Information Technology Security Guide
Lead Agency Publication G2-003

Hard Drive Secure Information Removal and Destruction Guidelines

Technical Security Branch
Technical Operations
Royal Canadian Mounted Police
Issued: October 2003

Disclaimer of Responsibility

This publication was prepared by the RCMP for the use of the federal government. The publication is informal and limited in scope. It is not an assessment or evaluation, and does not represent an endorsement of the technology by the RCMP. The material in it reflects the RCMP's best judgement, in light of the information available to it at the time of preparation. Any use which a third party makes of this publication, or any reliance on or decisions made based on it, are the responsibility of such third parties. The RCMP accepts no responsibility for damages, if any, by any third party as a result of decisions or actions based on this publication.

©Copyright 2003 Government of Canada, Royal Canadian Mounted Police (RCMP)
1200 Vanier Parkway, Ottawa, Ontario, Canada, K1A 0R2

This publication may be reproduced verbatim, in its entirety, without charge, for educational and personal purposes only. However, written permission from the RCMP is required for use of the material in edited or excepted form, or for any commercial purpose

TABLE OF CONTENTS

1 Executive Summary

The following is a summary of the guidelines recommended by the RCMP as a result of the findings of this document:

1.1 For a hard drive containing the following security level of information:

- **Protected "A" (Protected) or**
- **Protected "B" (Protected) or**
- **Confidential (Classified)**

We recommend:
That the drives be "cleansed" by a **triple** overwrite of the RCMP DSX disk-overwrite software (or a third-party equivalent that meets RCMP overwrite guidelines). It is important that this process be done in accordance with the Conditions for Use shown at Appendix A. The drives may then be re-used within the department, or if no longer required they may be donated to Industry Canada's Computers for Schools (CFS) program as per Treasury Board policy. Following the triple overwrite, if it is not feasible to re-use the hard drives or to donate them to the CFS program, the drives may then be disposed of or the material recycled.

1.2 For a hard drive containing the following security level of information:

- **Protected "C" (Protected) or**
- **Secret (Protected) or**
- **Top Secret (Classified)**

or for a hard drive which is deemed to be non-functioning

We recommend:
That the drives be either:

a. passed through a commercial disintegrator having a ¼ inch residue screen (residue must be finer than ¼ inch to pass through the disintegrator debris screen),

OR

b. passed through a degausser strong enough to overcome the coercivity of the data contained on the drive. This degausser must be listed on the National Security Agency (U.S. Department of Defense) Degausser Products List found at **http://www.dss.mil/infoas/degausserlst.pdf** or else obtain an independent laboratory's confirmation of the maximum Oersteds that can be degaussed.

Under either procedure the drives are no longer functional at this point - all material may then be disposed of or recycled.

2 Introduction

2.1 General

The focus of this guide is to address the problems facing government departments regarding the issue of cleansing, disposal and destruction of computer hard drives which contain various levels of classified or protected information. Many departments have questioned, both internally and to the lead agencies, what can and should be done with disk drives from unserviceable or outdated computers. At first glance this would not seem to be a significant problem. Unfortunately the same problem that exists for the safe disposal of other media such as paper, diskettes or magnetic tapes is even more complicated for this media. It is still up to a department to determine the highest classification of data that should be allowed on a disk drive but when that drive has to be disposed of and it is determined that there is Protected "C" or Secret and above information contained, special precautions must be taken. In early 2002, the RCMP sent out a short questionnaire to all members of the ITSC (Information Technology Security Committee). The ITSC is composed of the senior IT security personnel of most government departments. The questionnaire asked five questions relating to hard disk drive disposal:

1) How are your hard drives with Protected "C" or Secret and above information currently being disposed of within your department?
2) Approximately how many hard drives with Protected "C" or Secret and above information are currently being stored within your department?
3) If a centralized destruction service was provided would your department use the services?
4) Would your department prefer to do its own destruction?
5) Would your department share in the costs of establishing a central destruction site?

The responses varied in how they dealt with the problem. Most do not deal with much high level information on hard drives or simply do not allow it on their drives. Some already have a disintegrator in place. Others use only the DSX disk overwrite software.

The majority were in favour of a centrally located destruction facility as long as a secure delivery service could be established. As well, most did not want to be responsible for the destruction of their own drives due to the cost and their limited resources. The sharing of costs was not considered appropriate since it should be centrally funded.

There is no up-to-date Government of Canada standard which addresses the problem of disk drive disposal. The Technical Security Standard for Information Technology (TSSIT) (August 1997, Royal Canadian Mounted Police) does refer to disposal in Section 4.6, and the Security Equipment Guide G1-001 (online on the RCMP GenNet Web site), provides some guidance. However, comments gleaned from the questionnaire show there is no continuity in the way drives are handled before disposal. One comment summarized the feeling of many of the respondents: "If we want a formal program that every one will adhere to it must be centralized, regulated within (government) security policy and centrally funded. Otherwise the destruction will not be done properly". Based on those comments, it would be safe to say that until the problem of hard drive disposal/destruction is addressed, the risk of secure information being accidentally released will continue to rise with time.

2.2 Scope

The purpose of this guide is to mainly address the issue of Protected "C" or Secret and above information contained on hard disk drives. However, the content applies equally to all information contained in IT media and could be used as a reference for the disposal of all data contained on computer hard disk drives.

The securing of information at lower levels of sensitivity will also be discussed and recommendations made for their handling as well. The issue of whether disk drives containing encrypted information should also be cleansed will not be addressed in this guide. Since encryption methods can vary and their effectiveness over time can diminish with increased technology improvements, for the purpose of this guide, drives that contain encrypted information should be dealt with in the same manner as those that are not encrypted. This guide deals with the hard drive information content disposal problem as it relates to the Federal Government of Canada and its Information Technology security requirements as dictated by the Government Security Policy.

2.3 Objective

The objective of this guide is to make recommendations for implementing a standardized process which will address the following issues:

(1) the requirement to update and expand the RCMP TSSIT standards for media sanitization, and
(2) the proposal for a centralized destruction facility and a centralized degaussing facility.

