Department of Energy

CIAC

Computer Incident Advisory Capability

UCRL-TM-216347

Clearing, Sanitizing, and Destroying Disks

CIAC-2325

William J. Orvis

March 2005

Lawrence Livermore National Laboratory

DISCLAIMER

This work was performed under the auspices of the U. S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

TABLE OF CONTENTS

\

DOCUMENT CONVENTIONS

Characters you type exactly as shown are in **bold** type. This includes commands, paths, and switches. The names of user interface elements are also bold, such as the names of dialog boxes and long program names.

Variables for which you must supply a value are in *italic*.

Code samples are in `monospaced` font.

Boxed Notes provide relevant information that is not directly part of the current thread.

> Security Tip – Security tips and information related to the current thread.
>
> Warning – Something to worry about concerning the current thread.
>
> Note – Other information related to the current thread but that is not security related.

Words defined in the glossary are in italic font in the text.

1 OVERVIEW

A continual problem at DOE sites is how to clear, sanitize, and destroy hard disks that contain classified information. Disks that are used in classified programs have relatively straightforward rules concerning their protection and disposition. Unclassified disks that have gotten a small amount of classified information on them have a separate set of rules that must be applied to them before they can go back into unclassified service. This paper discusses how the DOE rules and guidance apply to different situations of non removable hard drives containing different amounts of classified information. It discusses the clearing and sanitization requirements set down by DOE and how to use different software tools to meet those requirements.

One point to make is that plans for clearing and sanitization of drives that are going to be put back into service must be approved by the local DOE Area Office. Publication of methods in this paper does not imply blanket approval by DOE. You must still get approval for the sanitization plans that you intend to use.

According to the current DOE orders and guidance on clearing and sanitizing disk drives, drives that a re going to remain in a classified program must be cleared before they can be reused. Classified drives that are going to be used in an unclassified program in a controlled area can only do so if they are sanitized, marked, and protected so that they never leave the controlled area without being destroyed. Classified drives that are going to leave a controlled area must be destroyed. Unclassified drives that have inadvertently gotten a small amount of classified information on them can have that information sanitized and then the drives can be put back into unclassified service. Sanitization and clearing requirements for each of these situations is spelled out in the guidance (Appendix A, DOE N 205.12).

> **Note:** Most DOE sites have additional requirements that often go beyond those listed in 205.12. For example, LLNL requires that all drives, including unclassified ones, leaving the site as salvage are degaussed (destroyed).

Software exists from both commercial and government sources for clearing and sanitizing drives and for examining the raw sectors on a drive to find all copies of the problem data. In this paper, we use the Norton Wipe Info, Norton Disk Edit, Norton Ghost, Jetico BCWipe, Microsoft Disk Probe, DIBS Mycroft, and the LLNL Scrub programs for clearing, sanitizing, and examining hard disks.

2 INTRODUCTION

A continual problem at DOE sites is what to do with hard drives that contain classified information. You cannot simply delete the classified files and reuse or dispose of the drives as the information can be recovered by a variety of techniques. Because of this, there are very specific rules within the DOE for handling hard drives that contained classified information. This paper discusses options for abiding by those rules for six distinct situations.

- Classified drives that are going to be reused in the same or higher level classified program.
- Classified drives that are going to be used in a lower level classified or in an unclassified program.
- Unclassified drives that have inadvertently had a small amount of classified information placed on them
- Unclassified drives that have inadvertently had a large amount of classified information placed on them.
- Unclassified drives containing sensitive information that are going to be released to the public.
- Unclassified drives that do not contain sensitive information that are going to be released to the public.

We do this for systems with Windows 95/98/ME, Winodws NT/2000/XP, Macintosh, and UNIX (Solaris, Linux) operating systems. This paper is only concerned with magnetic media hard drives with fixed (non removable) disks. It does not consider floppy disks, Bernoulli (zip) disks, magneto-optical disks or CDs.

> **Warning:** Keep in mind that while the DOE rules specify that the magnetic media need to be sanitized or destroyed, the method used must be agreed upon and approved by the responsible DOE area office. While this document describes techniques for sanitizing and destroying media, it does not provide blanket approval for using those techniques. You must still get approval for specific cases.

Hard drives used on a classified system are themselves classified to the highest level that the system is capable of handling. When a drive is no longer needed for the particular program, it can be reused in another program at the same or higher level.

Classified media that is going to be reused in a classified program at the same or higher security level must be *cleared* before it can be reused to make it nearly impossible to retrieve the classified information. Classification's "Need to Know" rule requires that the media be cleared because the new users of the media do not need to know the information previously stored on the drive even though they may have a sufficient security clearance to do so.

> **WARNING:** The disks used in some classified programs such as Special Access Programs (SAP) or Sensitive Compartmented Information (SCI) can never be reused in a different classified program. See your *ISSO* for guidance.

Classified media that are going to be reused in a lower level classified program must be *sanitized* before they can be reused. Classified media that has been sanitized may also be used in an unclassified program as long as they remain in a controlled area. If they ever leave a controlled area they must be *destroyed*. The destruction must insure that there is no way that information placed on them can ever be recovered.

A problem that occasionally occurs is finding a small amount of classified information on an unclassified system. How that information got there is not the concern of this report and could be via an e-mail message or attachment, downloaded file, or the inadvertent typing of restricted information by someone who did not know or who has forgotten what is allowed on an unclassified system.

If the amount of classified information is small, current DOE rules allow only that data to be sanitized and the drive put back into service as part of an unclassified system. If the amount of classified information is large, the media becomes classified and is treated in the same manner as any other classified media.

When unclassified computer systems are no longer needed in a program, they may be released to other programs or declared surplus and donated to outside organizations or disposed of. Before these systems can be transferred or disposed of they must be cleared and that clearing documented.

There are two types of unclassified systems to consider here; those that have had sensitive information stored on them and those that have not. Sensitive information includes all types of information defined as such by the DOE. For example, personnel information (medical, financial), Unclassified Controlled Nuclear Information (UCNI), Naval Propulsion Information (NNPI), For Official Use Only (FOUO), and CRADA information.

3 WHY FILE DELETION IS NOT SUFFICIENT

The ability to extract useful information from a hard drive is described with two different attack scenarios,

- *Keyboard attack*
- *Laboratory attack*

A *keyboard attack* is one in which the information can be recovered from the hard drive using simple keyboard commands. Programs exist both within modern operating systems and as separate packages to recover deleted files. For example, on Windows systems **undelete** is available to recover deleted files and **unformat** to recover files from a formatted disk. A *laboratory attack* is where a disk drive may be disassembled and special equipment used to recover files.

> **Security Tip:** Formatting a drive is not sufficient to eliminate classified information. Modern format commands are specifically designed to disturb the data as little as possible so that the data can be recovered if the user mistakenly formats his drive. Only a format command that includes the capability to overwrite all sectors in a drive with a known pattern can be used to clear or sanitize a drive.

Before you can securely clear or sanitize a drive you must understand why file deletion is not sufficient. Modern operating systems generally have a two level deletion process where a file is first moved into a trash can (the first deletion) and later, the trash can is emptied (the second deletion). Files in the trash can have not really been deleted but have only had their directory entry moved into the trashcan directory. These files are easily recovered by simply dragging them out of the trash can into a normal directory. Files are not actually deleted from the disk until the trash can is emptied and those files have only the directory entry removed, not the contents.

> **Security Tip:** The so-called *Double Deletion* (dragging a file to the trash and emptying the trash) does not remove the contents of a file from a disk drive, only its directory entry.

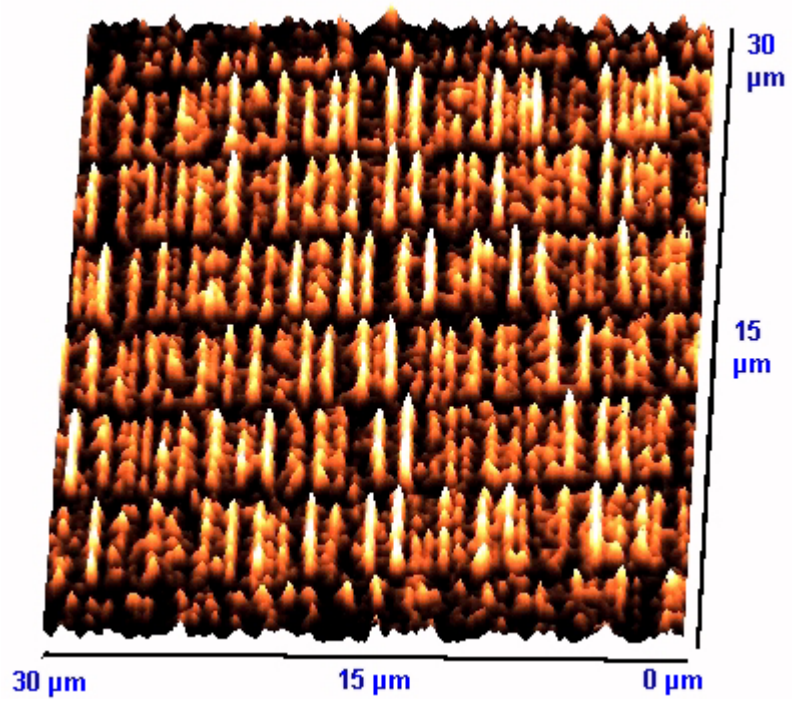
In most computer systems deletion of a file from the disk only deletes the file name from the directory and makes the space occupied by the file available for other files to use. It does not delete the actual file contents from the disk. This is equivalent to tearing out the table of contents of a book. The chapters are all still there and can be read by anyone who is interested. All that is missing is an easy way to find where a chapter starts. Tools are readily available, often built into the operating system, which can recover these deleted files with little effort or technical knowledge on the part of the user. This is a keyboard attack.

File deletion protection utilities such as Norton's Protected Trash give you even more chances to recover a deleted file. Utilities like this maintain copies of the deleted directory entries to make it easier for a recovery program to find and recover all or part of a deleted file on the disk.

After a sufficient length of time on a busy machine, all or part of the space occupied by the file may be overwritten by one or more different files making it impossible to be recovered using these standard software tools. However, it may still be possible to recover the file though that recovery requires removal of the drive and its analysis in a laboratory environment.

When a new track of data is written over some old data, it does not completely overwrite the old information. That is, a 1 written on top of a 0 is actually more like a 0.95 while a 1 written on top of a 1 is a 1.05. This extra data is seen as noise on top of the new data and is eliminated by the drive's electronics. Attaching an oscilloscope to the output of the drive head makes this noise visible and some data analysis of the noise that subtracts the new data can make the old data accessible. This is a laboratory attack.

Another problem with disk drives is that the drive heads do not always write a track in exactly the same place every time they write it. The result is data fringing at the edge of a track. The new data goes down the center of the track while older data runs along the edges. Again, special electronics that move the head onto the track edges may make them readable. Another method of reading the data uses Magnetic Force Microscopy (MFM) and Atomic Force Scanning Tunneling Microscopy (AFM). Both of these techniques create an image of the magnetic domains on the disk, including the fringing data along the edges of a track. For example, the image below is an MFM image of a hard disk drive (Topometrix, http://elchem.kaist.ac.kr/jhkwak/TopometrixWeb/datast4.htm). Bright and dark areas show the magnetic orientation. Tracks are horizontal in this image. Bits are recorded where the magnetic direction changes. These are also laboratory attacks.



From this you can see that overwriting a file does make it inaccessible via normal computer operations (a keyboard attack). You can also see that using overwriting it is

nearly impossible to make a file totally inaccessible to someone who can remove the drive and subject it to laboratory analysis (a laboratory attack). These facts are the basis for the DOE rules on clearing and sanitizing drives.

A good paper that explains the technical details of these effects is Peter Gutmann's *Secure Deletion of Data from Magnetic and Solid-State Memory*, which is available online at the University of Auckland (see References).

4 WHERE DATA HIDES

Data written to a disk drive does not always sit in a single file even if a single file is the final result of whatever operation put the file on the disk. When sanitizing a disk containing a small amount of classified data, you need to be aware of all the places that the data written while moving it onto the drive. Information found in a single file may not only be in that file but may be found in several different places on the disk. For example, if a file containing classified information is copied onto a hard drive it likely only exists in that single file. However, consider an incoming mail message with an attachment. If you download the message with Eudora (a mail reader), open the attachment with Word, and discover that it is classified, where on the disk could the file be?

