. However, DVDs cannot be sanitized by this method because their information-bearing layer is sandwiched in the centre. An alternative to surface grinding is the use of a special machine to punch thousands of tiny holes into the disk to destroy the data-bearing layer.

Hammer mills are durable utility grinders capable of grinding most materiel. The materiel is fed into the device and forced into repeated contact with a series of rotating, hardened hammers that do the grinding. The mill is encircled by a screen that allows only suitably small-sized particles to escape.

2.3.8 Incineration

Incineration involves the destruction of EDSDs in incinerators that are environmentally approved for plastics and other materiel.

2.3.9 Knurling

Knurling involves the use of a machine to apply pressure and heat to optical disks (CD or DVD) to elongate and curl them to a slight degree. This intent of this process is to destroy the optical “pits” and “lands” on the disk to effectively destroy the data. The potential of this process for destruction and disposal is under investigation.

This page intentionally left blank.

3 Handbook on Clearing, Sanitization and Destruction

This section provides an overview of clearing & sanitizing methods, and destruction standards, for all known types of electronic data storage devices.

Detailed explanations about the various methods and associated security issues are provided in the Annexes. In addition, Departments should consult the GSP Operational Standards and relevant CSE and RCMP guidelines regarding the proper handling of sensitive information and storage devices throughout their life cycle.

3.1 Destruction Technologies, Techniques and Equipment

Accepted destruction technologies are listed below. See Annex B for detailed explanations.

Table 1: Destruction Methods

Method	Approved Technology
Encryption	Cryptography approved by CSE for the classification level of the information on the device being destroyed.
Overwriting	RCMP overwriting criteria as per Annex B on overwriting of hard disks and other magnetic media.
Degaussing	Degaussers approved by CSE for the coercivity of the magnetic media to be destroyed.
Physical Deformation	CSE-approved methods for emergency purposes only as outlined in Annex B.
Shredding or Disintegration (with screen)	RCMP-approved equipment or standards, used in accordance with procedures in Annex B.
Grinding or Hammer Milling	RCMP-approved standards and procedures.
Materiel/Molecular Separation	No currently approved facility.
Surface Grinding (for CDs)	RCMP-approved standards and procedures
Incineration	Incinerators approved by Environment Canada for the material to be destroyed
Knurling	No currently approved facility.

Note: off-site media destruction must be closely observed by departmental security staff, and external labels that denote sensitivity must be removed prior to destruction and disposal.

3.2 Clearing for Re-Use within a Department

Single overwrite (a single pass of the overwrite software) may be used to clear magnetic disks for re-use within the Department in an equivalent or higher security environment. In this context, clearing enforces the "need-to-know" restriction within a group of users.

Downgrading Top Secret. Triple overwrite, which is more effective than single overwrite, may be used to clear Top Secret media for re-use within the Department in a Secret-level environment.

Security Issues with Overwriting:

If the overwrite process is successful, then it will be difficult for an attacker to recover data in the laboratory. However, the overwrite process is not always completely successful due to human error and/or the inability of software utilities that function at the application layer to overwrite bad sectors or hidden partitions, which may contain sensitive data. Given direct access to the hard drive, an attacker could recover that data using simple software tools, without the need of a laboratory. For these reasons, overwrite is not accepted as a stand-alone destruction method for disposal of magnetic media containing data that is extremely sensitive (Protected C or Secret and above); however, it is acceptable for "clearing" the media for re-use within a controlled security environment – i.e., within a community of users who lack the "need to know" but do have appropriate security clearances for the level of information that may continue to reside on hidden portions of the "cleared" storage media.

3.3 Sanitizing for Declassification and Disposal

Sanitize media prior to declassification for re-use in a less secure environment and/or release of the media outside the control of the government of Canada. Remove all markings or other external indications of the sensitivity of the data that was formerly stored on the media, and destroy the data or the device in accordance with the appropriate instructions5.

5 *Some adversaries have the means to do sophisticated laboratory analyses of incompletely destroyed magnetic media, and may make the attempt if they acquire magnetic media or fragments from a source of sufficient interest to justify the time and cost of laboratory analysis.*

3.4 Special Considerations – Emergency situations, and Overwriting

3.4.1 Emergency Destruction

The aim of an emergency destruction is to prevent or inhibit the recovery of sensitive information to the maximum extent possible within operational time constraints. Media should be destroyed in priority order based on the volume and level of sensitivity of stored data. As time and the availability of approved destruction facilities may be limited, normal techniques may be replaced with any practical method available. The techniques most readily available are physical deformation and incineration, which may be combined to optimize the effectiveness of the destruction.

Prior to destruction, the media devices must have all external labels, stickers, and other indicators denoting classification removed. EDSDs should be removed from host equipment if possible.

Tools for deforming magnetic or optical media include: nail gun, electric drill, vise, or sledgehammer.

For miniature or Flash memory devices, repeated and heavy blows by sledge hammer to pulverize the electronic components within the device may not destroy the actual memory chips but will effectively deter and delay recovery attempts. To further deter and delay any attempt at reconstruction, the remnants should be mixed with remnants of non-sensitive media.

3.4.2 Overwriting

For disposal of magnetic disks outside the controlled security environment, overwriting must be preceded by a comparison of the reported disk capacity (as determined by the overwrite software) versus the actual disk capacity (as calculated by the human operator). The purpose is to check for unread or hidden data repositories that cannot be accessed by the overwrite software at the application layer but could be accessible to an attacker using software tools such as a disk editor that operates at a lower level. The overwrite process itself must include a minimum of three passes including 1s, 0s, and a pseudo-random pattern over the entire accessible area of the magnetic tape or disk, followed by verification of results by the human operator.

3.4.3 Overwriting PDAs and BlackBerrys

Personal Data Assistants (PDA) are not designed to meet government security requirements. PDAs use a variety of mechanisms to restrict access to memory; however, these are rarely intended or proven to deter a laboratory attack. The question about secure disposal hinges on acceptance or not of the device's inherent safeguards against unauthorized memory access. BlackBerry PDAs offer data protection options that meet government security requirements for the protection of Protected B emails and attachments, within limits specified in various CSE bulletins and other documentation.

LOSS OR THEFT OF A BLACKBERRY UNIT:

As confirmed by CSE, the BlackBerry user data is deleted by over-writing when the maximum number of attempted passwords is exceeded or when the BES administrator successfully sends a Kill command to the device. However, if the Kill command is not received or executed, then a laboratory attack could be mounted on the memory module to read non-encrypted user data. To guard against loss or theft, therefore, departments should complement the above protections with Policies to govern the handling of the device and what types of information may be stored on it (maximum Protected A, or Protected B if the SMIME option is installed and correctly used).

MALFUNCTIONING PDAs:

As a matter of policy, departments should require the deletion of user data from all PDA devices before disposal or before returning such devices to the vendor. Unfortunately, it may not be possible to delete the user data if the device is malfunctioning and it is possible that data stored on a failed PDA device may be recoverable by parties with laboratory resources. Departments should assess the risk on a case-by-case basis, considering both the value of the data and the potential impact of disclosure. If the risk is deemed medium or high, then the device should not be released from departmental control. Instead, it should be destroyed using approved destruction methods, and the cost of replacement should be seen as a necessary security measure.

3.5 Destruction Standards - Magnetic Media

Applies to:

- Hard-disc drive (HDD)
- Floppy disks
- Magnetic tape (DAT cartridge, back-up tape, reel-to-reel, audio cassette, VHS, Beta, etc)
- Magnetic stripe cards

	Data Overwrite Declassification Standards	Overwrite Products
Unclas, PA, PB	*Disks or Tape*: Triple overwrite.	RCMP guidelines for selection of overwrite products.
C	*Disks or Tape*: Triple overwrite*****	
PC, S	*Disks or Tape*: Triple overwrite PLUS shredding/disintegration or grinding as for PA/PB.	
TS	*Disks or Tape*: Triple overwrite PLUS shredding/disintegration or grinding as for Secret.	
	Shredding, Disintegrating and Grinding Destruction Standards	**Destruction Products**
Unclas, PA, PB	*Disks*: at least 3 pieces, each maximum area < 580 mm^2 (e.g., 3x3”). *Magnetic tape***: pieces, each maximum length < 50 mm (2”). *Stripe cards*: pieces, each maximum area < 160 mm^2 (e.g., 1/2x1/2”).	RCMP Security Equipment Guide (SEG). *Note: triple overwrite may be used to downgrade TopSecret media (for subsequent disintegration or shredding as for Secret).*
PC, C, S	*Disks*: at least 3 pieces, each maximum area < 40 mm^2 (e.g., 1/4x1/4”). *Magnetic tape*: pieces, each maximum length < 6 mm (1/4”). *Stripe cards*: pieces, each maximum area < 10 mm^2 (e.g., 1/8x1/8”).	
TS	*Disks*: at least 3 pieces, each maximum area < 10 mm^2 I (e.g., 1/8x1/8”). *Magnetic tape*: pieces, each maximum length < 3 mm (1/8”). *Stripe cards*: pieces, each maximum area < 10 mm^2 (e.g., 1/8x1/8”).	
	Incineration	**Incinerators**
All Levels	Total destruction.	Facilities approved by Environment Canada for mixed plastics, etc.