The disclosure of less sensitive than Top Secret and Protected "C" information could potentially cause moderate harm or embarrassment to the national interest of Canada or individuals. These standards will then provide government departments with a viable, safe and cost-effective solution for handling this media. This guide will also serve as a reference for hard drive functionality and the safe destruction of its contents. Hopefully it will heighten the awareness of the reader and bring a resolution to the ongoing problem of disk drive disposal/sanitization once and for all. The intention is for ITSC members to review the recommendations and if they are found to be satisfactory, the guide will be forwarded for approval by the IT Management Standards Committee established by Treasury Board and the recommendations implemented on a timely basis. The RCMP Technical Security Branch would be available to assist in an implementation plan to establish a working model.

3 Problem definition

3.1 History

The safe and proper disposal of media containing sensitive information is not a new problem. The issue now, however, is the changing of media type. Information once contained on paper, microfiche or magnetic tape is now stored on IT media such as diskettes, CD-ROMs, DVDs, flash memory, memory cards and hard-disk storage drives. IT media is being made from ever more robust material, yet the technology for its destruction, or at least its availability, has not kept pace with this progression. As technology has progressed, the storage capability of this media, especially hard disk drives, has increased exponentially. This has increased the security risk for two reasons:

- The amount of corporate information which is potentially vulnerable has greatly increased.
- The methods by which this media is disposed of and their standards are still in their developmental stages.

It can be reasonably assumed that the Canadian government, and industry in general, will continue to use IT media for storage. Therefore, in order to address the concern of the safety of the information, procedures and standards will have to be implemented to provide a resolution to this growing problem.

There have been papers and guidelines produced in the past. As mentioned the RCMP previously developed the *Technical Security Standard for Information Technology (TSSIT)* which provided guidelines in Section 4.6. The *Security Equipment Guide G1-001 (online on the RCMP GenNet Web site)* also provides guidance. Other pertinent publications include *Operational Security Standards for Handling Magnetic Media* (Department of National Defence, May 1998) and *Clearing and Declassifying Electronic Data Storage Devices, Version 2* (Communication Security Establishment, September 2000) and *Media Sanitization and Data Recovery Technology Assessment Report* (Communications Security Establishment, March 1998). These reports addressed the need for Government of Canada standards for the proper cleansing and disposal of hard disk drives. However, until Government of Canada standards are adopted these reports and standards will not be the same for all government departments or may be interpreted as suggestions only.

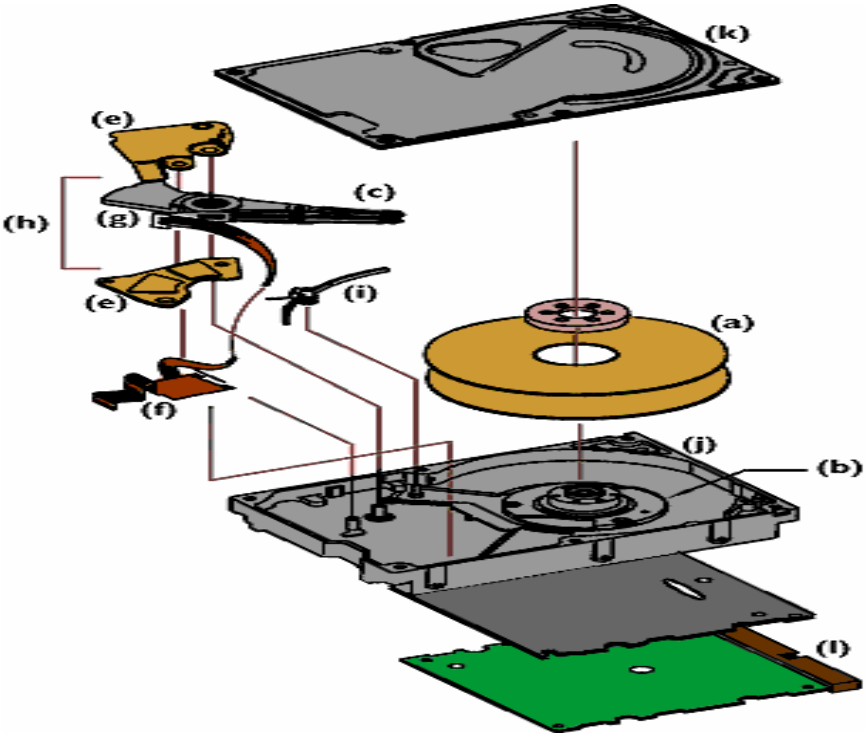
3.2 Hard Drive Construction

In order to better understand why the destruction of hard drive information is of such relevance, it is first necessary to describe their composition and how easily the information could be extracted.

A hard disk is part of a unit, often called a "disk drive", "hard drive," or "hard disk drive," that stores and provides relatively quick access to large amounts of data on an electromagnetically charged surface or set of surfaces.

A hard disk is really a set of stacked aluminium "disks" with a magnetic oxide coating. Each of the disks, like phonograph records, has data recorded electromagnetically in concentric circles or "tracks" on the disk. Each track is further divided into sectors, a set of which is called a “cluster”. A sector is addressed by its track number and sector number. A "head" (something like a phonograph arm but in a relatively fixed position) records (writes) or reads the information on the tracks. Two heads, one on each side of a disk, read or write the data as the disk spins. Each read or write operation requires that data be located, which is an operation called a "seek." Data already in a disk cache, however, will be located more quickly.

A hard disk/drive unit comes with a set rotation speed varying from 4500 to 7200 rpm inside a metal container. Disk access time is measured in milliseconds. Data is written and read by read/write heads, which are designed to ride on a microscopic cushion of air, without touching the platter. They register bits from the magnetic coating, which races past them. There will typically be six arms, each with read/write heads. The synchronous movement of these arms is performed by an electro-mechanical system called the head actuator. The hard disk data can only be attained via one head at a time. Since a hard disk typically contains three platters with a total of six read/write heads, the concept of *cylinders* is employed. Read/write heads move synchronously. Therefore, data is written up and down from platter to platter. One file can easily be spread over all six platter sides. Today's computers typically come with a hard disk that contains billions of bytes (gigabytes) of storage.



The "hard drive" gets its name from the part that actually stores information: a rigid disk called a platter (a), which is rotated by a spindle motor (b). To increase storage capacity, most hard drives feature two or more platters. Information is written to and read from the platter by a read/write head, located in the head stack assembly (c). An actuator arm (d) holds this assembly in place. In turn, the actuator arm is positioned by upper and lower magnets, also known as mag plates (e). The mag plates control the movement of the actuator arm across the platter surface. This movement, along with the spinning of the platter, gives the read/write head access to specific locations on the platter.