Eudora first connects to your mail server and downloads the e-mail message to the spool directory (copy 1). It then parses the e-mail file into the e-mail message and the attachment, making temporary files in the temp directory (wherever you have defined the variable TEMP to point to) (copy 2) and the spool directory (copy 3). The attachment is decoded and copied to your attachments directory (copy 4). The e-mail message is copied to Eudora's In mailbox. If the e-mail message is also classified you now have another copy (copy 5). While Eudora is running, it may be swapped out of memory into the *page file*. If this happens while it is downloading the classified e-mail or extracting the attachment then you have another copy on disk (copy 6) in the page file. If the e-mail is classified and you have a filter that moves the message to another mailbox, you have another copy (copy 7).

> **Security Tip:** Copies 1, 2, and 3 are encoded with a base64 encoding scheme if the attached file is binary such as a Word document. This is not encryption, it is only an encoding to change the binary into printable text so it can be e-mailed. The result is that you cannot search for the document using text in the Word document as they are hidden by the encoding.

> **Security Tip:** If the sender's e-mail program is setup to send e-mail as both plain text and styled (html formatted) text, the text of the e-mail message is doubled. The second copy will also contain html formatting codes which might make it difficult to search for using words in the message. For example, if you were searching for the text "**dirty** word" in the e-mail message and the styled message had **dirty** in bold but not word, the text in the e-mail would look like "dirty word" which would not match your search string.

When you open the attachment with Word and edit it, Word creates temporary files that may also contain the classified information (copy 8). This is especially true if you edit or delete the classified text. If you save the document with fast save mode turned off, Word saves the document in a new file (copy 9) and then renames, the old file (copy 4 again). If Word is swapped out of memory while the file is open, another copy could be in the page

file (copy 10). The more times you edit and save a file the more potential copies can be left on your disk.

> **Security Tip:** If while the copies of the problem file are being written or read the disk drive discovers that one of the sectors used by that file on the disk is going bad, it will copy the information out of that sector to a new one and then mark the old sector as bad. *Bad sectors* are not used by any normal programs and will likely be skipped by format and overwrite programs. Essentially, the drive hides these sectors from the operating system and they could contain the classified information. This is a very low probability event.

File search programs generally require that the drive be indexed before they can search for a file by the file's contents. That index file also contains the words that were in the classified file (copy 11) though they will be reordered and are unlikely to be comprehensible.

If your system goes into hibernation mode the system memory is written onto disk in a hibernation file. If you were editing a document when this occurs, the classified information is written out into the hibernation file (copy 12). This generally only applies to laptops operating on batteries though new, power saving desktop systems will also do it.

As you can see, the sooner you determine that a file is a problem and the less that you access it, the fewer copies of that file are likely to be found on your disk drive. You need to resist the urge to take a look at the file just to see what is there. If you must look at the file, use a hex editor (i.e. Norton Disk Editor) or a plain text editor like Notepad.exe so you don't create temporary files. Don't edit the file with a word processor under any circumstances. Editing the file to remove the classified information may only hide that information from you while leaving it in the file on disk.

4.1 DATA HIDING IN WORD PROCESSORS

When Microsoft Word operates in fast save mode, it does not rewrite a file every time it saves it, it only rewrites the changed sectors. If you delete part of a file with Word, it simply places a jump instruction in the file to jump over the deleted text to the next piece of visible text. When you save the file, the deleted text is still there in the file, you just cannot see it from within Word. If you open the file with a hex editor or a plain text editor you can see the deleted text.

In WordPerfect, the undo command can be set to be able to undo changes across file saves. What this means is that you can delete a paragraph in a file, save the file, and give it to someone else. That person can then open the file, hit undo, and see what you deleted. Thus, all your deleted text is still hidden in the document file on disk.

High-end word processors also generate temporary files which may contain added or deleted text and could contain the classified information. Most temporary files are created

in the currently defined TEMP directory or in the same directory as the file being edited where TEMP is an environment variable.

Most word processors have autosave or autorecover enabled to prevent you from losing a lot of work in the event that the program or system crashes. The autosave files are stored in different locations, depending on the word processor. For example, Microsoft Word saves them by default in,

```
c:\Documents and Settings\<username>\Application Data\Microsoft\Word
```

where `<username>` is the name of the currently logged on user.

4.2 DATA HIDING IN MAIL PROGRAMS

Mail programs are another special case of data hiding because of the way they manage documents and the number of different places that they store data. Most mail programs store mail in a UNIX style mailbox file, which is simply the raw e-mail messages placed one after the other in a text file. To this, they add an index file that contains some of the header information (To, From, Subject, Date) and the location in the mail file of the body of the e-mail. When an e-mail message is moved to another mailbox or deleted, only the entry in the index is removed. The actual message is left in the mailbox file. The message stays in the mailbox file until the file is manually or automatically compacted. Compacting a mailbox file simply copies all the e-mail messages into a new file, skipping any that were moved or deleted.

Mail programs also differ in how they manage attachments. Microsoft Outlook Express leaves the attachments encoded in the original e-mail message until you manually extract them. Eudora extracts all attachments as the e-mail messages are received and stores them separately in an Attachments directory.

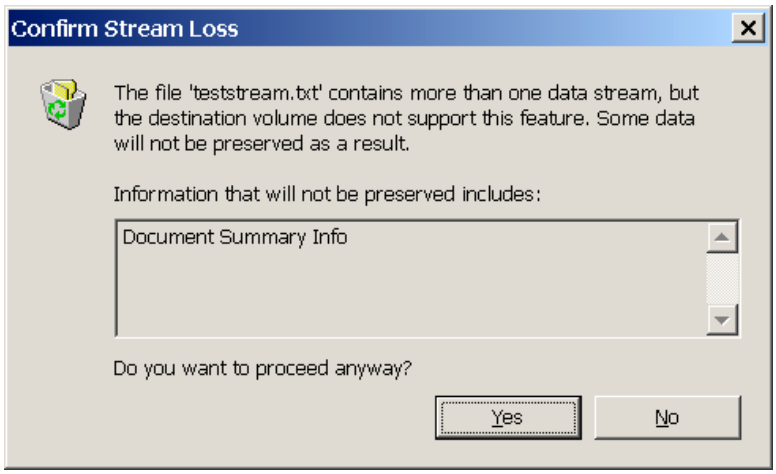
E-mail programs with styled text also have embedded objects, such as pictures that are embedded in the e-mail message. While technically, these are attachments, they are often treated differently from normal attachments. Eudora stores embedded graphics and files in an Embedded directory.

4.3 DATA HIDING IN ALTERNATE DATA STREAMS

As if this were not enough, there are other places data can hide on systems. On all Windows systems that use the NTFS file system (Windows NT/2000/XP) there is something known as an alternate data stream. Most files store data in the primary stream but could store data in an alternate stream. Most file listing programs such as the DOS DIR command or the Windows Explorer only show the primary stream even when data exists in a secondary stream.

As an example, you can add an alternate data stream to a file by adding summary properties to that file. In the Windows Explorer, select a file and choose the File, Properties command. In the Properties dialog box, select the Summary tab and add some data to the summary fields. Click OK and a second stream is added to the file containing

that summary data. To see if a file contains a secondary data stream, try to copy the file to a disk with a *FAT file system* such as a floppy. Because FAT file systems do not support alternate data streams Windows will give you the following warning that alternate streams are about to be lost.



4.4 Data Hiding in Slack Space

When disk space is allocated to a file it is done in *allocation blocks* containing several sectors rather than a byte at a time. Whenever a file fills a block, another is allocated. Allocation blocks are typically 2k to 32k bytes in size depending on the size of the disk drive. As a file is filled with data a pointer is created that points to the last byte written in the file. This pointer is the current *End-of-File* and generally does not correspond with the end of the currently allocated block. The space between the marker and the end of the block is known as the file *slack space*. The slack space generally has in it whatever happened to be on the disk at the time the block was allocated to the file.

Microsoft Word files handle slack space somewhat differently. When Word needs a new sector for a file, it grabs a whole sector and places the end-of-file marker at the end of the sector. Thus, it appears to have no slack space in that sector. However, Word is maintaining its own internal end-of-file within the last allocated sector. When a sector's worth of data is written to the disk drive, the unused part of the sector contains whatever was in memory when the sector's buffer was allocated. What this means is that if you were to edit two documents sequentially, the unused portion of the second document's sectors might contain part of the first document's content.

4.5 Data Hiding in Caches

As you use web browsers and mail programs to access content on the web and download files, many of those files are first downloaded into a cache. Depending on the program, that cache may have different names and locations.

4.6 DATA HIDING IN HIBERNATION FILES

Most laptops have the ability to go into *hibernation mode* when they are not being used in order to save battery power. To do that, they write the contents of memory into a *hibernation file*. When the machine wakes up, the contents of that hibernation file are read back into memory allowing the system to pick up where it left off. That hibernation file contains copies of whatever was in memory at the time the system was put into hibernation mode. When programs quit running, they don't erase the memory they occupied, they just leave it for the next program that is going to use that space to overwrite. If that block of memory is not needed before the system goes into hibernation mode, it will be written to disk and may contain whatever you were working on.

4.7 DATA HIDING IN DIRECTORIES

Most files stored on a hard drive have two separate parts, the file itself and the directory entry for the file. While directory entries do not contain a lot of data, they do contain the file name which can be over 100 characters long in modern operating systems.

4.8 DATA HIDING IN INDEX FILES

Most modern operating systems have the capability to index your hard drives in order to quickly find a file based on text within the body of the file. If a file containing classified information is indexed, the words that make up that information will be in the index file. While the words are in the file, they are not in order so the information is not directly readable.

5 DOE RULES FOR CLEARING, SANITIZATION AND DESTRUCTION

The DOE rules define three different processes for removing information from non removable magnetic media.

- *Clearing* – Erasing the data so that it cannot be retrieved by keyboard commands, such as running an "**undelete**" program. Clearing protects information from a keyboard attack but not from a laboratory attack.
- *Sanitization* – Erasing the data such that it is unlikely that even a laboratory attack can recover the data. Sanitization protects information from all but the most intense laboratory attack and even an intense attack is unlikely to be able to recover anything useful.
- *Destruction* – Erasing the data in a drive such that it can never be recovered by any means. Destruction involves physically destroying the magnetic recording medium. Destruction assures you that there is no possible way that information could ever be recovered from the drive. Drives that are to be destroyed should be sanitized first and then destroyed.

The rules for clearing, sanitization, and destruction are described in, *DOE N-205.12 Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware*, which is included in Appendix A.

The methods used for clearing and sanitization differ, depending on the type of classified information on the drive being cleared or sanitized and where it is going to be reused or destroyed.

The DOE Rules cover six different cases of hard drives being moved between different levels of classification.

- Classified drives that are going to be reused in the same or higher level classified program.
- Classified drives that are going to be used in a lower level classified or in an unclassified program.
- Unclassified drives that have inadvertently had a small amount of classified information placed on them
- Unclassified drives that have inadvertently had a large amount of classified information placed on them.
- Unclassified drives containing sensitive information that are going to be released to the public.
- Unclassified drives that do not contain sensitive information that are going to be released to the public.

Each of these will be considered in this chapter.

5.1 CLASSIFIED DRIVE STAYING IN A CLASSIFIED PROGRAM

Media that is going to stay within a classified program at the same or higher level of classification need be only cleared before it is reused. You must clear the drive to abide

by the need to know rule to prevent users in the new program from accessing data from the old program by normal means. The drive itself remains classified at the highest level it has been used at and must stay in a program that can handle that level of classification.

Clearing renders the information that was on that drive inaccessible to the current user as long as he is not able to perform a laboratory attack on the system.

Keep in mind that some classified programs do not allow disk media to be reused in any other program under any circumstances. For example, Special Access Programs (SAP) and Sensitive Compartmented Information (SCI) programs do not generally allow their hard drives to be reused. See your ISSM for specific guidance.

A three-pass overwrite is the approved method for clearing a classified drive being reused in a classified program at the same or higher level. The three-pass overwrite consists of:

1. Overwriting all writable locations with a character.
2. Overwriting all writable locations with the complement of the character.
3. Overwriting all writable locations with a randomly chosen character.

The *Designated Approving Authority (DAA)* for a site must approve the software tools used to perform the overwrites.

5.2 Classified Drive Moving to a lower level classified or an Unclassified Program

A drive used in a classified program may be used in a lower level classified program or in an unclassified program under certain conditions.

- The drive does not contain removable media.
- The new program must be in a controlled area.
- The drive must be sanitized with the three-pass overwrite.

If the drive is moving to an unclassified program, it must also abide by the following additional conditions.

- The drive must be marked as formerly containing classified data.
- The drive can never leave the controlled area without first being destroyed.

This rule applies only to hard drives with non removable media. The drive must stay in a controlled area and be marked so that it can never leave the controlled area without being destroyed. The drive can then be sanitized with a three-times overwrite. The sanitizing software must log any problems it has while sanitizing the drive.