	Emergency Destruction	Destruction Tools
All Levels	Refer to the Annex on Emergency Destruction.	Focused high-impact tool, vise, sledgehammer, etc.
	Degaussing	**Degaussing Products**
All Levels	Carefully follow degausser product manufacturer directions for tapes and disks. Degauss hard drives twice (for the second pass, turn the drive around in the chamber).	Degausser must be CSE-approved for coercivity of the specific media.

**Triple overwrite by itself may be deemed sufficient to declassify Confidential media. However, media containing Protected C or Secret information require additional shredding/disintegration or grinding as indicated above.*

***Exception for Digital Linear Tape (DLT): the standard for disintegration of large quantities of DLT may be relaxed to avoid disassembly for removal of internal metal rings prior to disintegration in medium-robust shredders.*

Encryption: Full-disk encryption for hard drives, or file encryption for tapes, using encryption products approved by CSE for that purpose and for the level of sensitivity of the stored data, provides reliable protection for data at rest (device turned off or user not logged on) and is an effective deterrent to recovery by casual attackers. Depending on departmental TRAs, encryption may obviate the need for destruction prior to disposal of media containing data that is Protected B or less. For higher sensitivities, encryption should not be deemed sufficient for disposal but may be combined with more destructive techniques – e.g., shred encrypted TopSecret media as though it were Secret.

3.6 Destruction Standards - Optical Media

Applies to:

- CD
- DVD

	Encryption Declassification Standards	Encryption Products
Unclas, PA, PB	Disk or file encryption.	CSE IPPL
PC, C, S	Disk/file encryption PLUS shredding/disintegration or grinding as for PA/PB.	CSE-approved Type I encryption.
TS	Disk/file encryption PLUS shredding/disintegration or grinding as for Secret.	CSE-approved Type I encryption.
	Shredding, Disintegration and Grinding Destruction Standards	**Destruction Products**
Unclas, PA, PB	CDs only: grind the disk surface to remove the coloured data layer; or CDs or DVDS: shred into small pieces < 160mm^2 in area (e.g., 1/2x1/2").	RCMP Security Equipment Guide (SEG).
PC, C, S	CDs only: grind the disk surface to remove the coloured data layer; or CDs or DVDS: shred into small pieces < 36mm^2 in area (e.g., 1/4x1/4").	
TS	CDs only: grind the disk surface to remove the coloured data layer; or CDs or DVDS: shred into small pieces <10mm^2 in area (e.g., 1/8x1/8").	
	Incineration	**Approved Incinerators**
All Levels	Total destruction.	Facilities approved by Environment Canada for the incineration of mixed plastics, etc.
	Emergency Destruction	**Physical Deformation Tools**
All Levels	Refer to the Annex on Emergency Destruction.	Focused high-impact tool, vise, sledgehammer, etc.

3.6.1 Exceptions

Overwriting:

- at the present time, overwriting is not approved for declassification and disposal of optical media containing sensitive information.

Degaussing:

- degaussing has no effect on optical storage disks and therefore is not approved for them.

Knurling:

- at the present time, knurling is not approved for declassification and disposal of optical media containing sensitive information.

Surface Grinding:

- removes the coloured layer of CDs where the data resides; however, this method does not work for DVDs where the information bearing layers are sandwiched in the centre.

3.7 Destruction Standards - Miniature Electronic Storage Devices & PDAs

Applies to: USB tokens and portable devices containing semi-conductor storage chips (including EEPROM "Flash" storage used in BlackBerrys and other PDAs), and Miniature glass-disk drives.

Level	Data Encryption Declassification Standards	Encryption Products
Unclas, PA, PB	Device or file encryption.	CSE IPPL
PC, C, S	Device or file encryption PLUS shredding/disintegration or grinding as for PA/PB.	CSE-approved Type I encryption.
TS	Device or file encryption PLUS shredding/disintegration or grinding as for Secret.	CSE-approved Type I encryption.

	Data Overwrite Declassification Standards	Overwrite Products
Unclas, PA, PB	Flash EEPROM storage devices: • overwrite all storage locations with a known pattern, then read back the expected pattern at random locations to verify. If the device is equipped with an erase function, then execute the erase function as a final step.	RCMP Security Equipment Guide (SEG). *Note: If a malfunction prevents overwriting, then destroy the device by other approved method.* *In the case of a non-approved erase function, the verification stage is essential – i.e., if the success of the overwrite cannot be verified, then destroy the device by other approved method.*
PC, C, S, TS	Flash EEPROM storage devices that have a CSE-approved erase function: • execute & verify the overwrite & erase functions in accordance with CSE guidance for the specific storage device product. Flash EEPROM storage devices without an approved erase function: • overwrite all storage locations 10 times with a known pattern and its binary complement, then verify by reading random locations. Execute the erase function (if so equipped) as a last step.	
	Shredding, Disintegration and Grinding Destruction Standards	**Destruction Products**
Unclas, PA, PB	Miniature drives or Flash/EEPROM devices: • reduce the device to pieces, each with maximum area < 160mm^2 in area (e.g., 1/2x1/2”).	RCMP Security Equipment Guide (SEG).
PC, C, S, TS	Miniature drives or Flash/EEPROM devices: • grind or pulverize the storage chip or the entire storage device into small pieces < 2mm in size, using a 3/32-inch screen.	
	Incineration	**Incinerator Facilities**
All Levels	Total destruction.	Environment Canada approved for plastics, etc.
	Emergency Destruction	**Deformation Tools**
All Levels	Refer to the Annex on Emergency Destruction.	Focused high-impact tool, vise, sledgehammer, etc.

Exceptions:

Degaussing: Degaussing is ineffective against miniature electronic storage devices and other devices that use Flash (EEPROM) semi-conductor storage chips and, therefore, is not approved for them.

Volatile Memory (RAM, DRAM, SRAM): Volatile memory loses its data when electrical power is removed but traces may linger for a short time due to cold temperature or electrical capacitance (especially for SRAM devices). Volatile memory should not be considered erased until 24 hours without power has passed.

"Clear" Command: PDAs use non-volatile memory (Flash EEPROM) to retain data when power is removed. Some PDA models provide a "Clear Command" to overwrite and/or erase this memory, but in most cases the process has not been independently verified and therefore is not approved for declassification and disposal of PDAs that contain extremely sensitive information. Exceptions may be made ONLY on products for which the CSE has specifically approved a built-in or add-on erasure process.

Annex A: ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
ATA	Advanced Technology Architecture or AT Attached
BIOS	Basic Input/Output System
CD	Compact Disk
CD-R	Compact Disk Recordable
CD-RW	Compact Disk Rewritable
CF	Compact Flash (card)
CFU	Considerations-for-use
CHKDSK	Check Disk (a DOS command)
CMRR	Center for Magnetic Recording Research (see UCSD)
CMRR	Code Mode Rejection Ratio
CRC	Cyclic Redundancy Check
CSE	Communications Security Establishment
DOS	Disk Operating System
DVD	Digital Video Disk
DVD+R	Digital Video Disk Recordable (from the DVD+R Alliance)
DVD+RW	Digital Video Disk Rewritable (from the DVD+R Alliance)
DVD-R	Digital Video Disk Recordable (from the DVD-R Alliance)
DVD-RW	Digital Video Disk Recordable (from the DVD-R Alliance)
EDSD	Electronic Data Storage Device
FAT	File Allocation Table
FAT16	16 bit version of FAT
FAT32	32 bit version of FAT
FDISK	Format Disk (a DOS command)
GB	Gigabyte
GoC	Government of Canada
GSP	Government of Canada Security Policy

HDD	Hard Disk Drive
IDE	Integrated Drive Electronics
IPPL	ITS Prequalified Products List (a CSE Industry Program for product evaluations)
ITS	Information Technology Security
MMC	Multi-Media Card
NSA	National Security Agency (U.S. government)
NTFS	New Technology (NT) File System
PC	Personal Computer
PC Card	Replacement name for PCMCIA
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
r/w or R/W	Read/Write
RAM	Random Access Memory
RAID	Redundant Array of Independent Disks
RIM	Research In Motion Corporation (manufacturer of the BlackBerry PDA)
RS-MMC	Reduced Size MMC
SATA	Serial Advanced Technology Architecture
SCSI	Small Computer System Interface
SD	Secure Digital (card)
TBS	Treasury Board Secretariat of Canada
TRA	Threat and Risk Assessment
UCSD	University of California San Diego (see CMRR)
USB	Universal Serial Bus
USO	Universal Secure Overwrite (UCSD CMRR “Secure Erase”)

Annex B: DESTRUCTION PROCEDURES

This annex provides a detailed discussion of the various clearing, sanitization, and destruction techniques available for the various types of electronic data storage devices.