Signals that are read or written by the head are amplified by the read/write preamplifier (f) which, along with the actuator coil (g) and the associated connectors, make up the flex circuit (h). Near the flex circuit is the airlock (i). When the drive is powered down, this device locks the read/write head into the "landing zone," a safe place on the platter where no information is stored. This helps prevents data loss. These components are encased in a base casting assembly (j) and a cover (k), which are sealed tightly in a clean room environment. This keeps out dust and other contaminants that can damage or destroy the drive.

Every drive also contains a printed circuit assembly (PCA) (l). The PCA houses the drive electronics that allow the

hard drive to communicate with the computer, and allow all of the hard drive components to work in synch. Among these electronics are a microprocessor that controls all of the drive functions; interface electronics, which communicate with the computer's interface bus; a controller ASIC, which operates all of the controller hardware for the drive; the read channel, which encodes and decodes the data; and a motor ASIC, which drives the motor and actuator coil.

The read/write head consists of a tiny electromagnet. The shape of the head end acts like an air foil, lifting the read/write head slightly above the spinning disk. When the disk rotates under the read/write head, it can either read existing data or write new data.

If a current is applied to the coil, the head will become magnetic. This magnetism will orient the micro magnets in the track. This is write mode. If the head moves along the track without current applied to the coil, it will sense the micro magnets in the track. This magnetism will induce a current in the coil. These flashes of current represent the data on the disk. This is read mode.

The read/write heads are incredibly tiny. In modern hard disks they float between 5 and 12 micro inches (millionths of an inch) above the disk. When the PC is shut down, the heads are auto-parked in a designated area of the disk so they will not be damaged during transport. The bits of data are stored in microscopic magnets (called *domains*) on the disk. They are written in this manner: before recording data, the drive uses the read/write heads to orient the domains in a small region so that the magnetic poles all point in the same direction. A reversal of polarity is interpreted as a digit one. Unchanged polarity is interpreted as a digit zero.

Although the physical location of a file can be identified with cylinder, track and sector locations, these are actually mapped to a logical block address (LBA) that works with the larger address range on today's hard disks. Essential data is held in three areas of the disk and access to this data is essential to the data recovery process. These three areas are: partition tables, the boot block and file allocation tables. The partition table contains the structure of the disk including start and end points, errors and details of corrupt areas. A hard disk contains a Master Boot Record, a file allocation table, a directory and the data area. The Master Boot Record contains information about the disk partitions. The boot record is a short program written in machine code which issues the instructions to load the operating system into memory. It also contains information about the disk such as the number of bytes per sector and the number of sectors per cluster. The boot record is stored in the first sector of the first track on a disk or platter containing the active operating system (e.g. MS-DOS). Once the code for the operating system has been found, the boot record starts loading that code into memory and then hands over the control to the operating system. The operating system then completes the boot up process. A contiguous set of cylinders must be allocated for storing the operating system.

3.3 Security Definitions

Most departments have internal policies relating to the security level of the data to be stored on their network and its devices. Unfortunately, the understanding of what constitutes the level of designated or classified information can vary from department to department. Even an individual’s interpretation of the definition can vary and often data resides on storage media which could, unbeknownst to the author, cause serious compromise to an organization’s integrity if it were to be exposed. For this reason, there exists various media cleansing methods which can be utilized with a reasonable level of expectation of its effectiveness. Since this guide is primarily geared towards the methods for protecting Protected “C” or Secret and above information on hard disk drives, the focus will primarily be geared toward the disposal of that information. However, the disposal of other less sensitive information will also be addressed.

In order to better understand what level of security should be applied to information, it is first necessary to understand the various security levels as defined within section 10.6 of the Government Security Policy:

> **10.6 Identification of assets**
>
> **Confidentiality**
>
> Departments must identify information and other assets when their unauthorized disclosure, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*, could reasonably be expected to cause injury to:
>
> a. the national interest. Such information is classified. It must be categorized and marked based on the degree of potential injury (injury: "Confidential"; serious injury: "Secret"; exceptionally grave injury: "Top Secret").
>
> b. private and other non-national interests. Such information is protected. It must be categorized and marked based on the degree of potential injury (low: "Protected A"; medium: "Protected B", high: "Protected C").
>
> (National Interest is defined as the "defence & maintenance of the social, political and economic stability of Canada").

The highest security level of the information contained on a disk drive that falls within the realm of these definitions means that the entire disk drive must be treated as if ***all*** of its contents were at this higher security level.

3.4 Media Destruction Types

Not only is data assigned a security classification but also the type of destruction necessary for the media is assigned a type. The methods of handling and disposal required for the media will depend upon the classification of data contained upon it. The principal consideration in the destruction of sensitive material of all kinds is to make the information indecipherable. The equipment or system used to destroy sensitive material is rated according to the degree of destruction accomplished and the level of sensitivity of the material being destroyed.

There are four levels of destruction, as defined within the RCMP Security Equipment Guide:

Type I: Destruction ensures that the molecular structure of the piece of information has changed to the point where no original pieces of information are in the resultant residue. Methods include incineration and melting. (Up to and including Top Secret).

Type II: Destruction ensures reducing all sensitive information up to and including Top Secret, written on media, to a size that is deemed safe to dispose of as unclassified waste. On any one piece of residue, there shall not be more than one complete alphanumeric character from any one line **and** not more than one complete alphanumeric character from the lines immediately adjacent. There shall not be more than three complete alphanumeric characters on any one piece of residue. Methods include shredding, disintegration and pulping (for paper). (Up to and including Top Secret).

Type III: Destruction is also accomplished by mechanical shredders and disintegrators however the standard is reduced. On any one piece of residue, there shall not be more than three complete alphanumeric characters from any one line. Methods include shredding, disintegration and pulping (for paper). (Confidential/Up to and including Protected "B").

Type IV: As approved on a case-by-case basis. This level of destruction is provided by contracted mobile or off-site destruction services. (Case by case basis).

The size of the resulting residue must be reduced and specifications be kept up to date as the media contains a higher and higher density of data. For this reason, it is best to use the above guidelines since they are not tied to any specific technology limitation. Although these specifications were developed originally for paper type media the same criteria can be used for IT media (i.e. destroying media to a limited number of "bits"). For specific devices recommended for the destruction of IT media (by type), the RCMP Security Equipment Guide is now available online through GeNet at http://www.rcmp-grc.gc.ca/tsb-genet/seg/guide/destruction_e.htm.