The person sanitizing the drive must review the results of the overwrite, verify that this methodology has overwritten all sectors on the drive, and that the control procedures have been employed. The drive must be marked with a label that describes the drive and indicates that it has been sanitized according to DOE N 205.12. The certifier must also document the sanitization and maintain that documentation for a minimum of 5 years.

The software being used to sanitize a drive must be approved by the site *Designated Approving Authority (DAA)* and the overwrite methodology must be approved and reviewed by the site's senior security officer.

Security Tip: Verification involves checking the log file for the sanitizing software to insure that all sectors have been overwritten and to then examine a few randomly selected sectors to insure that the logs are correct. Examining every sector would cost more than the drive is worth. For example, if you are examining a 100 Gbyte drive and assuming you can look at one 500 character sector per second it would take you over 6 years to look at every sector working 24 hours a day.

Security Tip: Considering the current low cost of new hard drives and the cost of clearing and verifying a classified drive, it may be less expensive to simply destroy the drive and buy a new one than to try to sanitize and reuse it.

WARNING: Keep in mind that not all classified drives can be reused in a controlled, unclassified program because of the security rules pertaining to the data on the drives. Contact your ISSM for specific guidance.

5.3 UNCLASSIFIED DRIVE CONTAINING A SMALL AMOUNT OF CLASSIFIED DATA

The rules in 205.12 (Appendix A) have a special case for an unclassified hard drive containing a small amount of classified information. In this case, the classified information must amount to less than 20 Kbytes of information and less than 0.01% of the hard drives capacity. That is, for all drives over 200 Mbyte capacity, the 20 Kbyte rule is the operational limit.

The amount of classified information on a drive is determined as the number of bytes of classified data on that drive and not as the size of the file that contains that data. For example, if an unclassified document contains one sentence of classified information, only the size of that one sentence is used to determine if the drive meets the eligibility requirements to be sanitized and returned to service. If more than one copy of the document is on the drive, the amount of classified data in each must be totaled to determine the amount of classified information on the drive.

Security Tip: The amount of classified information can be estimated by assuming that each character (including spaces) equals one byte. This is sufficient even if *UNICODE* characters (2 byte character code) are used because for English text the second byte is always 0.

A drive meeting this criteria can be sanitized and returned to unclassified operation by sanitizing only the affected area with the three-times overwrite described above. The Designated Approving Authority (DAA) must approve of the products used to perform

the overwrite and the sites lead system security officer must approve the overwrite methodology. This person must also review the results of an overwrite and verify that this methodology has overwritten all sectors on the drive.

In this case, it is possible to use automated methods to scan the disk for the classified words to assure the lead system security officer that the classified data has been completely removed.

5.4 Unclassified Drive Containing A Larger Amount of Classified Data

Any unclassified drive found to contain more than 20Kbytes or more than 0.01% of its size of classified information becomes a classified drive at the level of the classified information found on it. It then falls under the rules in sections 5.1 and 5.2 and can be used in a classified environment, can be sanitized and used in an unclassified program in a controlled area, or can be destroyed.

There may be a few situations where the contamination is more than 0.01% of the capacity of the drive and the drive may still be put back into unclassified service after only sanitizing the contaminated part of the drive. The *Information Systems Security Program Manager* (*ISPM*) must approve any attempt to sanitize a drive in this way and put it back into service.

This special release is generally available for systems such as a large file or mail servers. In such a system, after being sanitized, the affected area of the disk is likely to be overwritten many times with different data in a short amount of time making it unlikely that the data could be both found and retrieved by any reasonable means. This is also true of large *RAID* systems where the contents of a file don't reside on a single drive but are spread across many drives, effectively chopping up the classified information into many small pieces. In all cases though, the ISPM must approve returning the disk to unclassified service.

5.5 An Unclassified Drive Containing Sensitive Information

An unclassified hard drive that contains sensitive information must be sanitized with the three-pass overwrite described previously before it can be transferred internally, declared surplus, transferred to an external organization, or disposed of. Sensitive information includes: *Unclassified Controlled Nuclear Information (UCNI)*, *Naval Nuclear Propulsion Information (NNPI)*, *Official Use Only (OUO)* information, medical information, financial information, trade secrets and other company information that is part of a Cooperative Research and Development Agreement (CRADA).

Individuals performing the sanitization must document that work. The document must include:

1. description of the media (make, model, serial number, etc.)
2. classification level
3. purpose for sanitization (transfer, destruction, etc.)
4. procedures used

5.6 AN UNCLASSIFIED HARD DRIVE THAT DOES NOT CONTAIN SENSITIVE INFORMATION

Unclassified hard drives that do not contain sensitive information must be cleared with a one-pass overwrite before they are transferred internally, declared surplus, transferred to an external organization or disposed of.

Individuals performing the clearing must document that work. The document must include:

1. description of the media (make, model, serial number, etc.)
2. classification level
3. purpose of clearing (transfer, disposal, etc.)
4. procedures used

6 CLEARING DISKS

The least secure method of removing information from disk drives is clearing. Clearing disks involves removing the classified information in such a way that it cannot be recovered by a keyboard attack. That is, there are no simple keyboard commands available to recover the information. You would need to disassemble the computer and use special equipment to recover any of the cleared information.

According to the DOE rules, classified hard drives may only be cleared by degaussing or by a three times overwrite. Unclassified drives that contain sensitive information must be cleared with a three times overwrite and unclassified drives that do not contain sensitive information may be cleared with a one time overwrite.

> **Warning:** Degaussing a drive has the unfortunate side effect of destroying the drive electronics and erasing the *index tracks* on the disk. While you could remove the drive electronics before degaussing, the index tracks are actually written on one of the disk platters. The index tracks tell the hard drive electronics where the tracks are on the disk and are written on a drive at the factory when it is manufactured. Index tracks generally cannot be put back on a drive using a simple format or other command.

Most small hard drives can be degaussed without opening the case as the aluminum case does not prevent the degaussing fields from entering the device and interacting with the disk platters. As mentioned above, degaussed drives are no longer usable.

Clearing a drive by performing a one time or three times *overwrite* does not destroy the drive but leaves it available to be reused. The three times overwrite consists of overwriting all locations with a character, with the character's complement, and with a randomly chosen character. This clearing rule only applies to a classified drive that is going to remain in classified service. Because of the existence of bad sectors, you would like to use a clearing program that attempts to clear the bad sectors as well. Most sanitizing programs are not able to write to bad sectors because those sectors are hidden from the system by the drive. Luckily, if a sector is bad, the operating system will not try to write to it. Only if a sector went bad after classified data was written there would a bad sector contain the classified text which is a low probability event.

Systems with a format command that writes a disk pattern while formatting and that have an option to "ignore the grown defects list" can also be used to clear a drive, including the bad sectors. Older model Sun systems had these capabilities in the format command. Newer systems utilize drives that are not really formatted when the format command is run but only overwrite the directory structure. The format programs for these systems usually have an option to zero the drive which does overwrite all writable sectors with zeroes, performing a one pass clearing.

All of the methods available for sanitizing a disk or file in the next section are equally applicable to overwriting as overwriting is just a single pass sanitization. That is, if you sanitize a disk or file you have more than covered the DOE requirements for overwriting.

Verification is generally not required here as the disk is going to be reused in a classified program.

Security Tip: Most UNIX operating systems (solaris, linux, irix, etc.) do not have utilities for examining each disk sector to see what is on it or to perform overwrites of unallocated sectors. Disks on these systems can be moved to a PC or Macintosh computer, cleared and examined there, moved back to their original computer, and reformatted back into a configuration the UNIX operating system wants.

7 SANITIZING DISKS

There are three different situations where sanitizing hard disks comes into play,

- Sanitizing a whole disk so that it can be retired.
- Sanitizing a whole disk so it can be used in an unclassified program.
- Sanitizing an unclassified disk that contains a small amount of classified information so that it can be returned to unclassified service.

Classified disks that are going to be retired must be sanitized and then destroyed. If the drives are not going to be immediately destroyed by the organization that is retiring them then sanitizing the drives beforehand assures the organization that information cannot be obtained from the drives while they are waiting to be destroyed.

Sanitization of drives that are going to be reused in a lower level classified program or in an unclassified program come under the special rules in section 4.2. These rules require that the drive not only be sanitized but that it be marked and protected until it is no longer needed and that it be destroyed before being released from that protection.

Sanitizing a small amount of classified data on an unclassified disk comes under the special rules described in section 4.3. These rules allow the drive to be returned to unclassified service after sanitizing by overwriting.

7.1 SANITIZING DISKS WITH DEGAUSSING

Disks that are no longer going to be used are sanitized with a Type I or Type II degausser. As long as the drive is not made of a metal that absorbs magnetic fields (such as, *mu metal*) they can be degaussed without being disassembled. Most current drives have aluminum cases which do not impede the penetration of the degaussing magnetic fields. Lists of degaussers certified by the NSA as Type I or Type II are available.

The list of NSA certified degaussers is included in the NSA's *Information Systems Security Products and Services Catalogue (Degausser Products List)* available through the U.S. Government Printing Office (GPO), Post Office Box 371954, Pittsburgh, PA 15250-7954, as 908-027-00000-1.

7.2 DISK SANITIZATION SOFTWARE

There are several programs available that can sanitize a disk by doing a “government overwrite” of the disk. There are several different “government overwrites” available depending on which government document the programmer has read. Most government overwrites are based on DoD 5220.22-M (Jam., 1995). Note that the list of sanitization methods has been removed from newer versions of DoD 5220.22-M. The DoD overwrite in the 1995 document is to overwrite with a random character, the *complement of that character*, a different random character, and then verify the writing of that last character.

1. Random character.
2. Complement of the random character.

3. Different random character.
4. Verify last overwrite.

This is also the current DOE sanitization requirement. For example, if you choose a hex 00 as the first character, the second must be a hex FF, and the last can be any randomly chosen character.

1. 00 (binary 0000 0000)
2. FF (binary 1111 1111)
3. Random character
4. Verify.

The DoD and DOE overwrite specifications have the same effect on the hard drive in that they overwrite every bit position with a 0, a 1, and finally a random value.

> **Security Tip:** If you need to overwrite a whole disk and don't have the software to do so on the system that was contaminated, move the disk to a system where you do have that capability and do the sanitization there. It does not matter that it is a different operating system as you are going to destroy everything on the disk anyway, including the file system.

7.2.1 Norton Wipe Info and Ghost for Windows Systems

The Wipe Info program is a part of the Norton Utilities package. The current version of Norton's Wipe Info program (version 7) overwrites files or folders with a hex 00, a hex FF, and a character you pick. It then verifies that last overwrite.

1. 00 (binary 0000 0000)
2. FF (binary 1111 1111)
3. Random character you choose.
4. Verify the last write.

This program does not have the capability of wiping a whole disk volume or drive. To wipe a volume or a whole disk on a Windows system you must boot the system with a DOS disk (Windows 95/98/ME) and run the **gdisk.exe** program. **Gdisk.exe** is a partitioning program included in the Norton Ghost package. The Ghost CD itself is bootable and can be used to boot a system into DOS. **Gdisk.exe** is in the **\support** directory on the Norton Ghost CD. In addition to partitioning a disk, it can wipe a disk with the same wiping schemes as Wipe Info.

The default government overwrite with **gdisk.exe** is a seven times overwrite.

1. Character 1
2. Complement of character 1
3. Character 2
4. Complement of character 2
5. Character 3
6. Complement of character 3
7. Random sequence of characters.
8. Verify the last overwrite.

Use the following command to get a list of attached drives and drive numbers.

gdisk

Use this command to get information about a specific drive.

gdisk *drive* **/status**

Here, *drive* is the drive number (1 through 8) of the drive you want information about.

When you have determined which drive needs to be sanitized (be really sure of this) use the following command line to do a government overwrite of a whole drive.

gdisk *disk* **/diskwipe /dod**

Where *disk* is the number (1 – 8) of the fixed disk drive you want to wipe. The **/diskwipe** option tells **gdisk** to wipe the whole drive including all partitions, the partition table, and the master boot record. The **/dod** option makes it do a seven times overwrite using three characters, their complements, and a random sequence. Instead of **/dod**, you can use **/custom:***n* where *n* is the number of overwrites to perform. **/custom:7** is the same as **/dod**. The minimum 3 times overwrite required by DOE is achieved with the command.

gdisk *drive* **/diskwipe /custom:3**

See the ghost manual for the other capabilities and options of **gdisk.exe**.