The annex is divided into the following sections:

B.1 – Clearing

B.2 – Sanitizing

B.3 – Encryption

B.4 – Overwriting

B.5 – Degaussing

B.6 – Emergency Destruction via Physical Deformation

B.7 - Shredding and Disintegration

B.8 – Grinding and Hammer-milling

B.9 – Materiel Molecular Separation

B.10 – Surface Grinding for Optical Disks

B.11 – Knurling

B.12 – Incineration

B.1 Clearing

Reusable media, such as magnetic disks, re-writable optical disks, and memory-based devices may be cleared for re-use in the same (or equivalent or higher) security environment by overwriting all accessible locations with a single pass of 1s and/or 0s, and then verifying that the process was successful.

Software overwrite utilities that function at the application level will not overwrite data that may be contained in bad sectors or hidden partitions. Furthermore, successfully overwritten data may still be recoverable in a laboratory setting. Therefore, magnetic disks that have been cleared by overwriting must be retained within a departmental security environment appropriate for the level of information previously stored on the disk.

Clear core memory units and magnetic bubble memory of all levels of sensitivity by overwriting all locations with two pseudo-random patterns and a third known pattern followed by verification. Core memory units can be degaussed with an approved degausser.

Some USB thumb-drives and Flash cards, etc, may contain inaccessible non-volatile memory that cannot be cleared. This may require a more drastic destruction technique (see below).

B.2 Sanitizing

The sanitizing process is appropriate for erasable or reusable media such as magnetic disks, tapes, USB thumb-drives, flashcards, CD-RWs, etc. Prior to declassification and/or release outside the control of the department these reusable devices must be adequately sanitized and their data destroyed.

Remove all markings or other external indications of the sensitivity of data formerly stored on the EDSD, and destroy it (or the data within it) in accordance with the instructions below.

Note that most adversaries lack the means to do sophisticated laboratory analyses of incompletely destroyed magnetic disks. However, some adversaries may have that capability, and may make the attempt if they acquire magnetic disks or fragments from a known source of sufficient interest to them to justify the time and cost of laboratory analysis.

Non-erasable or reusable media, such as CD-ROMS and DVDs, must be disposed of according to the instructions below.

Core memory units and magnetic bubble memory of all levels of sensitivity can usually be sanitized by one of the following methods (*and* removing all markings or other external indicators of sensitivity):

- Overwriting all core or bubble memory locations two times with a pseudo-random pattern followed by a known pattern, and then doing spot-verifications to confirm that only the known pattern can be read.
- Degaussing core or bubble memory devices with an approved degausser. In the case of bubble memory, all shielding materiel must be removed from the device before degaussing.
- Pulverizing, smelting or disintegrating core memory.
- Collapsing bubble memory by raising bias voltages on bubble memory devices that are equipped with bias controls (consult manufacturer for technical guidance).

B.3 Encryption

Applicability: Magnetic Media (Hard Disk, Floppy, Tape, Magnetic Stripe Card), Optical Media (CD/DVD), and Semi-Conductor storage devices (USB Flash drive, etc).

Approved Technologies

- *Protected C or Classified.* For encryption of extremely sensitive media, only CSE-approved solutions may be used. Contact the CSE for more information about Type I encryption products.

- *Protected B and below*. For encryption of particularly sensitive media and below, the CSE recommends that Departments use GoC-approved algorithms and certified products listed under the IT Security Products Prequalification Program (IPPP) at the CSE website www.cse-cst.gc.ca

Description

Encryption is recommended for portable EDSDs that may be exposed to non-secure environments, casual loss, or targeted theft. The risk of compromise of sensitive information is greatly reduced if the device is properly encrypted. Encryption by itself does not replace other destruction techniques prior to authorized disposal, but it may reduce the amount of destruction that is required if the following conditions are met:

- the encryption has been applied to the media and/or data for all of its life cycle;
- the encryption product has been approved by CSE for the particular application and for the highest classification of information being processed; and
- users have applied strong access control passwords in accordance with departmental cryptographic key management policies.

Procedures

PROTECTED A/B: For portable EDSDs that contain Protected A or B information, encryption is a recommended security practice. On laptop computers, full-disk encryption (as opposed to file or folder encryption) ensures that protection is applied to all potentially sensitive information, including data stored randomly in temp files and operating system "swap" files. The procedure to declassify an encrypted laptop includes applying a one-pass overwrite to the encrypted hard disk (to conceal the fact of the encryption as well as to discourage any effort to recover the decryption key) and removing any external indications that the machine may contain Protected B data.

PROTECTED C / SECRET: Portable media that contain Protected C or Classified information should be encrypted as a matter of departmental policy to guard against compromise whenever the device may be subject to casual loss or targeted theft. Information at this extreme level of sensitivity must be protected with products that are specifically approved by the CSE for that level. Nevertheless, even when so encrypted, the device is not recommended for disposal without the application of a triple overwrite procedure or a more destructive method such as hard-disk degaussing or disintegration. In addition to the triple overwrite or disintegration process, the procedure to declassify the device includes the removal of any external indications that the device may contain sensitive information. If such indications cannot be removed (e.g., TEMPEST laptop or permanent markings), then the internal storage media should be removed for separate disposal.

TOP SECRET: Portable EDSDs containing Top Secret information should be encrypted with an encryption method approved by CSE for Top Secret, to guard against compromise whenever the device may be subject to casual loss or targeted theft. Nevertheless, even when so encrypted, the device is not recommended for disposal without an additional destructive process being carried out on them. In the case of a laptop, the hard drive should be removed for separate destruction in all cases.

B.4 Overwriting

See Annex C for known security issues concerning overwriting of various types of media.

Applicability: Magnetic Media (Hard Disk, Floppy Disk, and Tape), Solid-State Media (Personal Data Assistants, Portable Memory Devices), and Optical Disks (CD/DVD

Approved Technologies: Overwrite utilities for hard disks must meet RCMP criteria for functionality and reporting features to enable the human operator to determine if the entire disk is overwritten, and should be evaluated by recognized independent agencies such as a Common Criteria laboratory. Overwrite utilities for solid-state media are emerging as a feature on some vendor products but in general are unproven. An overwrite process for optical media is being developed at the University of Arizona but is not ready for general use.

Description
See Annex B for detailed guidance on overwrite procedures for magnetic media. To "clear" magnetic and solid-state media for re-use within an equivalent or higher security environment, perform a single-pass overwrite of the entire storage area. To "sanitize" the media, it is necessary to perform multiple overwrites and employ additional destructive methods (depending on the type of media and the level of sensitivity of stored information). Following the overwrite process, remove all external indicators that denote the sensitive nature of the contents of the disk, including markings, labels, and removable HDD slide mechanisms.

Procedures
PROTECTED A/B AND CONFIDENTIAL: Overwriting is an effective form of protection against the level of effort that an attacker might reasonably apply against magnetic or solid-state media containing "particularly sensitive" information. For this level of sensitivity, overwriting is highly recommended because it leaves the media in a re-usable condition for the purpose of recycling or for donation to the Computers for Schools program.

PROTECTED C AND SECRET: Overwriting is not permitted for sanitization of magnetic media containing Protected C or Secret information because it does not completely obliterate magnetic data traces against laboratory attack. However, overwriting may be considered in conjunction with other destructive methods such as disk deformation or disintegration into small fragments because that will add greatly to the complexity and difficulty of any laboratory analysis of captured storage materiel. Personal data assistants and portable memory cards contain non-volatile memory in solid-state chips or (in some cases) miniature glass disks. The risk is HIGH that any built-in erasure processes that may exist on these devices might not overwrite all data storage locations, and there is also some risk that even the areas that are overwritten may retain traces of the former data. Therefore it is essential that the human operator be able to verify the effectiveness of the overwrite process over all storage locations, and to perform multiple overwrites in the absence of a proven erasure method.

TOP SECRET: For Top Secret information contained on magnetic disks, a combination of overwriting and other destructive process will make analysis very difficult. For hard disks, there is a

theoretical possibility of recovery of data from overwritten sectors, and an ever-present risk that some sectors might not be overwritten in the first place due to human error and/or hidden sectors); therefore, a more destructive method must be selected to supplement the overwriting process. For PDAs and portable memory cards, there is a HIGH risk that portions of the non-volatile memory may be unaffected by unproven erasure processes; in addition, recoverable signal traces may remain in areas that are erased. Therefore a more destructive process is required if the device has been exposed to Top Secret information.

B.5 Degaussing

Applicability: Magnetic Tape, Hard Disk and Floppy Disk

Approved Technologies: See Annex D, "Degausser Products".