4 Existing problems

4.1 Disposal Methods

The RCMP has been approached on numerous occasions by federal government departments for a proposed solution to the problem of hard disk disposal or cleansing. Departments often send their outdated or unused computers offsite to schools or other organizations. The contents of the hard drives of these computers is of concern and the correct method of dealing with it requires analysis. Likewise, if a drive is found to be non-serviceable or in need of repair, it must be properly cleansed before being sent offsite.

The U.S. Assistant Secretary of Defense has published the directive *Disposition of Unclassified DoD Computer Hard Drives* (June 4, 2001). The directive addresses four methods and procedures for sanitizing and clearing hard drives. The four methods are: disk overwrite utilities, degaussing (demagnetizing), physical destruction and clearing data (deleting files). Their recommendations were taken into consideration in the development of this paper.

The Canadian Department of National Defence (DND) has published its own *Operational Security Standards for Handling Magnetic Media* (May 15, 1998). This standard and the Communications Security Establishment publication *Clearing and Declassifying Electronic Data Storage Devices, Version 2.0* (September 2000) were referenced in an effort to find common guidelines in order to produce recommendations bearing an industry-wide approval rating at a federal level.

The Universal Secure Overwrite (USO) standard which is being developed within the United States has yet to be released. This standard will determine the proper procedures of overwriting hard disk drives. Individual manufacturers are expected to adopt this standard once it becomes available so that the self-sanitization software will be built in the hard drives.

4.2 Data Recovery Methods

Depending on the level of need and the financial resources available to recover data from a disk drive, the ability to recover information could be extremely costly and time consuming or it could be as simple as running commercially-available data recovery software.

4.2.1 Unerase Utilities

Data is stored in random fashion on a computer. Computers use a FAT (File Allocation Table) to track the used and unused portions of a disk. Since files are not normally stored contiguously on a disk, the FAT keeps track of where each part of a file is stored on a disk. When data is deleted it is simply removed from the file allocation table thereby marking those sectors as available to store new data. Until new data which is stored in a random fashion on the disk is written to each and every sector that housed the deleted data, portions of that data are recoverable. There are software utilities commercially available which will provide access to this data which the user thought was “erased”.

4.2.2 Microscopy

Until it is overwritten several times potentially important information can be retrieved from a computer. Using magneto-resistive microscopy (also known as magnetic force microscopy (MFM)) it is possible to recover portions of this data. The technique is derived from scanning probe microscopy (SPM) and uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface of the disk where it interacts with the emanating stray fields. An image of the field is formed by moving the tip across the surface and

measuring the force in relation to its position. There are variations to the process but the end result is the same. Even a relatively inexperienced user can start getting images of the data on a drive platter in approximately five minutes. According to manufacturers' sales figures there are several thousand SPMs in use in the field today. If commercially available SPMs are considered too expensive it is possible to build a reasonably functional one (less than $2,000 U.S.) using a PC as a controller.

Truly deleting data from magnetic media is very difficult. When data is written to the medium, the write head sets the polarity of most, but not all, of the magnetic domains. This is partially due to the inability of the writing device to write in exactly the same location each time, and partially due to the variations in media sensitivity and field strength over time and among devices. Deviations in the position of the drive head from the original track may leave significant portions of the previous data along the track edge relatively untouched. Newly written data is often superimposed over previously recorded data which persists at the track edges. Each track contains an image of everything ever written to it, but the contribution from each "layer" gets progressively smaller with each overwrite.

4.2.3 Data Recovery Software

A number of commercial products and services are available which will recover or attempt to recover data from a disk drive using commonly available or proprietary algorithms. (e.g. a product such as "EnCase"). Depending on the situation, you can often rebuild the master and partition boot records (MBR, PBR) and FAT of the hard drive, and you can find and recover lost or damaged files and directories.

The success of the recovery depends on the extent of the damage to the media or the effectiveness of the means used to delete the data. While there is a strong likelihood that these products will recover a specific drive, there are some drives that cannot be recovered. The data can be missing, written over, fragmented or scrambled in a way that makes recovery virtually impossible for a single software tool. The drive may be electronically or mechanically damaged, making recovery impossible without tearing the drive apart in a clean room, replacing components, and then trying to bring the drive up.

The exact methodology used for data recovery is usually a trade secret and the cost is often directly related to the time and effort required for the recovery. The cause of the data loss, overwrite as opposed to a damaged disk, greatly influences the cost as well. In fact, it was determined that recovery of data damaged by an overwrite utility was not a feasible solution at most recovery services and that the drives be taken to specialized laboratories where microscopy techniques are utilized. The cost of microscopy techniques would certainly be prohibitive to the majority of the population due to its cost and specialized expertise. Also, the probability of substantial recovery is extremely low given all of the factors listed in the previous section.

5 Existing solutions

5.1 Partial Destruction by National Archives

The RCMP visited the National Archives site at Tunney's Pasture in January 2002. A tour was given of the facilities and their present disposal methods for both paper and IT materials. In respect to the IT media disposal, they presently dispose of tapes, diskettes and CDs (up to Protected "B") by having it ground up through an SEM (Security Engineered Machinery) disintegrator. This disintegrator however is not robust enough to handle the destruction of hard drives. Their present means of destroying disk drive media consists of drilling three or four ¾-inch holes through the disk assembly and then sending it to a local metal recycling plant (Bakermet) where it is pulverized into three to five inch pieces. The resulting products are then sent to a steel mill for remelting. The recycling employees are all security cleared.

5.2 Re-Use of Hard Drives

5.2.1 Re-Use of Media within the Same Environment

The RCMP TSSIT Guide has recommendations regarding the re-use of IT media in the same environment where confidentiality is a concern. These are contained in Appendix OPS-III (page 1). Specifically it recommends that "media can only be re-used for the same level of sensitivity or above."

5.2.2 Computers for Schools

Computers for Schools, an Industry Canada program, will pick up unwanted or outdated but functional computers from government departments/private companies and ship them to schools. The federal government-led program operates in cooperation with the provinces and territories and the private and volunteer sectors to collect, repair and refurbish donated surplus computers from government and private sector sources. The computers are then distributed free to Canada's schools and libraries after the RCMP's DSX Disk Wipe Utility is run on the hard drives.