7.2.2 Norton Wipe Info for Macintosh Systems

The Wipe Info program is a part of the Norton Utilities for Macintosh package. The current version of Norton Utilities for the Macintosh (version 8.0) includes two versions of Wipe Info. One for OS 8 and 9 and one for OS X. The OS X version of Wipe Info uses a character you pick, the character's complement, the character again, and verifies the last write. The default character is AA55 (binary 10100101)

1. Random character you pick.
2. Complement of the random character
3. Random character from step 1.
4. Verify the last write.

The OS 8, 9 version of Wipe Info uses a character you pick, the character's complement, and hex 00.

1. Random character you pick.
2. Complement of the random character
3. Hex 00 (binary 00000000)
4. Verify the last write.

The one you use depends on how you boot your system. Both versions of Wipe Info understand all of the Macintosh file systems so it does not matter which you use. That is, the OS 8,9 version of Wipe Info can wipe OS X disks. The newer Macintosh systems (the

latest G4 systems and the G5 systems) can only be booted into OS X. Slightly older ones can boot either OS 9 or OS X. The Norton Utilities 8.0.2 and later CD contains both OS 9 and OS X systems and can boot both older systems and the newer G4 and G5 systems.

While the Macintosh overwrite is not exactly the same as that required by DOE N-205.9, the effect is essentially the same. The difference is that the last overwrite does not use a randomly chosen character but this does not affect the overwriting.

Both the Macintosh and Windows versions of Norton Utilities include a disk editor program for examining sectors on a disk and searching for text strings. The disk editor is not automatically installed on Windows systems by the Norton Utilities installer but must be installed manually. DISKEDIT.EXE on Windows versions must run in a DOS shell. You must boot your system with a DOS disk (Windows 95/98/ME) and then run DISKEDIT.EXE.

On the Macintosh system, version 8 of the Norton Disk Editor is installed but is not listed in the Norton Launcher window. It is on your disk in Norton Solutions:Norton Utilities:Technical Tools:Norton Disk Editor. Version 7 of the Norton Disk Editor is on the CD in /Norton Utilities Folder/Norton Tools and in /Norton Utilities Folder/Norton Tools/Tech Support Tools. Version 8 of the Norton Disk Editor runs under OS X while you must boot the system into Macintosh OS 9 or earlier to use version 7 of this tool.

The Macintosh Norton Utilities CD is bootable so the Norton Disk Editor can be run from there. Version 8 of the CD will boot either OS 9 or OS X while Version 7 will only boot OS 9.

7.2.3 BCWipe

The current version of BCWipe (version 3) is a commercial package available from the Jetco website,

http://www.jetico.com

It runs on all versions of Windows and a development version runs on most UNIX type systems. The development version has been tested on the following UNIX systems.

- Linux 2.0-2.4
- FreeBSD 3.0-4.6
- OpenBSD 2.8
- Solaris 8
- Digital UNIX 4
- Irix 6.5

BCWipe has two built-in overwrites plus the capability to design your own. The built-in overwrites are a *government overwrite* and a *Gutmann overwrite*. The government overwrite uses three characters and their complements and finally a random sequence of characters for a total of 7 overwrites.

1. 35 (binary 0011 0101)

2. CA (binary 1100 1010)
3. 97 (binary 1001 0111)
4. 68 (binary 0110 1000)
5. AC (binary 1010 1100)
6. 53 (binary 0101 0011)
7. Random sequence
8. Verify the last write.

If you choose to do the government overwrite with fewer than seven passes, BCWipe always does a random sequence of characters as the last pass.

The Gutman overwrite is based on the paper *Secure Deletion of Data from Magnetic and Solid-State Memory*, by Dr. Peter Gutmann. In this paper, Dr. Gutmann is attempting to generate the effects of the alternating field of a degausser by writing specific sequences of characters onto the disk. It consists of four overwrites with random sequences of characters, 27 overwrites with different bit patterns, followed by four more random sequences.

1. Random sequence
2. Random sequence
3. Random sequence
4. Random sequence
5. 55 (binary 0101 0101)
6. AA (binary 1010 1010)
7. 92,49,24 (binary 1001 0010 0100 1001 0010 0100)
8. 49,24,92 (binary 0100 1001 0010 0100 1001 0010)
9. 24,92,49 (binary 0010 0100 1001 0010 0100 1001)
10. 00 (binary 0000 0000)
11. 11 (binary 0001 0001)
12. 22 (binary 0010 0010)
13. 33 (binary 0011 0011)
14. 44 (binary 0100 0100)
15. 55 (binary 0101 0101)
16. 66 (binary 0110 0110)
17. 77 (binary 0111 0111)
18. 88 (binary 1000 1000)
19. 99 (binary 1001 1001)
20. AA (binary 1010 1010)
21. BB (binary 1011 1011)
22. CC (binary 1100 1100)
23. DD (binary 1101 1101)
24. EE (binary 1110 1110)
25. FF (binary 1111 1111)
26. 92, 49, 24 (binary 1001 0010 0100 1001 0010 0100)
27. 49, 24, 92 (binary 0100 1001 0010 0100 1001 0010)
28. 24, 92, 49 (binary 0010 0100 1001 0010 0100 1001)
29. 6D, B6, DB (binary 0110 1101 1011 0110 1101 1011)
30. B6, DB, 6D (binary 1011 0110 1101 1011 0110 1101)

31. DB, 6D, B6 (binary 1101 1011 0110 1101 1011 0110)
32. Random Sequence
33. Random Sequence
34. Random Sequence
35. Random Sequence

Security Tip: If you are using the rule-of-thumb that more is better and plan to use the Gutmann wipe, realize that doing so on a large disk can take overnight or longer. Considering that you might have sit with the machine until it is considered clean, you might not want to go to this level of sanitization. The gain in security beyond three overwrites is minimal.

BCWipe looks different depending on if you are using the Windows or the UNIX version. The Windows version installs as a shell and is available by right clicking on a file or disk. When you right click on a file, the "Delete with wiping" command appears in the drop down menu. If you right click on a disk the item will be "Wipe free space with BCWipe". Both of these commands bring up dialog boxes that allow you to set the options and do the wiping.

To wipe a whole disk drive you must use the BCWipePD.exe program. Because most new versions of Windows prevent direct access to the disk drives you must create a bootable floppy (DOS, Win 95 or Win 98) containing BCWipePD.exe, boot the system with that floppy and then use BCWipePD.exe to wipe the hard drive.

bcwipepd.exe [**i|w|r] [-sdfshpl**]

i Display information about available physical drives:
w Wipe physical drive. One of the options, -d*X* or -f*X* must be used together with the w command to specify what drive is to be wiped.
wSILENT run without generating messages.
r Read sector. The command is useful for verification of the wiping process. The –s*X* and -d*X* or –f*X* options must be used with this command to specify what sector to read.
-d*X* Hard drive number (*X* is a disk number or '*' for all hard drives).
-f*X* Floppy drive number (*X* is a disk number or '*' for all floppy drives).
-s*X* Low 32-bit word of the sector number (*X* is a sector number).
-sh*X* High 32-bit word of the sector number (*X* is a sector number, default is 0).
-p*X* Number of passes (*X* is number of passes, default is 7).
-l*S* Append to log (*S* is a log file name).

The UNIX version of BCWipe is a command line utility. The program is available as rpm files for Linux and as source files for other versions of UNIX. You must first copy the files onto your system and then run **make** while in the BCWipe directory to build the executables. At the moment, this is development code and some of the features do not work.

When the program is ready, use the following command line to wipe files, free space, or whole drives.

bcwipe [**-VvsbBdrifhm**] *filename*

Here, *filename* is the name and path to a file, the name and path to a directory, or the name of a block device.

-h (help) Display help and exit.
-V (version) Display version and exit.
-f (force) Force wipe files with no write permissions. Also suppress interactive mode.
-r (recurse into subdirectories) Remove with wiping the contents of directories recursively.
-i (interactive) Prompt whether to wipe each file.
-I (disable interactive) Never prompt whether to wipe each file.
-v (verbose) Explain what is being done.
-b (block device) Wipe contents of block devices
-md U.S. DoD 5200.28 seven pass extended character rotation wiping.
-mg 35-pass Peter Gutmann's wiping (default).
-m *n* U.S. DoD 5200.28 *n* pass extended character rotation wiping.
-d (do not delete) Do not delete file(s) after wiping.
-S (wipe file slack) Wipe files slack. File slack is the disk space from the end of a file till the end of the last cluster used by that file. Cluster is minimal portion of disk space used by file system.
-s (system random) Use system random. Default is SHA-1 (Secure Hash Algorithm). System random faster but less secure then SHA-1.
-p Use 64Kb random pattern for random passes instead of full random. Much faster (especially on slow CPU) but less secure! (not recommended)

The BCWipe program includes a hex viewer for viewing the contents of files before and after wiping.

7.2.4 Scrub

The scrub code was developed at the Lawrence Livermore National Laboratory for sanitizing UNIX type file systems.

The scrub code is available on the CIAC website at:

http://ciac.llnl.gov/ciac/ToolsUnixGeneral.html#scrub

Download the SCRUB tar file onto a UNIX system, extract all the files, and run **make** while in the scrub source directory. Assuming it compiles, you can run **make install** to install the scrub executable and manual files into normal places but it is safer to leave it in the scrub directory and to run it from there. A linux .rpm file is also available for directly installing in a Linux system.

The scrub code uses four overwrites to clear a file or disk. A hex 00 character, a hex FF character, a hex AA character, a random sequence, and a hex 55 character. The program then checks that the last overwrite was successful.

1. 00 (binary 0000 0000)
2. FF (binary 1111 1111)
3. AA (binary 1010 1010)
4. Random sequence
5. 55 (binary 0101 0101)

The options are:

scrub `[-d] [-q] [-r] [-x|-X]` *file*

Where *file* is a raw special file (for example, **/dev/rdsk/sd0a**) or a regular file name. If a raw special file is used, scrub overwrites the whole drive. If a normal file name is used, scrub overwrites that file.

-r Include random pass (4). This is somewhat compute intensive due to choice of algorithm (MD5) so is disabled by default.
-d Show what will happen without writing anything to the disk or file.
-q Instead of printing a period after every block written, just print a line after each pass is completed.
-x Write one filesystem block beyond the file size. Note that without –x we already round the size up to the nearest filesystem block.
-X Scrub free space. Here, *file* is a dummy filename and path to a location in the file system you want to scrub. Scrub creates that file and keeps appending to it until write fails, i.e. filesystem full or file size limit reached. You may need to do this more than once to completely fill a file system.
-D Try to cleanse the directory entry using the same algorithm. After scrubbing, the file whose directory entry was scrubbed will still be available under a new name consisting of a string of 'U' characters in the root directory. This command does not scrub the file but only its directory entry.

For example, to scrub a single file and include the random sequence overwrite use the command:

scrub -r *filename*

where *filename* is the path and name of the file to be scrubbed. When scrubbing is done, don't forget to delete the file. If you need to delete multiple files you have to do them one at a time or create a batch file with multiple scrub commands in it.

Scrub all free space and include the random pass with the command,

scrub –rX *dummyfilepath*

Where *dummyfilepath* is a path to a dummy file in the files system you want to scrub. Use the **df** command to determine which file systems are on which disks. You may need to

run scrub multiple times with different dummy file names to get all of the free space in the file system. Keep doing it until the **df** command shows the file system to be 100% full. You can then delete the dummy files. Note that the last time scrub runs, it may hang when the file system is full and you will have to use Ctrl-C to end it. Scrub prints dots on the screen as it runs to let you know that it is still alive.

To scrub a whole file system, use the command,

scrub –r *rawdevicefile*

Where *rawdevicefile* is the name of a raw device file such as **/dev/rdsk/c0t0d0s0** which would scrub the root partition on many systems. Use the **df** command to see what partitions are mounted.

UNIX and the scrub program do not contain utilities for viewing and searching the contents of disk sectors. To do so you need a copy of the **unrm** program from The Coroner's Toolkit (TCT) by Dan Farmer and Wietse Venema. The Coroner's Toolkit is available from,

http://www.porcupine.org/forensics/tct.html

The **unrm** program copies raw disk blocks and turns them into files on another disk which can then be grepped through to find the problem text. A caution here is that you have just copied classified info onto another disk so you would need to dedicate a disk to this task and that disk would become a classified disk.

WARNING: Using **unrm** creates a second classified disk if the disk you are examining contains classified data.

7.3 SANITIZATION WITH OVERWRITING (WHOLE DISK)

Sanitization of hard disk drives using overwriting so that the drive can be reused in an unclassified program has special requirements listed in section 4.2. After determining that you have or will comply with the other requirements you can go ahead and sanitize the disk with overwriting.

WARNING: Here you are sanitizing a physical disk drive not a logical drive (disk partition). A physical drive can contain multiple logical drives, all of which are destroyed by this process.