Description

Degaussing is useful in erasing magnetic tapes, floppy and hard disks, and certain other magnetic media. However, degaussing cannot erase data on semi-conductor data storage and memory devices or PDAs.

If properly used and maintained, approved degaussers will destroy all data on any magnetic media for which they are rated. As a side effect, they also damage internal hard-disk mechanisms beyond repair.

The degausser product must be CSE-approved for the coercivity of the magnetic media to be sanitized (see Annex D).

Protected C, Confidential, Secret, & Top Secret Information
When relying on Degaussing to sanitize magnetic disks containing extremely sensitive information, departments need to have adequate operating and maintenance procedures to ensure that the product is effective throughout its life cycle (see Annex D).

B.6 Emergency Destruction via Physical Deformation

Applicability: Magnetic Hard Disk, Floppy Disk, Tape, Magnetic Stripe, Optical Disk, Solid-State Media, Portable Memory Devices, PDAs

Recommended Technologies: The following are recommended technologies for the emergency destruction of media or devices that contain sensitive information at any level: Nail Gun (with the charges but without the nails); Electric Drill; Other focused high-impact device (e.g., firearm); Vise; Sledge hammer.

Description
Heavily damaged hard disks with deformed disk surfaces are beyond any reasonable hope of recovery for most adversaries, and adversaries with access to sophisticated laboratory analysis facilities are constrained by opportunity, motivation, time and cost. Physical deformation alone might not deter a capable adversary if there is reason to believe that the information on the damaged disk is worth the

time and effort of analysis. *Therefore physical deformation is recommended only as an emergency destruction measure to protect materiel in imminent danger of capture by hostile forces.*

In the case of hard disks, the selected method should provide readily recognizable damage to the drive casing, to discourage the attacker from considering any attempt to analyze the contents. In addition to damaging the delicate head positioning mechanisms, the selected method ***must*** deform the surface of each disk within the HDD or disk pack.

Perform similar damage to all HDDs regardless of sensitivity, and remove all external markings, labels, and removable HDD slide mechanisms in order to make highly sensitive HDDs indistinguishable from less sensitive HDDs.

Laptop Computers: pre-marking for emergency destruction

Laptop computers deployed to sensitive operations areas should be pre-marked on the underside of the case to indicate the location of sensitive components. These marks should guide field agents where to apply the emergency destruction tool to damage the hard drive, optical disk, and/or floppy disk - as well as where not to apply the tool (i.e., for personal safety, avoid damaging the battery compartment).

Top Secret

- Heavily damaged magnetic disks with deformed disk surfaces might not deter a highly capable adversary if there is reason to believe that Top Secret data may be recovered. However, deformation may be suitable in emergency situations to protect materiel in imminent danger of capture by hostile forces – especially when the Top Secret disks are mixed indistinguishably with others.
- Deformation, when preceded by overwriting or encryption, may also be suitable for protection of media that is in storage or in transit. To discourage would-be attackers, the selected deformation method should cause obvious damage to head positioning mechanisms and disk surfaces.
- Prior to deformation, remove external sensitivity indicators and mix with less sensitive media similarly deformed, in order to increase the effort required for an adversary to find valuable data.

Additional Information:

Consult the CSE for additional documentation on emergency destruction.

B.7 Shredding and Disintegration

Applicability: Magnetic Hard Disk, Floppy Disk, Tape, Magnetic Stripe Card, Optical Disk, Portable Memory Devices, Portable Information Processing Devices, Solid State Media

Approved Technologies: Refer to the RCMP Security Equipment Guide (SEG), G1-001 and G1-002.

Description: Commercial disintegrators, shredders, grinders and hammer-mills may provide cost-effective destruction of hard drives. These methods also can be used on miniature and portable media.

Procedures:

Prior to destruction, all disks must be stripped of external indicators of their former sensitivity levels - including markings, labels, and removable HDD slide mechanisms.

Departmental security staff must closely observe every facet of the destruction process, and ensure that no remnants are excessively large and that all remnants are mixed indistinguishably with other less sensitive disk and HDD fragments.

To deter subsequent analysis by unauthorized parties, the destruction process must reduce the media to small pieces of a size not to exceed the values provided in the Destruction Standards charts (section 3 of this guideline).

- Coarse Pieces. Coarse shredding preceded by overwriting or by encryption is an effective protection measure for media in storage or transit or for emergency destruction because it reduces a capable adversary's chance of success in recovering usable information – particularly when fragments containing highly attractive information are mixed indistinguishably with less-sensitive fragments of other disks. Nevertheless, sizeable remnants of recognizable disk surfaces are theoretically vulnerable to laboratory analysis. Departmental TRAs should take this into account if there is any possibility for an adversary to determine that a particular fragment comes from an extremely sensitive information environment.
- Fine Particles. Reduction of media to smaller particle sizes will deter attempts to recover data by microscopy. Although several factors make it extremely difficult to reconstitute useful data from the remnants of a destroyed hard drive, nevertheless magnetic disks provide potentially high data densities on each remnant particle. In the case of optical disks, recovery of data files from disk pieces is a slow and resource intensive process – but advanced recovery techniques do exist and continue to be developed to improve success rates and speed.

B.8 Grinding, Hammer-milling, and Pulverization

Applicability: Magnetic Media (Hard Disk, Tape, Floppy, Magnetic Stripe), Re-writeable Optical Media, Portable Memory Devices, Portable Information Processing Devices, Solid State Media

Approved Technologies: Refer to the RCMP Security Equipment Guide (SEG), G1-001 and G1-002.

Description
Grinding and hammer-milling are processes that reduce solid materiel to tiny fragments. Commercial grinders may provide quick and cost-effective destruction of entire hard drives. This same technique can be used on portable media although more economical means may be more practical.

Pulverization is a process of smashing or crushing materiel. This may be effective for destruction of hard drives, provided that the pulverization is done to such an extent that the disk surfaces cannot subsequently be separated from the rest of the destroyed materiel for laboratory analysis.

Prior to destruction, remove all exterior markings that indicate the media sensitivity of the media, including markings, labels and HDD slide mechanisms, and deeply score the surface of the disk in several places on both sides of the disk (modern CDs and DVDs may contain data-bearing layers on both sides).

Departmental security staff must witness the destruction process.

Unclassified and Protected A & B Information.
Grind or hammer-mill into at least three pieces of a size that meets destruction standards at Section 3 of this guideline.

Confidential, Protected C, Secret, and Top Secret Information.

- The process must reduce all individual disk surfaces to at least three pieces of a size that meets the applicable destruction standards at Section 3 of this guideline. The facility must be RCMP-approved. Departmental security staff must closely observe every facet of the process, as well as ensure that no remnants are excessively large and that all remnants are mixed indistinguishably with other less sensitive disk and HDD that were hammer milled.
- Prior to delivery to the hammer-milling facility, all disks must be stripped of sensitivity indicators, including markings, labels, and removable HDD slide mechanisms.
- Note: When preceded by overwriting or encryption, the grinding or hammer-milling process is highly effective at reducing even the most capable adversary's chances of success in recovering usable information – particularly when the fragments containing highly attractive information are mixed indistinguishably from other fragments of less sensitive shredded disks. Nevertheless, the process may leave sizeable remnants of recognizable disk surfaces that are theoretically vulnerable to laboratory analysis, and departmental TRAs should take this into account if there is any possibility for an adversary to determine that a particular fragment comes from a Top Secret environment. Otherwise, grinding or hammer-milling (preceded by degaussing, overwriting, or encryption) is an effective protective measure for storage, transit, or emergency destruction.

B.9 Materiel Molecular Separation

A promising new environmental recycling technology not approved for EDSD sanitization at this time.

B.10 Surface Grinding for Optical Disks

Applicability: Optical Media (all types)

Approved Technologies: Refer to the RCMP Security Equipment Guide (SEG), G1-001 and G1-002.

Description
The grinding process reduces the coloured surface area (the information-bearing layer) to a fine powder, leaving behind a transparent plastic disk suitable for recycling or disposal.

Prior to surface grinding, remove all exterior markings that indicate the sensitivity of the media, and deeply score the surface of the disk in several places on both sides of the disk (modern CDs and DVDs may contain data-bearing layers on both sides).

Unclassified, Protected A-B-C, and Confidential, Secret, or TopSecret Information: Surface grinding is approved for all types of optical media including read-only, recordable and re-writeable DC/DVD. Commercial grinding products chosen for this purpose must completely remove the entire information-bearing layer of the disk.

B.11 Knurling

Applicability: Optical Media (all types)

Approved Technologies: None to date.

Description
Commercial knurling products reduce optical disks to an elongated and slightly curled shape, which destroys the data "pits" and "lands" over the entire disk. Prior to destruction, remove all exterior markings that indicate the sensitivity of the media, and deeply score the surface of the disk in several places on both sides of the disk (modern CD/DVDs may contain data-bearing layers on both sides).