It is **mandatory** for Government of Canada departments to offer their surplus computers to the Computers for Schools program, as per the Appendix, Section 8.2.2 of the Treasury Board policy *Disposal of Surplus Moveable Crown Assets* which reads:

> 8.2.2 All personal computers (MS-DOS/Windows and MacIntosh) and associated monitors, keyboards, mice, printers, modems, servers, hubs, network cards, disk operating systems and related equipment which become surplus to government requirements must be offered intact to the Industry Canada Computers for School Program. Custodians are not authorized to sell, trade, donate or otherwise dispose of these assets prior to making this offer. Custodians are responsible for disposal of any equipment that is not accepted by the CFS Program.

Also in the same Appendix, Section 8.2.3 states:

> Custodians should ensure that surplus computers are not 'cannibalized' or otherwise rendered unusable prior to transfer. The practice of removing hard drives, random access memory (RAM and other essential components from computers before transferring them should only be done in those rare situations where security requirements dictate it".

It is strongly recommended by the RCMP to run the DSX utility **before** computers are sent to the Computers For Schools Program to ensure the confidentiality of data. No data higher than Protected "B" should reside or have previously resided on these drives before leaving the client department. In order to

ensure the successful elimination of secure information, CFS uses the RCMP DSX disk overwrite utility at the triple overwrite setting.

The reason for the success of the CFS program is its cost-effectiveness. In order to ensure this continues, hard drives **must** be included with the computers they receive. However, for the very limited number of machines (less than 5%) whose drives contain Protected “C”, Secret, or Top Secret information, it is recommended that those drives be destroyed as per our recommendations.

5.3 Running Disk Overwrite Utilities

There is commercially available software available which will entirely overwrite a computer hard disk multiple times. One would think that the more times the overwrite, the more difficult the recovery. However, more than three overwrites generally buys little if any added benefit. Multiple overwrites are likely to track one upon the other and if the recording head has been shifted such that it is leaving track-edges, then multiple overwrites will do little to eliminate them.

The general concept behind an overwriting scheme is to flip each magnetic domain on the disk back and forth as much as possible (which is also the basis behind degaussing) without writing the same pattern twice in a row. Magnetic media must be overwritten many times with alternating patterns in order to erase it. There is a complication in that the disk surface must be saturated to the greatest possible depth. Very high frequency signals only scratch the surface of the magnetic medium. Disk drive manufacturers use the highest possible frequencies in order to achieve ever-higher densities but in order to do an effective overwrite, the lowest possible frequencies are required in order to penetrate as deeply as possible into the recording medium. The write frequency also determines how effective previous data can be overwritten. The track write width is also affected by the write frequency - the track width decreases as the write frequency increases.

Some recording media are magnetically harder than others. For this reason, drive manufacturers publish figures for the magnetic "hardness" of their media and call this their ***coercivity***. They use two units to express their coercivity. The original Oersteds (Oe) (named for H.C. Oersted 1777-1855) or alternatively the present day kiloamperes per metre (kA/m). The media coercivity (its bonding capabilities) also affects the width of the write and erase bands. The width drops as the coercivity of newer higher-density drives increases.

In order to understand the theory behind the choice of data patterns to write for an effective disk overwrite it is necessary to understand the recording methods used in disk drives. The head itself only detects transitions in magnetisation so the simplest recording code uses a transition to encode a 1 and the absence of a transition to record a 0. Since putting a long string of zeros would make clocking difficult, a limit is made on the maximum number of consecutive zeros that are written for data patterns to be used for the overwrite.

The RCMP offers a disk overwrite utility, called DSX, free of charge to all government of Canada departments and agencies. It was developed in-house and allows for a single or triple pass overwrite. When the triple pass option is selected, binary 0s are written on the first pass, binary 1s on the second pass and an ASCII text pattern composed of the DSX version number and date/time stamp for the third pass. Each overwrite pass is followed by a read verify pass. Media I/O errors are reported and diagnosed at the sector level.

Where disk errors occur it is conceivable that intelligible information remains in areas not successfully overwritten. If the capacity of the disk to be overwritten, as reported by DSX, is less than the manufacturer's specifications, the excess portion will not be overwritten. This difference in reported size could either be an intentional deviation or a technical misrepresentation. This software does not currently support the UNIX operating system but there is such commercially available software which will perform similar functions.

There are three possible shortcomings to the effective use of Disk-Overwrite utilities. They are: human error, software failure and data remnants.

Human error or software failure can be caused by improper running of the overwrite software and the assumption that the software ran thoroughly when in fact it did not. Appendix "A" of this guide outlines the "Conditions For Use (CFUs)" for the proper usage of a Disk-Overwrite utility.

Data remnants can occur at track boundaries (edges). The disk read/write heads do not always pass concentrically over the exact or original bit pattern due mostly to mechanical and electrical variables and tolerances. The result is that residual "track edges" of the original bit patterns are generally left on the disk platter even though the bulk of the track will have been overwritten. The microscopy techniques described above can be used to image these edges. Depending on the number and remnant quality of these edges, processing can be done on them to reconstruct the original (overwritten) bit patterns of information. In order to ensure that residual track edge phenomena are not present on a disk, it is essential to perform deliberate +/- overwrites which extend beyond the original track edges. Standard disk controller firmware does not provide this type of offset control at this time. In effect, overwriting can never be 100%; some unknown technique may one day be able to restore data.

Blocks or clusters of data that show damage are eventually marked as bad and this can be done by the software itself. (i.e. SCSI hard drives) or by software (the operating system). In many cases, it is impossible to "scrub" bad blocks (the hard drive itself makes them inaccessible). This is where the drive must by physically destroyed or degaussed.