7.3.1 Sanitizing Windows 95/98/ME Disks

You have two choices here, **Gdisk** (part of Norton Ghost) or **BCWipe**.

Using Norton Gdisk

Norton **gdisk.exe** must be run on a DOS partition that is not on the hard drive that is going to be wiped. You can use a bootable floppy, bootable CD, or a DOS partition on a

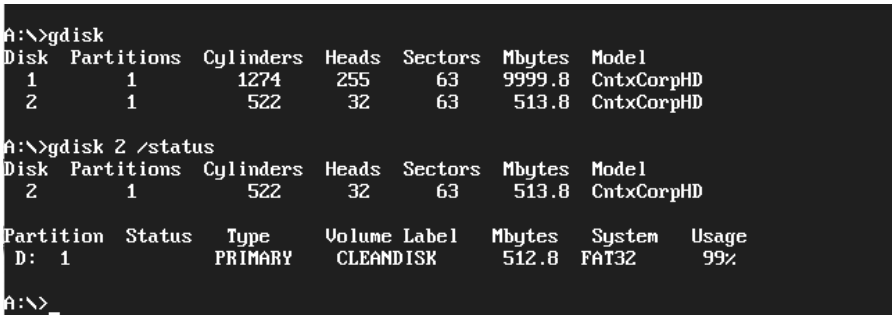
different hard drive from the one you are going to sanitize. The Norton Ghost CD is a bootable CD and can be used to boot the system and run **gdisk**. **Gdisk** is in the **\support** directory of the Ghost CD. The instructions here are for using a bootable floppy. Instructions for a bootable CD or hard disk partition are largely the same except that you may need to **cd** to the directory that contains **gdisk** and **diskedit** before running them.

1. Create a bootable floppy for the system.

2. Copy **gdisk.exe** and **diskedit.exe** onto the floppy.

3. Boot the system with the floppy.

4. Figure out the hard disk number for the disk you want to wipe. Use **gdisk** with no options to get a list of the drives and with a drive number and the **/status** option to get more information about a single drive.



   Save the information for the disk you plan to sanitize to use while repartitioning and formatting the drive.

5. Assuming you want to sanitize the second physical disk, run **gdisk** with the following command line.

   gdisk 2 /diskwipe /dod

   or to overwrite three times,

   gdisk 2 /diskwipe /custom:3

   Change the drive number to sanitize a different drive.

6. When **gdisk** completes, run **diskedit** and examine several random sectors on the disk to make sure that **gdisk** sanitized the whole drive. The whole volume should be filled with random hex characters.

This disk is now sanitized and must be repartitioned and formatted before it can be used. The **gdisk** program can be used to partition and format the drive for use in a windows system as **gdisk** has the capabilities of **fdisk** and **format**. For example, the following command partitions the drive into a single, primary partition, formats the partition, and labels the partition CLEANDISK.

gdisk /cre /pri /sz:100% /for /v:cleandisk

```
E:\SUPPORT>gdisk 2 /cre /pri /sz:100% /for /v:cleandisk
Checking existing disk format.
Verifying 512.83M
Format complete.

Volume label is CLEANDISK

  536,674,304 bytes total disk space
  536,670,208 bytes available on disk

        4,096 bytes in each allocation unit
      131,024 total allocation units on disk
      131,023 available allocation units on disk

Volume Serial Number is 3B11-17FA

Partition  Status   Type     Volume Label   Mbytes   System   Usage
 D:  1  *CREATED*  PRIMARY    CLEANDISK      512.8  FAT32      99%

E:\SUPPORT>_
```

Don't forget to mark the disk drive and the outside of the computer with labels that indicate the drive formerly contained classified information and that it must be destroyed before leaving the controlled area.

Using BCWipe

To sanitize a whole drive, **BCWipe** must be setup in much the same way as **gdisk**. **BCWipe** must be run from a bootable DOS partition that is not on the drive that is going to be wiped. You can use a bootable floppy, bootable CD, or a DOS partition on a different hard drive from the one you are going to sanitize. The instructions here are for using a bootable floppy. Instructions for a bootable CD or hard disk partition are largely the same except that you may need to **cd** to the directory that contains **bcwipepd** before running them.

1. Create a bootable floppy for the system.

2. Copy **bcwipepd.exe** onto the floppy.

3. Boot the system with the floppy.

4. Figure out the hard disk number for the disk you want to wipe. You can use the **bcwipepd** program to help you. To see information about the attached disk drives use the following command (note that the **i** is a command not an option)

bcwipepd.exe i

```
A:\BCWIPEPD>bcwipepd i
 BCWipePD i
Removable drive 0 1440 KB:
 sector size 512,
 total sectors 2880 - B40(hex)
Procedure -> getPDriveInfo
Phys drive 1: Heads 0, sectors 0
Fixed hard drive 0 9999.7 MB:
 sector size 512,
 total sectors 20479536 - 1387E30(hex)
Fixed hard drive 1 513.8 MB:
 sector size 512,
 total sectors 1052352 - 100EC0(hex)

A:\BCWIPEPD>
```

5. Assuming you want to sanitize the second physical disk, run **bcwipepd** with the following command line.

   bcwipepd w –d1 –lwipe.log

   The **–d** switch selects the physical hard drive to sanitize where **0** is the first drive, **1** is the second, and so on. The **–l** switch followed by a file name creates a log file. The default is to do the seven times overwrite. To overwrite more or fewer times set the number of times with a **–p** switch followed by the number of times to overwrite the drive.

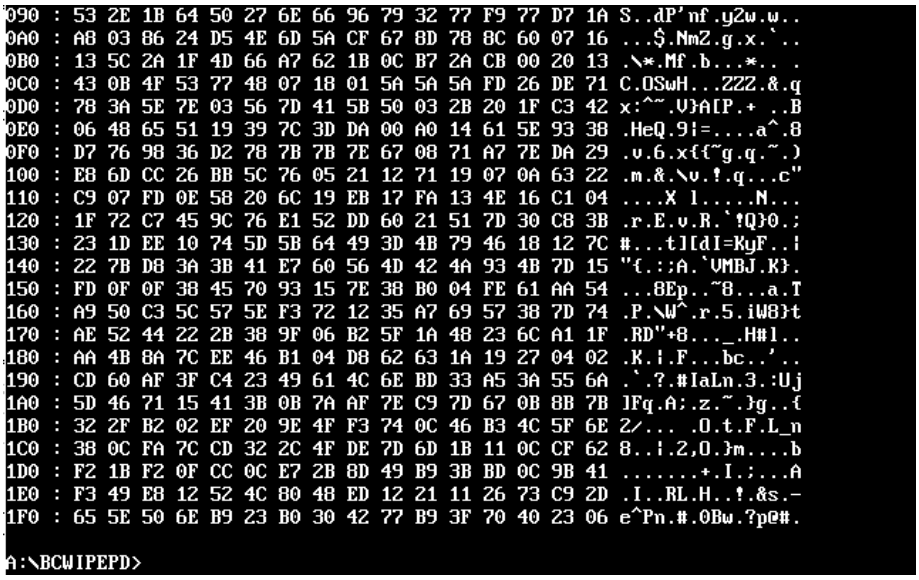
```
A:\BCWIPEPD>bcwipepd w -d1 -lwipe.log

Fixed hard drive 1:
 Size           - 513.8 MB
 Total sectors  - 1052352 - 100EC0(hex)
 Sector size    - 512

The drive will be wiped ( pass quantity - 7 ).
All data on the drive will be lost!

Approximate time is 9 min
|  99% doneiping process [N]? - y
A:\BCWIPEPD>
```

6. When **bcwipepd** completes, examine the log file for any problems.

7. Run **bcwipepd** again with the following command line.

   bcwipepd.exe r –d1 –s0

   This line prints out sector 0 on the second disk (1) so you can see that it has been wiped appropriately. Do this for several random sectors to assure yourself that bcwipepd worked. The sectors should contain the last character used to overwrite the drive, which is random characters if the standard DoD wipe was used.



This disk is now sanitized and must be repartitioned and formatted with **fdisk** and **format** before it can be used. Don't forget to mark the disk drive and the outside of the computer with labels that indicate the drive formerly contained classified information and that it must be destroyed before leaving the controlled area.

7.3.2 Sanitizing Windows NT/2000/XP Disks

Windows NT/2000/XP disks are sanitized in exactly the same way as Windows 95/98/ME. As the wiping program is run from a DOS boot disk, the type of file system on the disk being wiped does not matter as everything is being destroyed.

7.3.3 Sanitizing Macintosh Disks

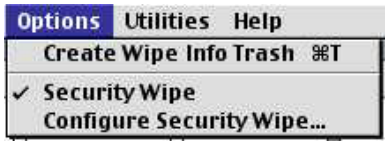
Macintosh disks are sanitized using Norton Wipe Info and examined using the Norton Disk Editor +. Norton Wipe Info and Disk Editor + do not run under OS X so you must reboot your system in OS 9 or earlier. You also cannot wipe the boot disk so make sure you boot from a disk other than the one you want to sanitize. As an alternative, you can boot the Norton Utilities CD.

1. Boot the Norton CD or boot an OS 9 or earlier disk that is not the disk that needs to be wiped.

2. If you booted from a different disk, copy **Wipe Info**, Disk **Editor +,** and **Norton Shared Lib** onto your boot disk. If you need it, the manual for **Disk Editor +** is on the CD in the **Norton Disk Editor.PDF** file in the **Tech Support Tools** directory.

3. Double click on **Wipe Info** and the Wipe Info dialog box appears.

4. Check **Security Wipe** on the Options menu. This turns on the three times overwrite described in section 7.2.1.



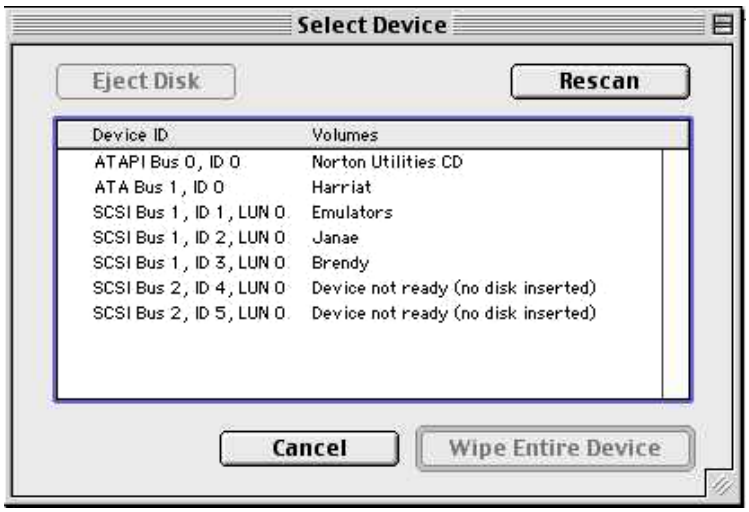
5. You can change the character pattern used to overwrite the disk by choosing the Options, Configure Security Wipe command and setting the characters in the dialog box. The default value of hex AA55 gives a repeated binary bit pattern of 1010 1010 0101 0101 as the first pass and the complement (55AA) as the second. The last pass is all zeroes. This is a reasonably good choice but to add some randomness to the patterns you could change it, for example,

FF00	(binary 1111 1111 0000 0000)
924924	(binary 1001 0010 0100 1001 0010 0100)
66	(binary 0110 0110)
CC	(binary 1100 1100)
6DB6DB	(binary 0110 1101 1011 0110 1101 1011)

6. The Wipe Disk option button on the Wipe Info dialog box only wipes a single partition on a disk. It does not wipe the whole disk. To wipe the whole disk, including all partitions on the disk, the disk driver, and the partition table, choose the Wipe, Wipe Entire Device command.

7. The Select Device dialog box appears and lists all available physical devices connected to this system. Choose the device to wipe and click Wipe Entire

Device. Click Wipe in the dialog box that asks you if you really want to do this.



When this completes, the drive has been wiped three times with three different patterns. However, the last pattern is not a randomly chosen character as specified in 205.9 (Appendix A). Wiping the drive a second time using a different, pattern for the first wipe satisfies this requirement.