Protected A/B/C and Confidential/Secret/TopSecret Information: Knurling is under consideration for approval for destruction of all types of optical media including read-only, recordable and re-writeable CD/DVD. Contact the CSE for updated information.

B.12 Incineration and Melting

Applicability: Magnetic Hard Disk, Floppy Disk, Tape, and Magnetic Stripe Card, Optical Disk, Solid-State Media, Portable Memory Devices, and PDAs

Approved Technologies: The incinerator must be approved by Environment Canada for the plastics and other materiel involved.

Description
Incineration can completely destroy all media devices, at all levels of sensitivity.

Melting is a different process whereby materiel is heated to a temperature that is less than its flash point but high enough to melt it, which can make it an effective destruction process for hard drives.

If using commercial facilities, departmental security staff must witness the destruction process.

This page intentionally left blank.

Annex C. OVERWRITE UTILITIES FOR HARD DRIVES

It is often desirable to erase sensitive data from hard disks with the intent of downgrading them to Unclassified and releasing them outside the controlled environment – e.g., for recycling to the Computers for Schools program. In this case, the only solution is to utilize overwrite techniques to erase sensitive data from the storage media. However, there are security risks when using an overwriting process to erase sensitive information from hard disks.

This annex addresses security concerns with overwrite processes for hard-disk drives, and provides guidance on solutions to mitigate these concerns.

C.1 Security Concerns with Overwrite

Technical expertise is required to overwrite hard drives reliably. It is not a straight-forward process. There are several areas of concern with overwrite as a method of erasure:

- Human errors in handling the overwrite software;
- Software inability to overwrite all disk space;
- Lack of tools to verify either the disk capacity or the effectiveness of the overwrite;
- The track-edge phenomena.

Human Error

Human error can lead to the exposure of sensitive data through the release of a hard disk that was thought to be overwritten but in fact is only partially overwritten. Examples of this include being unsure of how to operate the overwrite software correctly; and not following all procedures carefully. In order to verify that the overwrite software is not missing any disk spaces, it is critical that the human operator correctly calculate the actual amount of space on each disk.6

Software Inability to Address All Disk Spaces

There is a large diversity in the manufacture of hard disk technology and the interfaces with various operating systems. A given software package may not work reliably on some platforms. Among the more common problems is the failure of the software to overwrite data in protected or bad sectors. Often, this data can be retrieved by other software that goes further down in the software control layers to get at disk geography, or by simple laboratory devices – e.g., a spin scan and recording head would be sufficient (microscopy would not be required). A common problem in DOS systems deals with how the software determines disk size. Sometimes the software will take the disk size from the Basic Input/Output System (BIOS), which can result in less than a full overwrite. If BIOS settings for disk size are changed, then previously written data may not be accessible to the overwrite program. The

6 See “How to Calculate Disk Capacity” at the end of this section.

result may be a miscalculation of the size of the disk during the overwrite sequence, which can result in sensitive data exposed to possible recovery.

The diversity and rapid evolution of disk technology makes the reliable evaluation of disk overwrite software very difficult. Nevertheless, if a department is to trust a given product, then independent laboratory evaluation is essential – e.g., under the Common Criteria. Note that a product can be tested and shown to work on a particular platform, but it is very hard to extrapolate that to other platforms or other versions of the operating system, etc. The RCMP Technical Security Branch provides one software program free to departments. One or two commercial products are known to meet RCMP requirements for independent laboratory evaluation and availability of reporting features to assist operator verification procedures. And the University of California San Diego (UCSD) Center for Magnetic Recording Research (CMRR) freely publishes a "Secure Delete" overwrite utility that is supported by most if not all IDE hard disks manufactured after 2001.

Track-Edge Phenomena

When writing to a disk, or when using overwrites to sanitize a disk, the disk read/write (r/w) heads do not pass concentrically over the exact centre of the data bit track. This is due mostly to mechanical and electrical variables and tolerances. To improve *read* reliability, the *r/w cycle* is designed to write *wide* and read *narrow*, however it still leaves partial bits on the track edges after multiple overwrites.

These residual "track-edges" of the original (partial) bit patterns are generally left on the disk platter even though the bulk of the track has been overwritten. Microscopy techniques can be used to image these edges. Depending on the number and the magnetic remanence quality of these edges, processing can be done on them to reconstruct the original (overwritten) bit patterns of information.

Performing overwrites with absolute assurance that track-edges have been fully overwritten requires a high degree of control of the write head, which is not available in standard common disk drives. To ensure that residual track-edge phenomena are not present on a disk (following overwrite), it would be necessary to perform deliberate +/- offset over-writing to extend beyond the original track-edges. Standard disk controller firmware does not provide this type of offset control, but ongoing research at the UCSDCMRR is aimed at achieving this capability.

Disk manufacturers have provided general support on their IDE product lines for the afore-mentioned UCSD CMRR Secure Delete standard. The CMRR continues to develop this standard with the objective of introducing controlled offsets that would enable the entire track to be overwritten during two passes of the software. The RCMP and the CSE will monitor this development work for possible future application in government departments.

Methods of Attacking an Overwritten Hard Disk

For the purposes of this guideline, risk can be characterized as the probability of a security incident happening and the impact that it will have if the incident does happen. The threat is an event or agent that causes an incident to happen. Vulnerabilities are characteristics or flaws in process or equipment that promote or allow threat events to occur. There are two main areas of concern with respect to the exposure of sensitive data on magnetic media that have been overwritten:

- A threat agent attempting a keyboard attack; or
- A threat agent attempting a laboratory attack.

A keyboard attack will be possible if there were errors in the overwrite procedure or if the software did not overwrite all of the data. A laboratory attack on track-edges is possible but it requires a very well equipped research laboratory with costly microscopy equipment and highly trained researchers with a great deal of time and patience. To justify this effort, an adversary would require high motivation plus an expectation of significant gain to justify this level of effort.

Independently evaluated overwrite software

Whenever possible, the use of independently evaluated overwrite products should be used.

Multiple Overwrite

Applicable standards call for multiple overwrites of disks. Research in the late 1990s did not support the notion that multiple overwrites would add much in terms of reliability or security (except perhaps for very early disk technology where r/w head "wobble" was a significant factor), but other research seemed to indicate that a one-pass overwrite is insufficient. Unclassified laboratory tests were reported to have shown that it is possible to filter some useful information out of one level of overwrite, but not after the addition of a second overwrite pass. Over-writing with contemporary products would not positively obliterate residual track-edges using off-track over-writes. Over-writing will make any data information recovery process very difficult, but not impossible.

- *Note: work is continuing at the UCSD CMRR on the concept of "off-set" overwriting. This involves the disk controller of the hard drive being erased, to assist the overwrite process by offsetting the first overwrite pass slightly to one side of the centre of the data track and then offsetting the second overwrite pass slightly to the other side. The combined effect would be to completely overwrite all parts of the data track, including the edges, in just two passes.*

C.2 Training

Minimum training in the proper application of these overwrite procedures should be provided by departments to the operators who manage the overwrite processes. The training should provide the necessary skill sets and motivate the operators to meet the exacting technical requirements of this important security task.

C.3 Overwrite Software Considerations for Use (CFU)

The following considerations for use (CFU) are offered as guidance for users when overwriting a hard disk drive. The CFUs generally apply to any disk overwrite activity.

The CFUs are based on the minimum functionality required of any disk overwrite utility or verification application, along with generic procedural requirements to provide assurance that the target disk has been adequately overwritten. They are derived from various standards to ensure adequate protection against data recovery from sanitized disks and from results of CSE testing conducted in 1999.

CFU #1 - Treat and control all overwrite and overwrite-verification utilities as sensitive configuration items.

- Overwrite applications are not classified but they should be treated as controlled items with high integrity and configuration management requirements. Procedures should be documented to ensure adequate controls are enforced to prevent unauthorized modification or subversion of the overwrite software.

CFU #2 – Overwrite verification should use a separate, validated application.

- An overwrite verification utility is used specifically to verify that all addressable locations of the hard drive have been overwritten with the prescribed pattern. In order to accomplish this function with trust, one must have an application that has been validated as capable of viewing the entire disk drive. Using a verification function that has been included as a separate procedure within the overwrite application is problematic. Any inherent shortcomings the overwrite function may possess will surely be included in the verification function.

CFU #3 - Prior to overwrite, calculate the REAL disk drive capacity.

- It is imperative that the total addressable capacity of the disk drive is determined prior to commencing the overwrite procedure. It is not adequate to assume the drive has the capacity as reported by the BIOS, FDISK, CHKDSK, or Windows, etc because there is no standard for how they report disk drive capacity. Frequently, drive capacity is reported using different units, i.e., binary or decimal byte equivalents. This can be confusing and, unless the actual capacity is known, the results of the overwrite process will be in doubt. The only reliable method of determining the addressable storage capacity of the disk is to calculate it (see below).