5.4 Degaussing

Degaussing (or returning the recording media to its original state) is an alternative means of erasing media which requires specialized equipment. It is possible in most equipment to erase data by passing the medium across an erase head but this normally would be a lengthy process. It is speedier and much more practical to submit the medium to a field which can be made to demagnetize it in one short operation. This is achieved by subjecting it in bulk to a series of fields of alternating polarity and gradually decreasing strength. Equipment capable of doing this is called a degausser. Its function is to reduce to near zero the magnetic flux stored in the magnetised medium. Flux density is measured in Gauss or Tesla. The degaussing field is produced by passing an alternating current through coils which energize the erase heads. It is considerably stronger than the field used in the original recording and magnetises the medium alternately in opposite directions each half cycle. The degaussing field is measured in Amps/metre. During the process, the media item is passed at a slow constant speed across the heads and out of their erasing fields. This is similar in many respects to a car slowly progressing through the water mist in an automatic car wash. The erase field is automatically controlled by the unit as the operator loads and processes the media. However, the operator is still responsible for ensuring that the media is positioned correctly and that the full erase process is completed. It is achieved by controlling the speed at which the screened drawer containing the media unit is closed and then withdrawn. In other words, the speed of movement of the drawer plays a critical part in the degaussing procedure.

Bell Laboratories in the USA introduced the unit "bel" named after Alexander Graham Bell, the inventor of the telephone. A unit of one bel was applied to any measurement of sound related to the ear. The bel means simply "twice as loud as another sound ". For practical purposes the smaller unit the decibel or dB was employed. A base reference 0dB was introduced, the value of which was dependent upon the type of sound measurement being made, e.g. sound pressure or electrical energy.

Degaussing will work through most drive cases. Research has shown that the aluminium housings of most disk drives attenuate the degaussing field by only about two decibels. For typical disk drive media, the short-term field needed to flip enough of the magnetic domains to be useful in recording a signal is about 1/3 higher than the coercivity of the media. Coercivity, measured in Oersteds (Oe) is a property of magnetic material and is defined as the amount of field necessary to reduce the magnetic induction in the material to zero - the higher the coercivity, the harder it is to erase data from the medium.

Each type of magnetic media is distinguished by the rate of coercivity required to ensure the medium is brought back to its zero state. Due to the variations of media formats and their corresponding magnetic densities, a correct and effective degaussing process is often difficult to achieve. Coercivity strength of an applied magnetic media determines which type of degausser should be applied to the particular magnetic media being targeted for sanitization. Higher coercivity rates are usually required to degauss hard disk storage media and many degaussers designed for commercial use do not have the magnetic energy required to erase media with a higher coercivity rate.

Degaussing often destroys the hard drive’s timing tracks and servo motors, and usually demagnetizes the permanent magnets of the spindle motor on sealed drives. Thus they can seldom be used after degaussing.

5.5 Hard Drive Destruction

Destruction of a hard drive is the process of physically damaging a media so that it is not usable in a computer and so that no known exploitation method can retrieve data from it.

The level to which destruction of the drive needs to be conducted is a matter of debate or need. A hard drive could be made inoperable by physical force such as the drilling of holes (as is done at National Archives) or hammering that will disfigure, bend, mangle or otherwise mutilate the hard drive so that it cannot be re-inserted into a functioning computer. It could be sent to a metal destruction facility (i.e. smelting, destruction or pulverization). Application of a concentrated abrasive substance such as sanding or grinding of the disks’ recording surface can be effective but is more labour intensive, including disassembly to gain access to the drive’s surface.

The most physically effective, environmentally sensitive and cost-effective method of physical destruction of hard drives would appear to be destruction by industrial quality disintegrators. These machines feature interchangeable waste sizing security screens and use a fast, dry mechanical cutting process to shred the average size disk drive assembly. Using rotating blades of varying cutting durability and strength, these devices grind the metallic drives small enough to fall through a screen sized by a user’s requirements. Disk drive assemblies could be reduced to a size of ¼ of an inch with an extremely high level of confidence that the confidentiality of the information on those drives would not be compromised.

Realistically, data is distributed throughout a platter or perhaps multiple platters of a disk assembly. In order to make meaningful sense of information extracted from these platters, it would more than likely be necessary to know the exact location of this information throughout the platters to create a contiguous,

logical reconstruction of the original data. Even if it were possible to reconstruct the File Allocation Table (FAT), it would be virtually impossible to reassemble the thousands of metal fragments (and disregard the other non-platter contents of the drive assembly) to re-create the original platters in order to locate that data. The media would also have to be reconstructed such that it could be mounted again and spinning at the correct speed to extract the information. A proper threat/risk assessment would be necessary, of course, to measure the risk of this happening. Also, the level of security of the data contained on the media would have to be determined. However, the probability of reconstruction would still remain extremely low. In order to be 100% sure, the media could be destroyed to the molecular level (e.g. melting via heat or chemical breakdown utilizing acid). Neither of these two solutions is environmentally sound but is worth consideration. Degaussing and/or using an overwrite utility could also be utilized beforehand to augment the effectiveness of the disintegration.

5.6 High-Intensity Heat Application

The RCMP Explosives Disposal and Technology Section (EDTS) has developed a Hazardous Material Portable Thermal Burner for the purpose of destroying ammunition, drugs, exhibits, tobacco, etc. They have proposed that it could be modified to allow for up to three trays of 40 disks (120) to be subjected to intense heat for a cycle time of 30 minutes. The heat produced would be from 800 to 1200 degrees Fahrenheit which should be sufficient to alter the molecular structure of the drives enough to remove all data from the drives. However, this would have to be tested and verified by an independent laboratory. The drives would not be operational after this process and would have to be disposed of in a waste disposal facility, possibly after they have gone through a physical destruction process as an added insurance. The cost of running the burner would be minimal since the three propane tanks equipped with the device have a total burning time of approximately 15 hours.

6 Proposed solutions & procedures

6.1 Centralized Physical Destruction

As previously discussed, the RCMP met with the National Archives of Canada, represented by the Head of their Reference and Disposition Services, a Disposition Officer and a Reference Processing Officer, to discuss the idea of centralized destruction. A tour was given of their current operations and they were questioned on their ability to provide an extension of their current destruction facilities to include hard disk drives. At the time it was thought that with proper funding for the increased staff and updated shredder technology they would be receptive to expanding their destruction services to include computer disk drives. Unfortunately, upon further discussion, they felt it was not a strategic direction they were prepared to undertake at this time.

At a subsequent meeting of the Information Technology Security Committee (ITSC) a proposal was made for a business case to be submitted to Public Works and Government Services Canada (PWGSC) for their analysis concerning the establishment of such a facility. This is currently under development by the RCMP in conjunction with CSE.