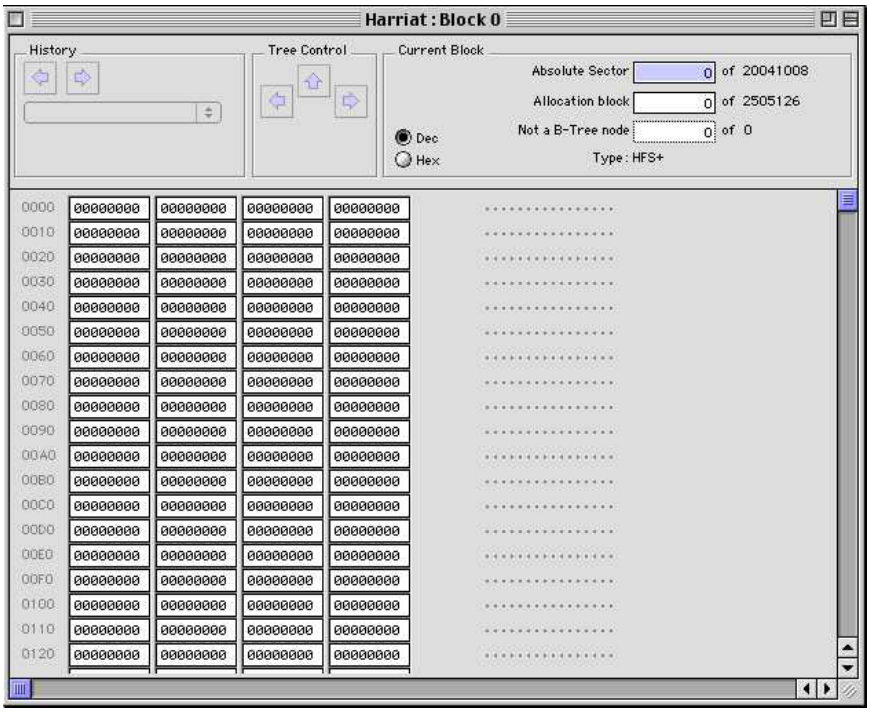
8. When Wipe Device completes, choose the **Options, Configure Security Wipe** command. In hex mode, type a different pattern for the first wipe. Remember that hex characters consist of pairs of numbers and the letters A through F.

9. Choose the Wipe, Wipe Entire Device command, select the drive and Wipe the device a second time.

10. When the Wipe command completes quit Wipe Info.

The drive has now been wiped six times with two different patterns, the two complements of those patterns, and twice with zeroes. This is more wiping than required in 205.9 (Appendix A) and makes up for the fact that Wipe Info cannot do a randomly chosen character as the last wipe.

11. Start the **Norton Disk Editor +** and the Disk Editor Window appears. The window should show all zeroes as shown here because the last overwrite uses 00 as the pattern. Check several sectors on the drive using the slider at the bottom of the window to make sure Wipe Info has cleared the whole drive.



12. Quit the Disk Editor

Your disk is now completely wiped and must be initialized before it can be used. Don't forget to mark the disk drive and the outside of the computer with labels that indicate the drive formerly contained classified information and that it must be destroyed before leaving the protected area.

7.3.4 Sanitizing UNIX Disks

There are two options for sanitizing disks on UNIX systems, the UNIX version of BCWipe and the Scrub code. Because the UNIX version of BCWipe is still in development, it is not yet ready for production work. Both of these solutions are available as Linux RPM files or as source code so they can be compiled on individual systems.

For Linux installations running on PC hardware you can use the same solution as for Windows disks (see section 7.3.1 Sanitizing Windows 95/98/ME Disks) if that is more convenient. You are going to be booting from a floppy and you are wiping the whole disk so the sanitizing software does not need to know anything about the file system on that disk.

Using BCWipe

Not yet available for production work.

Using Scrub

To use the Scrub code, copy it onto your system and install it. If you have a Linux system, download the rpm version. If you have a different version of UNIX, download the source file archive. The rpm version of scrub can be installed directly on a linux system using the **rpm** program. The source file version must first be unpacked using **gunzip** and **tar**, and then compiled by running **make**. If the compilation completes successfully, you will have a **scrub** executable in the source file directory. Note that **scrub** must not be on the disk you are planning to sanitize.

Scrub sanitizes a disk by wiping a raw device file. Make sure you are wiping the correct partition of the raw device file to insure that you are getting the correct disk. Look in the **/dev** or **/dev/rdsk** directory and find the list of raw special files. Raw special file names will be things like **c0t0d0s0** or **sd0a** depending on the system. In both cases, the rightmost character is the partition number on a disk. That is, **c0t0d0s0** and **c0t0d0s1** are two partitions on the same disk as are **sd0a** and **sd0b**. The partitions **c0t0d1s0** and **c0t0d2s0** are partitions on two different disks as are **sd1a** and **sd2a**. Not all raw special files are connected to actual disk partitions but are there in case you add a disk or partition to your system.

On Linux systems disks are named,

- hda, hdb, hdc, … – for IDE disks
- sda, sdb, sdc, … – for SCSI disks
- eda, edb, edc, … – for ESDI disks
- rd or ida, idb, … – for RAID disks.

Followed by numbers for the partitions on an individual disk. That is, **/dev/hda** is the raw device file for the entire first disk and **/dev/hda1** is the first partition on that disk.

On Solaris systems you can run the **format** command to see the partitions defined on each disk. Be careful when you run **format** as you can change things on your disk and damage your system. Run the **format** command and choose the disk to display from the list you are given. Type the **partition** command and then the **print** command to see the partition table of the selected drive, which should be like the following.

```
partition> print
Current partition table (original):
Total disk cylinders available: 29649 + 2 (reserved cylinders)

Part      Tag    Flag     Cylinders         Size            Blocks
  0       root    wm       0 -  6095        2.93GB    (6096/0/0)   6144768
  1       swap    wu    6096 -  8176        1.00GB    (2081/0/0)   2097648
  2     backup    wm       0 - 29648       14.25GB    (29649/0/0) 29886192
  3 unassigned    wm       0                0         (0/0/0)            0
  4 unassigned    wm       0                0         (0/0/0)            0
  5 unassigned    wm       0                0         (0/0/0)            0
  6 unassigned    wm       0                0         (0/0/0)            0
  7       home    wm    8177 - 29648       10.32GB    (21472/0/0) 21643776
```

Type **quit** twice to end **format**. Here you can see that the disk, **c0t0d0**, contains 4 defined partitions out of the 8 possible. The raw special file for partition 0 is **/dev/rdsk/c0t0d0s0** and is the root partition. The partition number is the number that follows the s in the raw device file name. From the table, you can see that this partition does not comprise the whole disk but only cylinders 0 through 6095. The disk also

contains swap (cylinders 6096 through 8176) and home (cylinders 8177 through 29648) partitions that take up the remaining disk cylinders. Wiping any of these partitions only wipes that partition and not the whole disk. Note here partition 2, the backup partition, contains all the cylinders in the drive. By wiping the backup partition, you wipe the whole drive. The raw special file for this backup partition is **/dev/rdsk/c0t0d0s2**. This is the raw special file you would want to run scrub on to wipe this entire disk.

Be sure to write down this partition information if you want to repartition the drive in the same way when you are done sanitizing it.

To scrub this partition you would run the following command.

scrub –r /dev/rdsk/c0t0d0s2

When scrub completes you will have to reformat this disk to divide it into partitions and to put a file system on the partitions. Don't forget to mark the disk drive and the outside of the computer with labels that indicate the drive formerly contained classified information and that it must be destroyed before leaving the protected area.

On Linux systems, run the **fdisk** utility to list the current partitions. As with **format**, be careful what you do with **fdisk** as you can damage a system with it. Run the **fdisk** command followed by the name of the device file you want to examine. For example, to examine the second IDE disk type,

fdisk /dev/hdb

type the **p** command to print the current partition table. The **p** command lists all the partitions on the disk and their names. Type the **q** command to quit **fdisk**.

Again, be sure to save this partition information if you want to repartition the disk in the same way after you sanitize it.

To scrub this disk run the following command.

scrub –r /dev/hdb

When scrub completes you will have to re partition and reformat this disk to divide it into partitions and to put a file system on the partitions. As before, don't forget to mark the disk drive and the outside of the computer with labels that indicate the drive formerly contained classified information and that it must be destroyed before leaving the protected area.

7.4 SANITIZING AN UNCLASSIFIED DISK CONTAINING A SMALL AMOUNT OF CLASSIFIED DATA

The special rules listed in section 4.3 allow you to sanitize a disk used in an unclassified program that contains a small amount of classified information and be able to continue using that disk in the unclassified program. Before doing this, you must be sure your

system comes under the rules listed in 4.3 and in DOE 205.9 (Appendix A). If the amount of classified information on the drive exceeds that allowed you cannot use this procedure.

> **Security Tip:** The amount of classified information does not necessarily equal the size of the file that contains it. Do not use the file size when figuring adherence to the clarification memorandum. Use the actual size of the classified information. You should also keep in mind that there may be multiple copies of the classified information on the drive and that it is the total size of all of these copies that must be used to determine adherence to the memorandum.

The first step in all cases is to not delete the file that contains the classified information. It is much easier to locate and sanitize a drive if the problem data is localized in a file. If you delete the file, the sectors in the file become available for other programs to use and may become part of another file and be difficult or impossible to find.

The basic procedure is

1. Disconnect the system from any computer network.
2. Find all copies of the problem data
3. Do a DOE overwrite of the files that contain the classified data
4. Delete those files
5. Do a DOE overwrite of swap space
6. Empty the trash and do a DOE overwrite of all free space
7. Search for the problem data again

The overwrite of swap space is to get any copies of the file that might have been swapped to disk. The wipe of free space is to get any copies of the data that might have been saved in deleted files. The last search is to make sure you have gotten all known copies of the problem data.

The biggest difficulty here is in determining the location of all copies of the problem information. If a file containing the problem information has been deleted and overwritten by another file, it will be impossible to satisfy the DOE requirements without sanitizing the whole drive so it is very important to make the user stop using their system for anything as soon as you know it has a small amount of problem information on it. If it is likely that copies of the problem information have been deleted and overwritten by other files, the sanitization procedure is changed to the following,

1. Disconnect the system from any computer network.
2. Find all copies of the classified data.

3. Determine that some have been overwritten and therefore their location is unknown.

4. Do a DOE overwrite of the known copies of the classified data.

5. Delete those files.

6. Do a DOE overwrite of swap space.

7. Empty the trash and do a DOE overwrite of all free space.

8. Search for the classified data.

9. Copy all files to a different disk.

10. Sanitize the problem disk.

11. Copy all files back.

12. Search for the classified data.

Sanitizing and deleting the files containing the problem text before copying those files to another disk is to insure that you are not copying the problem text onto the new disk and than back to the problem disk. Sanitizing the whole disk assures you that you have done the required number of overwrites of the problem data wherever it may have been on the disk. The last search is just to make sure that the problem data has not been missed in the process.

Another problem is for problem data that arrives in e-mail messages. Depending on your e-mail reader, the problem data may end up in several different files on the disk. E-mail is stored in mail files which are sequential e-mail messages packed end to end in a single file. When you move a message to a different mail file or delete a message, your mailer does not really remove the message from the mail file but only deletes its name from the index. The message is not really removed from the mail file until you compress or compact your mailboxes.

Compacting mailboxes may be manually initiated or it may be automatic. Because of this, you need to immediately kill your mail program as soon as you determine that a message contains classified information. I don't mean shut down the mail program but actually kill it with the task manager. You do not want to take the chance that the mail program will clean up your mailboxes for you and empty the trash.

Another problem with mail messages is with attachments. If the classified information is in an attachment, it can be written several places depending on what e-mail reader you use. If you use Eudora, the attachment is extracted from the e-mail message and a temporary copy is placed in <mailfiles>\spool\<account name> where <mail files> is the location of your mail files (the default is \Program Files\Qualcomm\Eudora) and <account name> is the name of the user account the mail is coming in under. After the

attachment is saved into the spool directory, it is unpacked and saved in the <mail files>\attach directory or to wherever you have designated attachments to go in the preferences. Thus, you already have one deleted copy of the problem file on the disk in addition to the copy in the attach directory. The copy in the spool directory is in whatever format the attachment was in when it was attached to the e-mail message. Normally this will be text for a text attachment or base64 for everything else.

> **Security Note:** Base64 is a conversion of a binary file into a 64 character printable format so that it can be attached to an e-mail message. The format is not readable but can easily be converted back to the original format.

If you use Outlook Express as your mail reader, the incoming mail is directly attached to the in box mail file, including the attachment. The attachment is not extracted from the file unless you tell it to. If you open the attachment without saving it, it is extracted into the temp directory (can be a lot of different places) and is opened from there.

The following sections describe how to do the different tasks necessary to clean a small amount of classified information off of an unclassified disk.

7.4.1 Immediately Stop What You Are Doing

If you think your system contains classified information, immediately stop what you are doing. I don't mean stop when you are done or stop when it is time to go home, I mean right now. No matter how badly you want to send just one more e-mail or type just a few more lines into a document, pull your hands off the keyboard (that includes the mouse) and put them in your lap. Simply quitting an application, saving a file, or typing a few more words could significantly increase the amount of work necessary to clean your system or could even cost you your hard drive.