CFU #4 - Ensure that both the Overwrite and Verification Applications report the REAL disk capacity.

- A complete overwrite of all addressable areas of a disk drive is only possible if the overwrite application is 'aware' of the total capacity. Calculate and compare the real disk capacity with the capacity reported by the overwrite application. If the calculated capacity is greater than the reported capacity, then the disk drive will only be overwritten up to the reported limit, and will NOT be completely overwritten.
- It is equally important that the verification application be similarly capable of accessing the entire hard disk drive.

CFU #5 - Treat disk drives containing BAD sectors as not being overwritten, until verification proves otherwise.

- Occasionally a disk drive will undergo the overwrite procedure and subsequently report the presence of "bad" sectors. An essential performance requirement for verification applications is that they must be capable of imaging these reported bad sectors, to allow confirmation that they have been fully overwritten. Otherwise the bad sectors must be considered as containing residual data, in which case the disk drive has not been completely sanitized. Disk drives with unverified overwrites of bad sectors should not be released for re-use; instead, they should be separately destroyed. In certain cases, the disk controller may contain logic to automatically re-map around a bad track, causing no errors to be generated on overwriting. Normally this is documented in the equipment technical specifications.

CFU #6 – Require that Overwrite Applications be run from a bootable floppy disk.

- With the exception of the UCSD CMRR "Secure Overwrite" utility (which acts directly on the disk controller at a level that is below the operating system), most disk drive overwrite utilities act as applications that are designed and tested to run within a specific operating system. Due to the drive-capacity reporting anomalies reported in CFU #3, each of these utilities will calculate or determine capacity based on its own algorithms and using operating system-dependent functions. Overwrite utilities should never be run from within any version of any operating system unless specifically recommended by the developer and validated for that particular version of the operating system.

CFU #7 – Enforce the Use of Documented Procedures and/or Checklists when using overwrite applications for sensitive protected and/or classified situations.

- To ensure consistency and repeatability of results for use of overwrite products, and to aid in product-specific user training, the development and enforced use of documented, application-specific procedures are recommended. Since typical overwrite software products are highly user-configurable, and because the sequence of procedural steps used to overwrite and subsequently verify the correct overwriting of hard disks are critical, checklists are a useful means of guiding users through a validated and repeatable process. Ideally, these procedures and checklists should be specific to the product used for overwrite and should be developed and certified for official use by a competent authority. Any and all changes to these procedures and checklists should be subject to formal revalidation and certification for use.

C.4 How to Calculate Disk Drive Capacity

In order to verify that the overwrite software is able to erase all parts of the disk, the operator must
(i) correctly calculate the actual capacity of the disk, and
(ii) compare that value to the capacity that is reported by the overwrite software.

- Disk capacity measurements are subject to interpretation. It is a coincidence that every 10th power (exponent) of 2 is approximately equal to every 3rd power of 10. This has resulted in two different definitions of these numbering systems. Depending on the context, there are two different meanings of 'Kilobyte', 'Megabyte' and 'Gigabyte'. This situation can cause confusion, especially in respect to disk size capacity measurements, where both measurements are often used without being defined. The following Table is a comparison of these numbering systems.

Comparison of Numbering Systems

Name	Binary Value	Decimal Value
Kilobyte (KB)	2e10 = 1,024	10e3 = 1,000
Megabyte (MB)	2e20 = 1,048,576	10e6 = 1,000,000
Gigabyte (GB)	2e30 = 1,073,741,824	10e9 = 1,000,000,000

Formula to calculate the capacity of a disk drive

The following formula calculates a number representing the total number of bytes that can be stored on the hard drive:

*Cylinders * Heads * Sectors * 512 (bytes per sector)*

The result is a decimal number. To convert this number to the decimal equivalent of the binary value, divide it by the appropriate binary value. For example, for a disk that contains 6704 cylinders, 15 heads and 63 sectors:

6704 x 15 x 63 x 512 = **3,243,663,360 bytes,** or
3.24 GB using 10^9 or decimal values, or
3,243,663,360 / 1,073,741,824 = **3.02 GB** in binary Gigabytes, or
3,243,663,360 / 1,048,576 = **3,093 MB** in binary Megabytes.

Sector Header Information

When a disk is formatted, additional areas are created on the disk for the disk controller to use for sector numbering and for identifying the start and end of each sector. These areas precede and trail each sector's data area, which accounts for the difference between the formatted capacity and the unformatted capacity of a disk. This difference can sometimes be as much as 17%. All drives use some reserved space for managing the data that can be stored on the drive.

Normally a sector is defined as 512 bytes but technically this is not precise. Each sector on a disk typically occupies 571 bytes of the disk, of which only 512 bytes are usable for user data. The actual number of bytes required for the sector header and trailer can vary from drive to drive.

Each sector of a disk has a header that identifies the start of the sector and a sector number, as well as a trailer that contains a checksum (to help ensure the integrity of the data contents). Each sector also contains 512 bytes of data. The data bytes are typically set to some specific value, such a F6h (i.e., 1111 0110) when the disk is being manufactured or low level formatted. In addition to the gaps within the sectors, gaps exist between the sectors on each track and also between the tracks; none of these gaps can contain any user data. These gaps account for the difference between the formatted and unformatted capacity of a disk drive.

Within the sector prefix gap there is a data word - called *Sector ID* – which consists of the Cylinder, Head and Sector Number fields, as well as a CRC field to allow for verification of the ID data. Most controllers use bit 7 of the Head Number to mark if a sector is found *bad* during a low-level format or surface analysis. This system is not necessarily universal and some manufacturers may use other methods to mark a bad sector. Typically, one of these ID fields contains the bad sector marker.

To determine the capacity of a hard disk drive:

- Remove cover of PC and read the make and model number of the hard disk drive, and
- Refer to manufacturer literature or website for specific technical information on that model.

Disregard the MB or GB ratings, as it will not be clear whether these are computed in decimal or binary. Note the geometry specification in Cylinders, Heads (sides), Sectors per track, and sector size (usually 512 bytes).

This page intentionally left blank.

Annex D. DEGAUSSER PRODUCTS

Introduction

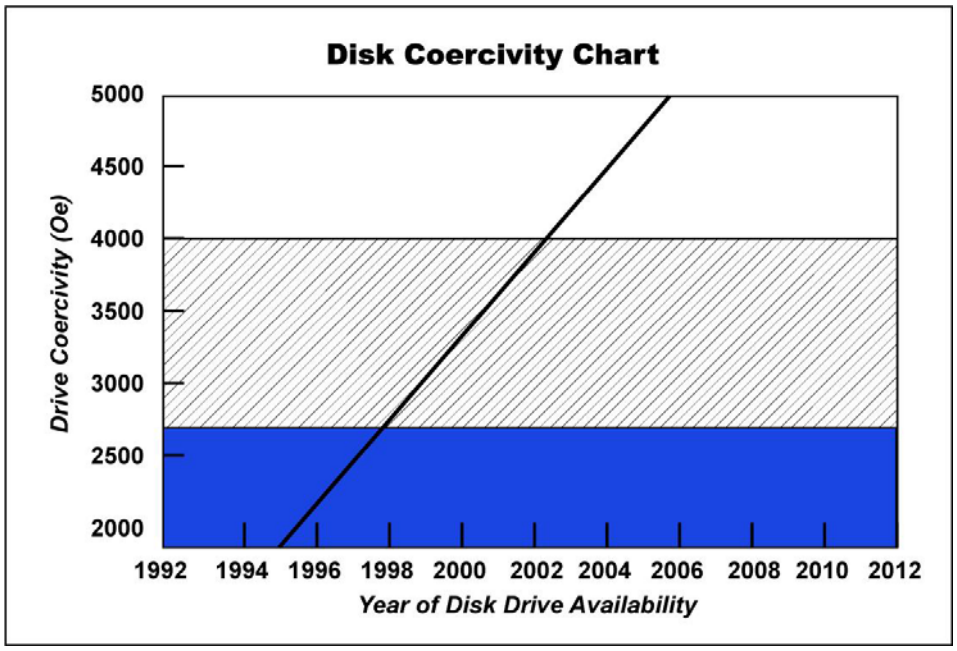
Degaussers apply an inverted magnetic field to disks or tape media to reduce information bits to zero. When this process is applied properly, all information on the media is made unrecoverable by any known technology. However, different types of magnetic tape and different models of hard drives have different susceptibilities to degaussers and their inverted flux fields.

Effective degaussing requires that the magnetic flux field that is applied by the given degausser product is sufficiently strong to completely destroy the magnetic data patterns of the particular media that is being erased.