The expense of running a centralized media destruction facility for all government departments would offset the cost of every department having to run their own. Departments could either store the drives onsite until they were ready to ship them to the centralized location or send them on an as-needed or regular schedule. Client departments currently arrange for their own secure delivery of paper products for shredding and it would be logical for this arrangement to continue for the process of disk drive/media destruction. Upon running the drives through the shredding machine at a centralized location, the resulting material would be safe enough for disposal at a smelting plant or landfill site. The cost of providing a centralized facility would include the purchase of a suitable machine, setting up the proper environmental conditions (including air filtration and noise reduction) and the staffing of the positions to carry out the process. The machine would require regular maintenance and the blades would have to be replaced/re-sharpened as necessary. The clients would run a disk overwrite utility on the drives, if physically possible, before sending them away for destruction. If not possible to run the disk overwrite utility, it would be imperative for the drives to be securely delivered to the facility.

It is proposed:

That, due to processing time factors, costs and limited instances of destruction requirements for this classification of material, the central destruction of IT storage media only be necessary for Protected "C" or Secret and above information, and that the media be first run through the centralized degaussing facility.

6.2 Centralized Degaussing

Likewise, the expense of purchasing and running a centralized degausser for all government departments would offset the cost of every department having to run their own. A unit could be purchased and run with one or two operators. Again, the exact costs would be determined by the robustness of the machine, its environmental requirements and the required technicians. A bonded and security-cleared courier could be used for transporting the drives to the centralized location where they would be degaussed on a scheduled or ad hoc basis by security-cleared technicians. The unit would be of a high enough rating such that it would provide ample Oersteds to erase any size of disk drive.

As technology improves and the recording density on disk drives increases, the strength of the unit would be reviewed on a yearly basis and it would be upgraded as necessary. When properly applied, degaussing would render any previously stored data on the hard drive media unreadable. Persons performing the degaussing function would have to be properly trained and certified. Because of its physically destructive nature, degaussing would only be used on drives which were not intended to be reused.
The delivery to the centralized degaussing facility would be the same process as that described for destruction above. The clients should run a disk overwrite utility on the drives, if physically possible, before they are sent away for degaussing. If this is not possible, it is imperative that the drives be securely delivered to the facility.

It is proposed:

That, due to processing time factors, costs and limited instances of degaussing requirements for this classification of material, the centralized degaussing of IT storage media only be necessary for Protected "C" or Secret and above information.

6.3 Disk Overwrite Utility

The RCMP will continue to offer its disk overwrite software (DSX) to government departments free of charge with limited support. Departments wishing to use the RCMP DSX Disk Overwrite Utility would continue their practice of contacting the Technical Security Branch to have a copy created for them. One copy would be provided per departmental security officer for distribution within the department. Updates can be sent either via email or via regular mail. It would be the responsibility of the departments to contact the RCMP for any updates to the DSX software or to change their contact person within the department. This software is not suitable for declassifying hard disks and the user assumes all risks for the improper usage of the software whether intentional or accidental. As mentioned, the risks could include the possibility of residual data still being available for extract given the right circumstances and the determination of the attempt to extract.

It should also be noted that overwrite utilities such as DSX only work if the drive is functioning properly. If there is a physical drive problem, then another method of removal/destruction will be required. In this case hard drive destruction and/or degassing is recommended. This would however permanently damage the hard drive and any existing warranty for the drive would most likely be voided. For these limited conditions, this loss would have to be considered a monetary loss necessary to enforce departmental security.

It is proposed:

That the DSX software (or equivalent) is suitable for the erasure of up to and including Protected "B" (for protected information) and is suitable only for Confidential (for classified information), when the "Disk Overwrite Utility Conditions For Use" (see Appendix A) are followed. The resulting "cleansed" drives could then be re-used but preferably in the same environment of the same department and only for storage of data of the previous security level or lower.

6.4 Computers for Schools Program

Government departments must continue to send their surplus computers to Industry Canada's Computers for Schools program. As proposed below, those very limited number of computers which have or

previously contained very sensitive material must have their hard drives dealt with in the manner explained. All others - the majority - should first run the RCMP DSX (or equivalent) Disk Overwrite utility to overwrite the hard disks in these computers before sending them to Industry Canada. Labels should then be attached to the devices identifying them as being "Overwritten By Department". Industry Canada must still run the utility again upon receiving them before sending them for use to the various school boards.

It is proposed:

That Industry Canada's Computers For Schools Program continue to receive surplus computers from Government departments as per Treasury Board policy. The hard drives in these computers must not have previously contained Protected "C" or Secret and above information. All drives, no matter the security classification, must be functional to the degree that a Disk Overwrite utility can be run on them and if that is not possible, they also cannot be given to the program. Those few drives that don't qualify for the program must be disposed of separately via the proposed destruction/degaussing facility. All other drives are acceptable within the donated computers but only if they are functioning and have been through a triple-overwrite Disk Overwrite utility with a "Overwritten By Department" identifier on them before leaving the client department. Industry Canada is still required to run an overwrite utility as per their current pre-distribution process.

7 Conclusion

Only the user knows the importance of his/her data. That is why it is so vital that a Threat/Risk Analysis be completed by a department to determine the sensitivity of the data they handle. In the case of hard drives, one must look at the probability of information being extracted from a drive. If a drive is degaussed and/or overwritten with a utility and subsequently put through a disintegrator, what is the likelihood of the resulting shards of metal ending up in the wrong hands with the right equipment and technology? Or if only a Disk Overwrite Utility is used for cleansing the disk, what are the odds that someone will have the technology, knowledge and good fortune to be able to extract residual data from these platters? And what are the odds of someone locating secure information on that material given that data is spread out over one or more platters? What would be the risks to a government department or individual if this information were to be made available to the general public or covert entities?

It would appear from the results of the original survey sent out to the ITSC that there is a limited amount of highly sensitive information contained on hard drives. This would result in a limited amount of labour for both degaussing/overwriting and physically destroying the drive. Therefore, we recommend the following:

7.1 For a hard drive containing the following security level of information:

- **Protected "A" (Protected) or**
- **Protected "B" (Protected) or**
- **Confidential (Classified)**

We recommend:
That the drives be "cleansed" by a **triple** overwrite of the RCMP DSX disk-overwrite software (or a third-party equivalent that meets RCMP overwrite guidelines). It is important that this process be done in accordance with the Conditions for Use shown at Appendix A. The drives may then be re-used within the department, or if no longer required they may be donated to Industry Canada's Computers for Schools (CFS) program as per Treasury Board policy. Following the triple overwrite, if it is not feasible to re-use the hard drives or to donate them to the CFS program, the drives may then be disposed of or the material recycled.