7.4.2 Disconnect The System From The Network

Pull the system's network connection by removing the network cable from the computer. In most cases, this is an Ethernet cable but could be different, depending on how you connect to the Internet. If you are using a modem to dial-in to the network, turn off the modem or pull its plug.

7.4.3 Log What You Know

Presumably, the suspect information is sitting in front of you because you just noticed it. If it is visible, you can scroll through it to confirm it is classified. Do not close the application where it is displayed. If it is in a closed file, don't open it. On a piece of paper, write down where the classified information is as best you can. Include everything you know about its location. Is it in an e-mail message, attachment, or a file? What is the file name? Where is the file located (attachment or separate file)? If you need to look at a directory, open a command Window (terminal window on a Macintosh or Unix system) and look for the file using typed commands. Do not touch word processors, e-mail programs, web borwsers, file explorer, or finder windows. Don't try to print the

information as you will just create more copies on your machine and possibly on your print spooler and printer as well.

7.4.4 Determine If the Information Is Classified

If the information is visible, get a derivative classifier or other knowledgeable/authorized person to take a look and make a determination. Again, you can scroll the window but do not close the file or quit the application. If the knowledgeable person determines that it is not classified, you are done; go back to work. On the other hand, if the information is classified you need to go on to the next steps.

7.4.5 Shutting Down the System

It is likely at this point that you will want to shut the machine down and store it somewhere safe. Do not quit your applications. Do not do a normal shutdown. It would be safest from a contamination point of view to simply pull the plug. First check the disk light and listen to make sure the hard disk is not being accessed. If it is not being accessed, quickly pull the plug to shut down the system.

If you cannot pull the plug, kill, don't quit, the running applications. On a Windows system, press Ctrl-Alt-Del to open the task manager and kill all the applications from there, then do a shutdown.

In a Macintosh OS-X or Unix system, open a terminal window, and use the ps command to get the process ID numbers of your running applications. You only need the IDs of the foreground applications such as word processors and mail readers. Use the command

```
kill -9 <pid>
```

to kill the processes where <pid> is the process ID. Then do a normal shutdown.

On a Macintosh OS 9 and earlier system select an application and press Cmd-Option-Esc to kill it (don't kill the finder). After all applications have been killed, do a shutdown.

7.4.6 Determine Where the Classified Information Came From and Where it is

Using the information gathered in the last step, try to figure out where the classified information came from and where it is likely to be on your disk. Do not startup your system and look around yet. It is important to know if the classified information is in a single file that you copied, downloaded, or typed onto your system, or in an e-mail message or an e-mail attachment.

If the information is in a file you have typed, or downloaded onto your system, have you opened it in an editor? What editor did you use? How many times have you edited it?

If the information is in an e-mail message, what e-mail reader do you use? Is the classified information in the body of the e-mail or in an attachment? Do you have filters that would automatically move the e-mail to a different mail file? If it is in the

attachment, have you opened it? What did you open it with? How many times did you open it?

From the discussion in part 4, estimate the number of copies of the classified information that are on your system and where they are likely to be. Estimate how much classified information is on your system in bytes. Assume a double spaced printed page is 1250 bytes of text.

7.4.7 Locate All Copies of the Classified Information

Boot the system with a floppy or CD containing a low level sector search/editor program. Different editors are available for different systems. Use the search capability to search the disk for the classified information. Make a list of the sectors that contain classified information. List the file names that contain the sectors if the sector editor gives them. Determine how many bytes of classified information is on a system assuming a full sector contains 500 bytes. See *8.1 Finding the Information*.

7.4.8 How Much Classified Information Is There?

Using your estimates from the last two sections, determine the total number of bytes of classified information that is on the drive. Is it less than 0.01% of the drive's capacity? If it is more than 0.01%, stop here, you are done and your drive is now a classified drive and must be protected as such.

Compare your estimate of the number of copies of the classified information that is on the drive with the number of copies you actually found. Keeping in mind that your estimate is only an estimate, do you think you found all the copies of the classified information that is on the system or do you think some copies may have been deleted and overwritten by other files?

If you think you have found all the copies, you can sanitize this drive by sanitizing the copies you have found. Go to *8.2 Sanitizing Individual Files on a System*.

On the other hand, if you think some copies may have been deleted and overwritten, you will need to copy your data off the drive, sanitize the whole drive, and then copy the data back. Go to *8.3 Sanitizing the whole drive and Putting the Files Back*.

8 METHODS FOR FINDING AND SANITIZING SMALL AMOUNTS OF DATA

The following sections contain methods for performing the tasks outlined in part 7.

8.1 FINDING THE INFORMATION

Figuring out where classified information is on a disk involves searching all the sectors on the drive for the information. Before you can search your drive for the problem information, you need a unique string to search for. Hopefully, you have a printed copy of the problem information that you can use to determine what to search for. Note that the

string does not need to be classified, it just must be unique enough to locate the problem files.

> **Note:** Keep in mind that some files now store text as Unicode instead of ASCII characters. Unicode characters are two bytes in size instead of one like ASCII to handle the larger, Asian character sets. For normal text (Arabic letters and numbers), the second byte is always 0 so in a hex editor the text will look s p a c e d o u t.

> **Security Tip:** When choosing some unique text to search for, try to choose some that is unclassified so the act of searching for the text does not create more copies on the disk and so that your notes are not classified.

If you don't have a printed copy of the file to work from or a copy on a classified workstation you can look at, you will need to look at the known file to find a string to look for. If at all possible, do not start up the normal operating system to look for the file as doing so may overwrite some of the copies. Especially don't use an editor like Microsoft Word to look for the file as it will create even more copies of the problem text on your system.

The best way is to boot the system into a single user mode such as DOS and use a disk editor such as the Norton Disk Editor to look at the contents of the file. The tools and methods used here for searching for the text are the same as would be used to look at the contents of a single file.

8.1.1 Searching for Text on a Windows 95/98/ME System

Windows 95/98/ME systems generally use the FAT file system to store data on a disk. If you use a disk editor that understands the FAT file system, you will be able to determine which file the Classified text resides in.

If your editor does not understand the FAT file system, you will still be able to search for and find the problem data but will only know what sector the data resides in, now which file owns that sector. You will also not be able to look at the contents of a specific file.

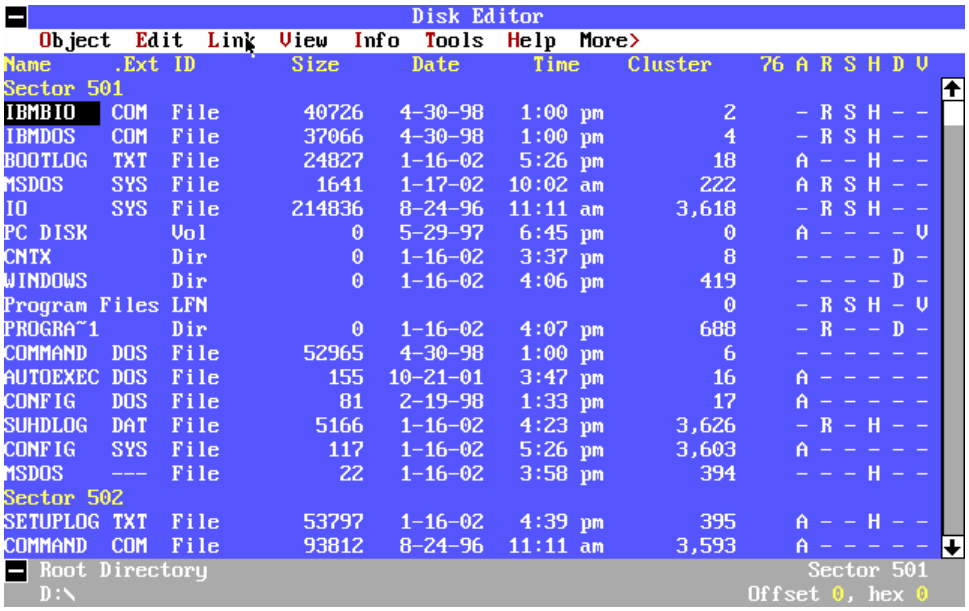
Some disk editors listed here are the Norton Disk Editor included with Norton Utilities and the DIBS-MYCROFT search engine.

8.1.1.1 Viewing a File with the Norton Disk Editor

The Norton Disk Editor understands the FAT file system and can be used to view the contents of files and to search by sectors for specific text. The current version does not understand Unicode so you will need to either know if your text is Unicode or not or search twice, once for the Ascii version and a second time for the Unicode version.

1. Boot your Norton floppy or CD and use cd to change to the Norton Utilities directory. This will usually be C:\Program Files\Norton Utilities or C:\Program Files\Norton System Works\Norton Utilities.

2. Run diskedit.exe. The following image shows the root directory of the startup drive.



3. Use the Object, Drive command to select the disk drive containing the problem data. You can use the mouse or press Alt and the colored letter in the menu name.

4. Double click the directory names in the window to move to the directory containing the problem file or scroll down to the directory name with the arrow keys and press Enter. Double click the problem file name or scroll down to it and press Enter.

5. Scroll through the file until you find some unique text near the problem text. Write it down exactly as it is written in the file.

8.1.1.2 Searching with the Norton Disk Editor

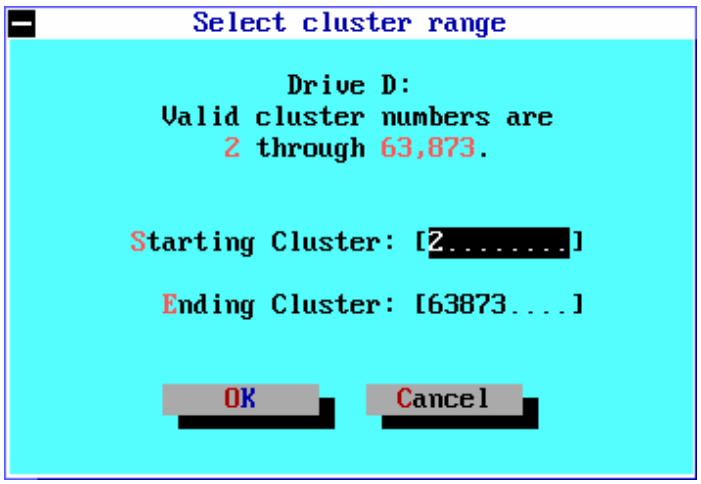
In addition to viewing a file, the Norton Disk Editor can search raw sectors for strings of text. For the case of a FAT file system, the Norton Disk Editor can also tell you which file the found text resides in. This is not the case for an NTFS or Linux file system.

1. Boot from your Norton floppy or CD and start Norton Disk Edit.

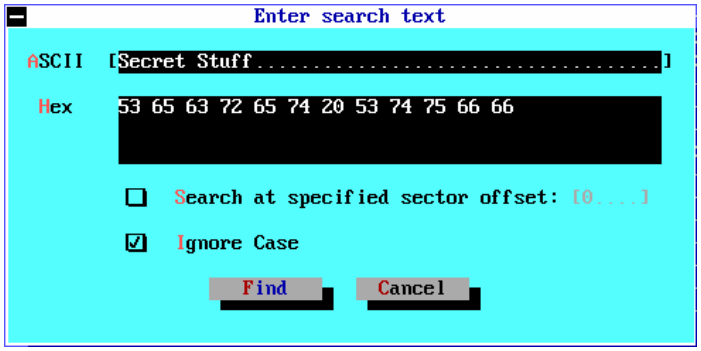
2. Use the Object, Drive command to select the disk drive containing the problem data. You can use the mouse or press Alt and the colored letter in the menu name.

3. Choose the Object, Cluster command.

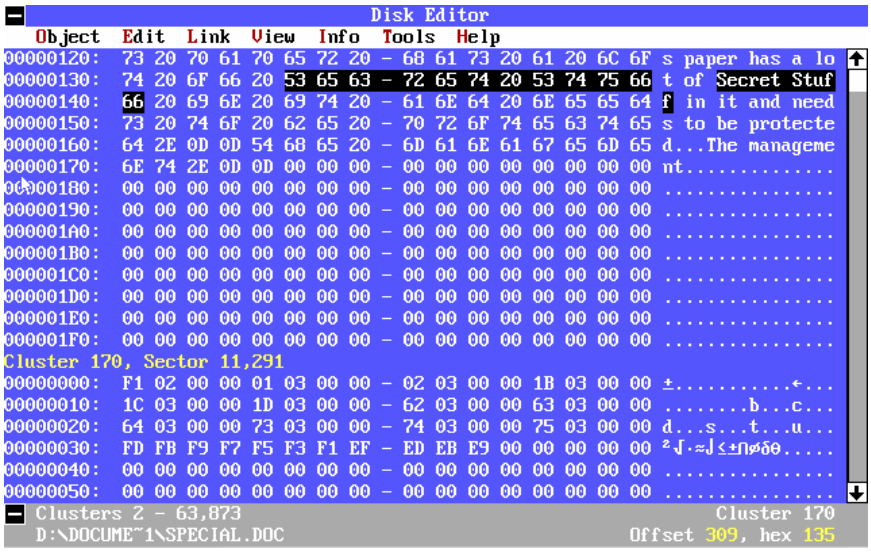
4. In the dialog box select clusters 2 through the end of the disk and click OK.