Magnetic tape and older-generation hard disks can be erased by relatively low-power degaussers, whereas modern hard disks require extremely powerful degaussers. The reason is that modern hard disks are designed with special alloys that have very strong resistance to magnetic change, which enables manufacturers to decrease the size of magnetic regions on the disk to allow for higher data densities.

Resistance to magnetic change is referred to as *coercivity* and is measured in *Oersteds (Oe)*. In general, HDDs manufactured between 1999 and 2003 have coercivity up to 3,000 Oe, and a degausser must be approved for that level to ensure complete data erasure. HDDs manufactured in 2004-2005 have coercivity of 4,000 Oe and beyond, with the trend continuing to approximately 5,000 Oe in 2006.

The following Disk Coercivity Chart is provided courtesy of *Data Security Incorporated*, and is based on data from the testing programs of the Center for Magnetic Recording Research (CMRR) at the University of California San Diego (UCSD)…



Departments should contact the CSE to ensure that HDDs of any given year of manufacture can be reliably erased by the specific degausser being used.

Degaussing Standards & Procedures

- The CSE approves the use of specified products on the US government degausser products list, for the secure erasure of specified types of magnetic tape and/or hard-disk drives containing data at all levels of sensitivity.
- The degausser that is to be used must be approved for the type and version of media being erased. Specifically, the degausser must apply sufficient magnetic flux to overcome the media's actual resistance to magnetic change (referred to as *coercivity*, and measured in *Oersteds*), as determined by special laboratory testing.7

7 The University of California at San Diego (UCSD) Center for Magnetic Recording Research (CMRR) performs ongoing research to assess the field strengths of current degausser products and the required strengths to overcome the resistance to magnetic change on different types and generations of magnetic disk and tape media. Results of this testing are applied to the US NSA Degausser products list, which is recognized by the CSE for selection of degausser product models for specific types and versions of magnetic media.

- Human operators must be knowledgeable to use the degausser correctly for each different type of magnetic media that may be encountered; and
- Departments must adhere to the degausser manufacturer's usage, maintenance and upgrade instructions to ensure that the degausser continues to function correctly at is rated power output throughout its life cycle.

Degaussers for Hard Disks or Tapes

Commercial degausser products are added to the US evaluated products list following laboratory testing for degaussing effectiveness and long-term reliability. Many are approved for magnetic tapes, and several are approved for hard disks of older manufacture, but relatively few tested products are capable of generating the extremely powerful magnetic fields that are needed to erase modern hard disks.

Some degaussers have been tested and approved for both tapes and disks.

Degaussers for Tapes Only

Most magnetic tape can be erased by relatively low-power degaussers, but some types require stronger degaussing fields. For example, "3590"tape has a *coercivity* of about 1700 Oersteds, which means that it can be effectively erased by a degausser that has a *coercivity approval* that is equal to or greater than 1700 Oe, such as the *DSI Model Type III (943-0001)*, as well as the *DataTape Inc TD-1700* and the *Metrum DataTape TD-170* (however the latter two are no longer manufactured). Degausser products that are approved only for lower-coercivity tapes do not have enough power to erase higher-coercivity tapes.

Re-Use after Degaussing

TAPE… Many types of magnetic tape can be re-used after degaussing, but not all. For example, the *Magstar 3490 tape* product contains factory-recorded servo tracks that degaussing will destroy, thus rendering the tape unusable. Departments that wish to re-use tapes after degaussing should ask their tape manufacturers about re-use after degaussing, or contact their degausser manufacturer to ask if they know which brands of tape would be unusable after degaussing.

HARD DRIVES… Older low-coercivity hard drives may be re-usable after degaussing with low-power "wand" degaussers; however, modern hard drives cannot be re-used after degaussing because the degaussing fields to erase them need to be so strong that they also damage delicate drive components such as head positioning mechanisms. This damage may invalidate warranty coverage in the case of a failed hard drive that must be degaussed (for security reasons) prior to return to the vendor. In such a case, it may be possible to negotiate a change in the warranty terms so that the vendor will accept the return of a degaussed hard drive; otherwise, the department will have to bear the cost of replacement rather than return a failed non-degaussed hard drive containing sensitive information.

Coercivity of Various Magnetic Media

Current information regarding coercivity differences between different brands of magnetic tape is hard to find. *Fiji Corporation* published a fairly comprehensive list in a white paper in 2003, and in most cases it should be possible to obtain information directly from tape manufacturers. Hard-disk coercivity values are deemed to be sensitive proprietary information by vendors; however, it is known through testing that coercivity levels have been climbing sharply for successive generations of hard disks since 1999. In concert with this steep rise in hard-disk coercivity levels, a few security vendors have been developing degausser products with correspondingly greater degaussing power – and sufficient reserve power to enable them to remain effective for the near-and-medium term as hard-disk coercivities continue to climb.

Degausser Products List

To be approved by CSE, a degausser must have a coercivity approval that is equal to or greater than the coercivity of the type of media to be erased, as shown in the US NSA Degausser Evaluated Poducts List at http://www.nsa.gov/ia/ .

Annex E : PARTIAL DESTRUCTION – SECURITY ISSUES

This annex discusses the security risks of using Partial Destruction (as opposed to complete destruction) to sanitize electronic data storage devices containing sensitive information.

E.1 Risk Factors

Risk can be considered as the likelihood of the threat event occurring and the impact that it will have if it does occur. The likelihood of an exposure to a technically sophisticated attack will be governed by a variety of underlying factors such as:

- How knowledgeable are the people doing the destruction;
- How good are the procedures;
- How tightly controlled is the process; and
- How reliable is the chosen method for the particular devices to be destroyed.

Overwriting

A large diversity in hard disks being overwritten increases the likelihood that bad sectors will be overlooked or that miscalculation of disk size will occur. This increases the likelihood of a successful keyboard attack against the overwritten hard disk drive.

Measuring the Impact of Compromise

The classification and designation of information in accordance with the *Access to Information Act*, the *Privacy Act*, and the Government Security Policy *"Identification of Assets"* operational security standard provides a measure of *impact* if the information is compromised (e.g., unauthorized access to Secret information is deemed to have the potential to cause "serious injury" to the national interest). This measure can be further refined:

- *Type of Impact* – e.g., embarrassment, loss of confidence in government, financial losses or gains, loss of privacy, chance of litigation, etc;
- *Extent of Damage* – e.g., one branch of a department, the whole department, all of government, outside government, etc.
- *Effect of Time* – e.g., when does the information eventually become unclassified; and
- *Actual Sensitivity* – e.g., deciding if it was classified correctly to start with (and how certain you are of what is on the disk).

E.2 Threat Agents

The nature of the threat agent should be considered:

a) *Identification of likely threat agents* – e.g., foreign intelligence, organized crime, knowledgeable hacker, amateur hacker, casual thief, computer recycler, etc.

b) *Capability and resources of the threat agent* – e.g., can the attacker deploy sufficient resources to set up a microscopy lab and recruit and train experts to run it?

c) *Motivation and expected gain* – e.g., would the agent attempt a sophisticated laboratory attack (at great expense and time, without guarantee of success) without some prior knowledge that the EDSD actually contains worthwhile data?

d) *Opportunity* – how would the threat agent get into a position to receive the EDSD? Would this be the attacker's only way to get at this type of data – i.e., is there an alternative method of obtaining the information that is more reliable or efficient?

Annex F: TYPES OF STORAGE DEVICES

This annex lists the known types of EDSD covered by this guideline at time of publication.

F.1 Magnetic Tape

Magnetic tape comes in various formats, including:

- Reel (e.g., computer data tape),
- Cassette (e.g., audio tape), and
- other packaging such as VHS video.

For the purpose of sanitization by Degausser equipment, magnetic tape is categorized by its resistance to magnetic change - i.e., "Coercivity" as measured in Oersteds (Oe) – as follows:

- Type I tape is rated less than 350 Oe,
- Type II tape is rated between 350 and 750 Oe, and
- Type III "high energy" tape (4mm or 8mm) is rated between 750 and 1700 Oe.

F.2 Magnetic Disk

Floppy disk. This media type comprises the standard 3½", 5¼", and 8" size as well as others that utilize a flexible magnetic platter within an external enclosure.

Hard disk . Hard-disk drives are available in different interface types, including: ATA, Serial ATA (SATA), SCSI, Fibre Channel, etc. All are characterized by their extremely large storage capacity. Caution should be taken before relying on non-destructive erasure methods to sanitize hard disk media. Due to ever changing technology, various results will be obtained for different types or versions.

*Secure Erase*8. The Secure Erase protocol is supported on virtually all ATA and SATA drives with a capacity greater than 15-20GB (manufactured after about 2001). However, Fibre Channel and SCSI drives generally do not support Secure Erase (as of 2005).

Degaussing. The data density of hard-disk drives continues to increase as manufacturers develop new ways to concentrate more data into smaller areas. Hard-disk platter surfaces made of newer magnetic alloys cannot be erased by older degausser products. Contact the CSE to inquire about currently approved degaussers.