7.2 For a hard drive containing the following security level of information:

- **Protected "C" (Protected) or**
- **Secret (Protected) or**
- **Top Secret (Classified)**

or for a hard drive which is deemed to be non-functioning

We recommend:
That the drives be either:

a. passed through a commercial disintegrator having a ¼ inch residue screen (residue must be finer than ¼ inch to pass through the disintegrator debris screen),

OR

b. passed through a degausser strong enough to overcome the coercivity of the data contained on the drive. This degausser must be listed on the National Security Agency (U.S. Department of Defense) Degausser Products List found at **http://www.dss.mil/infoas/degausserlst.pdf** or else obtain an independent laboratory's confirmation of the maximum Oersteds that can be degaussed.

Under either procedure the drives are no longer functional at this point - all material may then be disposed of or recycled.

7.3 Summary

To summarize, departments/agencies are ultimately responsible for the integrity, availability and confidentiality of their information. In order to ensure these qualities, Government of Canada standards must be developed for the erasure, destruction and disposal of all hard drives and other magnetic storage media. Failure to do so could result in a department or the Government of Canada being subjected to embarrassment, irreparable damage to their reputation or even pose a serious threat to the stability of its infrastructure or the safety of its employees and Canadian citizens.

In closing, here is an excerpt of the statement made on September 6, 2000 by Mr. Michael Robert Overly to the Subcommittee on the Constitution of the Committee on the Judiciary, U.S. House of Representatives. Mr. Overly is a well-respected expert on information technology storage and its legal repercussions. He was a research engineer for many years in the defence industry. He is an attorney and the author of the well-known reference book *Overly on Electronic Evidence*. He was called before the Subcommittee to present his opinion on a plan to adopt clear policies regarding employees' use of computer resources:

> *"Businesses have three general areas of concern regarding employee use of their computer resources: (1) minimizing potential liability of the business to its employees or third parties; (2) protecting sensitive business information from unauthorized disclosure; and (3) reducing potential waste of computer resources. These concerns require businesses to have the ability to monitor and review employee use of their computer resources to insure those resources are used properly.*
>
> *Employees, on the other hand, generally evidence a profound lack of appreciation of the potential liability that may arise from use of their employer's computer resources, particularly e-mail. Much of the problem results from the incorrect perception of most employees that their electronic communications are entirely ephemeral in nature: existing for only a short time and then permanently erased. Nothing could be further from the truth. Records of e-mail and computer use may be maintained for many years. Even deleted messages and files may be retrieved weeks or months after they were thought deleted."*

8 References

1) Government Security Policy (GSP), February 1, 2002, Treasury Board of Canada Secretariat

2) Technical Security Standard for Information Technology (TSSIT), August 1997, Royal Canadian Mounted Police

3) Beyond Fingerprints - Recovery of Electronic Evidence http://www.ontrack.com/datatrail/beyondfingerprints.pdf

4) Disposition of Unclassified DoD Computer Hard Drives, U.S. Department of Defense (June 7, 2001) http://www.defenselink.mil/nii/org/sio/ia/diap/documents/ASD_HD_Disposition_memo060401.pdf

5) Destruction of DoD Computer Hard Drives Prior to Disposal (January 8, 2001) http://www.defenselink.mil/nii/org/cio/doc/computerdisposal.pdf

6) Operational Security Standards for Handling Magnetic Media, Canada Department of National Defence, May 15, 1998

7) Media Sanitization & Data Recovery Technology Assessment Report, Communications Security Establishment, March 31, 1998

8) Clearing and Declassifying Electronic Data Storage Devices, Communications Security Establishment, September, 2000.

9) Digital Archaeology: Rescuing Neglected and Damaged Data Resources http://www.ukoln.ac.uk/services/elib/papers/supporting/pdf/p2.pdf

10) Hard Disk Overwrite & Inspection Utilities for IBM-PC & Compatible Systems, RCMP, April 2002

11) Secure Deletion of Data from Magnetic and Solid-State Memory, Peter Gutmann, Department of Computer Science, University of Auckland.

12) Statement by Mr. Michael Robert Overly before the Subcommittee on the Constitution of the Committee on the Judiciary, U.S. House of Representatives, September 6, 2000. http://www.house.gov/judiciary/over0906.htm

13) Electronic Evidence and Records Retention http://www.willyancey.com/electronic_evidence.htm

14) http://www.hivercon.com/hc02/talk-seifried.htm

15) http://cryptome.unicast.org/cryptome022401/nispom/nispom.htm (DOD 5220.22-M)

16) Treasury Board Policy “Disposal of Surplus Moveable Crown Assets” http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/materielmanage/dsmca1_e.asp#Appendix%20-%20Guidelines

APPENDIX A - Disk Overwrite Software "Conditions For Use (CFU)"

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 at least the same configuration management and security protection controls as the disks they will be used to overwrite. Document your procedures to ensure adequate controls are enforced to prevent unauthorized modification or subversion of the overwrite software. Place and maintain under Configuration Control. Ensure your procedures prevent all access by unauthorized users of this program to ensure all data is securely erased.

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 which 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 be 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. There is no standard for reporting disk drive capacity. Frequently, drive capacity is reported using different units, i.e., binary or decimal byte 'equivalents'. This can be very 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 disk drive's addressable storage capacity is to calculate it.

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 sector areas 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 sector areas should not be released for reuse. In certain cases, the disk controller may contain logic to automatically re-map around a bad track, causing no errors to be generated on overwrite.

CFU #6 - Require that Overwrite applications be run from a bootable floppy disk.

Disk drive overwrite applications are only designed and tested to run within a very specific operating system. Due to the drive capacity reporting anomalies reported in CFU #3, the disk overwrite utility will calculate or determine capacity based on its own algorithms and using operating system-dependent functions. Never use overwrite applications that are run from within any version of any operating system unless specifically recommended by the developer and unless the application has been 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 situations of the protected and classified categories.

The development and enforced use of application-specific, documented procedures are recommended to ensure consistency and repeatability of results for use of overwrite products, and for product-specific user training. Since typical overwrite software products are highly user-configurable items, and because the sequence of procedural steps used to overwrite and subsequently verify the correct overwriting of hard disks is 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 subjected to formal revalidation and certification for use.