8 For more information about Secure Erase, visit the website of the University of California San Diego (UCSD) Center for Magnetic Recording Research (CMRR). http://cmrr.ucsd.edu/Hughes/subpgset.htm

F.3 Magnetic Stripe Card

Magnetic Stripe is a type of storage media that may be manufactured on the back of identification cards or access-control pass cards, etc. The magnetic stripe contains various forms of information that may be sensitive.

F.4 Optical Disk

This section includes CD-ROM, CD-R, CD-RW, DVD, DVD-R, DVD+R, DVD-RW, and DVD+RW disks. These disks come in a variety of sizes. All should be handled identically. New forms of DVD and video disks are being introduced to the marketplace. These may be viewed as higher-capacity versions of existing optical disk media, with similar security issues and methods of sanitization. However, their higher data densities require finer levels of data destruction – especially when used to store extremely sensitive information.

F.5 Electronic (Solid State) Storage Media

Solid-state storage for the purposes of this document refers to any technology that forms the basis of on-board storage memory, excluding optical and magnetic media devices. Solid-state media such as RAM, SRAM, DRAM, etc are typical within modern computer systems. Bubble memory and core memories may still be available on some older equipment.

F.6 Personal Data Assistant (PDA)

PDAs include BlackBerry, Palm, Pocket PC, and iPod devices.

The BlackBerry, which is widely used within Government of Canada, offers additional security features to meet government security requirements for sensitive but unclassified information.

Palm-based systems may offer digital connectivity for email and full wireless networking.

Apple Computer Inc and Motorola Inc are including iPod functionality within their wireless telephones. The iPods offer full system functionality and large storage capacity. As these newer devices become available, security staff need to recognize the amount of data that they can transport. Their outward appearance is that of a standard cellphone, but internally they may be multi-Gigabyte storage devices.

F.7 USB and FireWire Interfaces

FireWire (IEEE-1394) and USB interfaces on computers and PDAs allow the connection of external storage devices such as USB hard drives or memory sticks (“thumb-drives). Memory stick devices are constantly increasing in capacity after eclipsing the 2GB mark in the early-to-mid 2000s, and on some systems they could replace the internal hard drive as the primary disk media. Many modern computers

allow for boot-up from a USB or FireWire device. As this becomes more prevalent within Government of Canada, the resulting security concerns and issues will need to be addressed.

F.8 Portable Memory Devices

Portable memory devices (or drives) come in a variety of shapes and forms (see below). Some are solid-state devices, while others are miniature one-inch hard drives with one or two wafer-thin platters.

It is difficult for the casual user to discern which type of media device is being utilized within a given device. For example, there are several versions of the Apple iPod music player/datastore devices: the iPod Shuffle uses a solid-state flash card (512MB or 1GB); the iPod Mini uses a mini hard disk (4 or 6GB); and the iPod and iPod Photo use a multi-platter mini hard disk drive (30 or 60GB). The iPod Photo can store and display photographs.

Many portable memory devices can interface with a PDA such as a Palm or BlackBerry. Some can fit snugly within the devices but others would protrude from the case of the device. Many have BlueTooth interfaces for wireless connection to other devices, headsets, etc.

Portable memory is an area of rapid technological development. The following table is an overview of portable memory devices available in 2005.

Table 2. Portable Memory Devices (c.2005)

Type	Description	Size	Interface & Bus	Memory & Power
Compact Flash Card (CF)	A solid-state flash memory disk card for PCMCIA-ATA. Used more as a hard drive than as RAM.	Matchbook size 36x 43: Type I = 3.3mm thick, Type II = 5 mm thick	50-pin connector (two rows of 25 pins on edge of card). 16-bit data bus	Flash memory is non-volatile, i.e., retains its information when power is removed from the card. Consumes minimal power.
MicroDrive *(4GB Hitachi digital media)*	A high-capacity rotating mass-storage device (a tiny glass disk). Function is similar to solid-state flash memory but is more fragile and requires energy to spin.	Conforms to a Compact Flash Type II package (36.4x42.8x5mm)	16-bit data bus	4GB capacity (uses FAT32 file system for storage over 2GB). Requires the device to support FAT32 (many digital cameras and most PDAs do).

Type	Description	Size	Interface & Bus	Memory & Power
Multi-Media Card (MMC)	Solid-state disk cards with no moving parts. Provides greater protection of data than conventional magnetic disk drives.	Postage-stamp size (32x24x1.4mm).	7-pin connector 1-bit data bus	As with CF cards, they are designed with non-volatile flash technology, which retains information once power is removed from the card.
Reduced-size Multi-Media (RS-MMC)	Designed for mobile phones.	Shorter length (18x24x1.4mm).	Potential to use with PDAs (using a mechanical adaptor to fit a full-size MMC slot).	The RS-MMC slot can accept a full-size MMC (part of it sticks out).
Secure Digital Card (SD)	Similar to MMC design, with addition of a locking switch to prevent accidental erasure of data, and security controls for Content Protection Rights Management.	Similar size to MMC (32x24x2.1mm)	9-pin connector 4-bit data bus for higher transfer rate	SD card slots often can accommodate MMC cards as well.
Mini-SD card	An electrically compatible extension of the SD card standard	More compact size (21.5x20x1.4mm)	Same hardware interface and bus as standard SD. Can use an adaptor to fit a standard SD card slot.	Smaller capacity than SD (due to size)
Memory Stick (Thumb-drive)	Built-in erasure prevention switch to protect contents. • There is a *standard* stick, plus two variants (the Memory Stick *Duo* card and the Memory Stick *Pro* card).	The size of a gum stick (50x21x3mm). • The *Duo* variant is smaller (uses an adaptor to fit a standard slot).	10-pin connector 1-bit data bus	Solid-state memory • The *Pro* variant has higher capacity and higher data transfer rate.

Type	Description	Size	Interface & Bus	Memory & Power
Extended Memory Card	May support extensions for additional functionality – e.g., a multimedia card with both smartcard and memory chip			

This page intentionally left blank.

Annex G: CSE AND RCMP CONTACT POINTS

(for Government of Canada departments and agencies)

CSE IT Security Branch – ITS Client Services <insert email address >

RCMP Technical Security Branch – ITS Client Services <insert email address >

This page intentionally left blank.

Annex H: REFERENCES

1. Government of Canada Security Policy (GSP) February 2002, and the GSP Operational Standards 2005
2. IT Security Bulletin B2-001 “Hard Drive Declassification” (RCMP TSB) draft October 2004
3. Magnetic Disk Media Overwrite and Inspection Utilities (CSE CIPR-15) March 1997
4. National Defence Security Instructions (NDSI) Chapter 72: Magnetic Storage Media Secure Handling Instructions (DND A-SJ-100-001/AS-000) October 1999.
5. Degausser Evaluated Products List (US NSA annex to NSA/CSS Policy Manual 9-12), March 2006
6. US Information Assurance Advisory IAA-006-2004 (overwriting and downgrading), (U/FOUO), (US NSA/IAD) 18 October 2004
7. US Guidelines on PDA Forensics (US NIST SP800-72), draft August 2004
8. US Automated Information System Security (US DoD 5220.22-M chapter 8) http://www.dss.mil/isec/nispom_0195.htm
9. UK CESG clearing and declassification standard (replaces Memo7) 2005
10. Secure Deletion of Data from Magnetic and Solid-State Memory, by Peter Gutmann (University of Auckland) July 1996
11. Data Remanence in Semiconductor Devices, by Peter Gutmann (IBM T.J. Watson Research Center), 2001
12. Can Intelligence Agencies Read Overwritten Data: a Response to Gutmann http://www.nber.org/sys-admin/overwritten-data-guttman.html
13. Recovering Unrecoverable Data: a Channel Science White Paper Commissioned by Data Recovery Labs Inc, written by Charles H Sobey 14 April 2004 http://www.actionfront.com/ts_whitepaper.asp
14. Reliability and Security of RAID Storage Systems and D2D Archives Using SATA Disk Drives - ACM Transactions on Storage Vol.1 No.1 pages 95-107, by G.F.Hughes & J.F.Murray, December 2004 http://dsp.ucsd.edu/~jfmurray/publications/Hughes2004.pdf
15. Disk Drive Secure Erase: CMRR Secure Erase Protocols (University of California San Diego) October 2004 http://cmrr.ucsd.edu/Hughes/subpgset.htm
16. Technical Report #630, “Semi-invasive attacks – a new approach to hardware security analysis”, by Sergei Skorobogatov (University of Cambridge – Computer Laboratory), April 2005 http://www.cl.cam.ac.uk/TechReports/
17. Media Destruction guidance and products (US NSA)2006 http://www.nsa.gov/ia/government/gover00001.cfm