5. Choose the Tools, Find command and type the unique text into the text box. To search for Unicode text, type the Ascii text first, switch to the Hex window and insert a 00 after each character code. For example, the hex codes for Secret are 53 65 63 72 65 74. In Unicode that would be 53 00 65 00 63 00 72 00 65 00 74 00. Click Find.



6. When Disk Edit finds the text, it displays the contents of the sector it found the text in. Examine the contents of the sector to insure that it is part of the problem data. Write down the cluster number and the name of the file the cluster was found in (See the bottom of the screen). If no file is listed, the data is in the free space and the file that contained it was deleted.



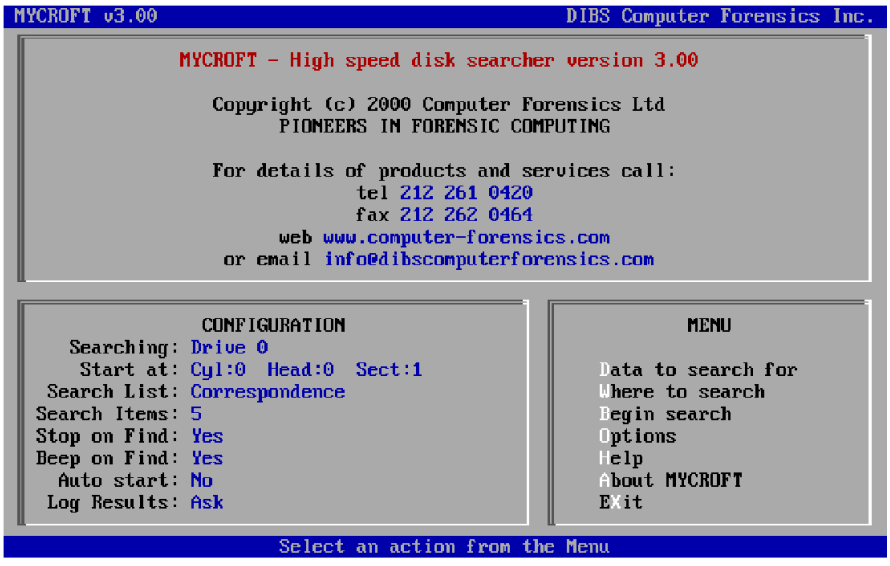
7. Choose Tools, Find Again to search for another copy. Continue this until you have a list of all the locations of the problem data and the files that contain it.

8. Quit Disk Editor

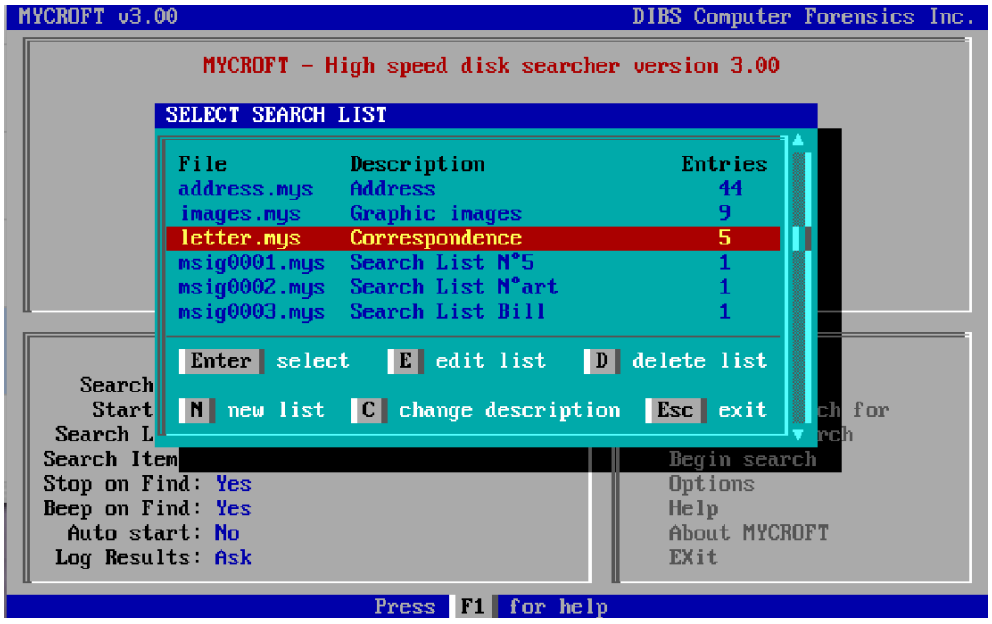
8.1.1.3 Searching with DIBS-MYCROFT

DIBS-MYCROFT is a very fast sector search engine. It does not know about file systems so it cannot tell you what file contains some information, only which sector on the disk contains it. Its usefulness is determined by its speed and the fact that it can search for multiple (up to 460) strings at the same time. It also locates both ASCII and Unicode versions of the string.

1. Boot the Mycroft floppy and the Mycroft window appears.

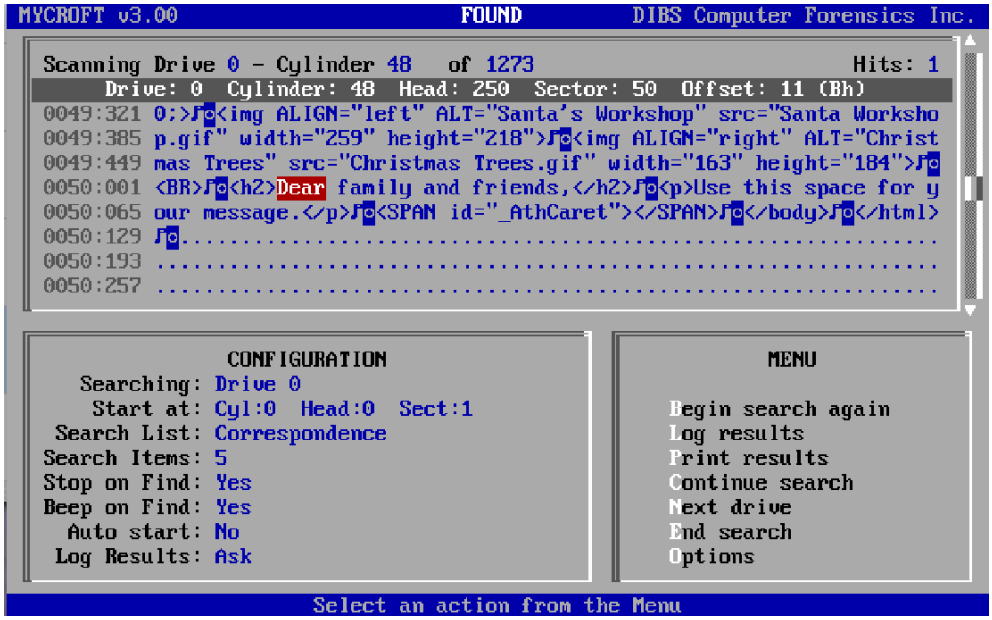


2. Press D to choose the data to search for. In the window that appears, you can choose an existing list or create your own. Choose the list to use and press Enter.



3. Use W to choose the drive to search.

4. Press B to begin the search. When Mycroft finds a match it displays it in the upper window along with the location.



5. Examine the contents of the sector to insure that it is part of the problem data. Write down the cylinder, head, and sector number for the located text and the text found if you are searching for more than one string.

6. Press c to continue searching.

7. Continue searching and writing down the location until you reach the end of the disk.

8. Press e to end the search and x to quit.

At this point you know what sector the problem data is in and know if it is Unicode or not but not the file or cluster. If this is a FAT file system you can go back to a program like the Norton Disk Editor to find the actual file the data is in.

8.1.2 Searching for Text on a Windows NT/2000/XP System

Searching for text on a Windows NT/2000/XP system is complicated by the fact that the file system is probably NTFS. You can use the Norton Disk Editor or DIBS-Mycroft to search for the classified information on a sector by sector basis but there is no easy way to determine what file owns the particular sector. The only sector editor that understands ntfs is DiskProbe but even it cannot give you the file a sector belongs to. It is also very slow compared to the Norton Disk Editor or DIBS-Mycroft.

The general procedure here is to use DiskProbe to look at a known classified file to get the text to search for and then use the Norton Disk Editor or DIBS-Mycroft to determine how many copies are on the system. You can then use DiskProbe again to look at suspect files to try and figure out what files contain the classified information.

8.1.2.1 Viewing a File with Microsoft Disk Probe

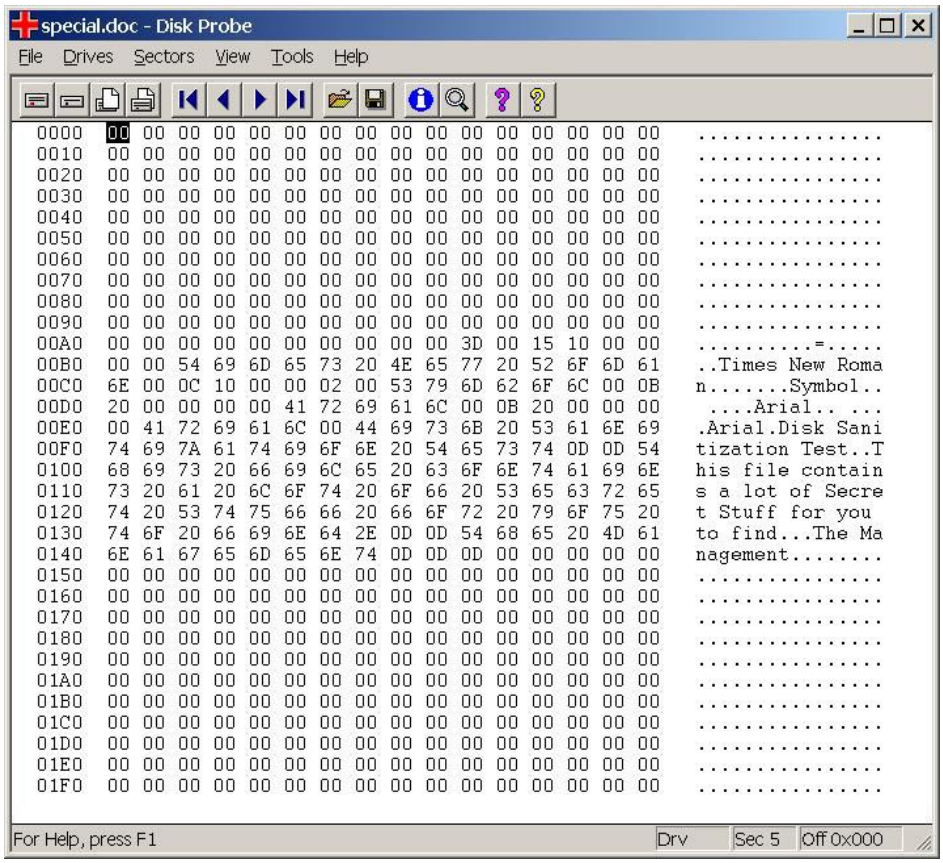
Microsoft Disk Probe is part of the Support Tools for Windows on the Windows installation CD and understands the NTFS file system. If it does not already reside on the problem system, do not install it. Run a copy on a floppy disk or CD.

1. Boot your Windows system into Safe Mode by pressing F8 during startup and selecting Safe Mode. We use safe mode to prevent the network from connecting and to prevent startup programs from running, which might write files on the disk.

2. Run Disk Probe.

3. Choose the File, Open command and open the file containing the problem data. Disk Probe opens to the first sector of the file.

4. Scroll through the file until you find some unique text near the problem text. Write it down exactly as it is written in the file.



8.1.2.2 Searching With Norton Disk Editor

See section 8.1.1.2 Searching with the Norton Disk Editor.

8.1.2.3 Searching with DIBS-MYCROFT

See section 8.1.1.3 Searching with DIBS-MYCROFT.

8.1.2.4 Searching with Microsoft Disk Probe

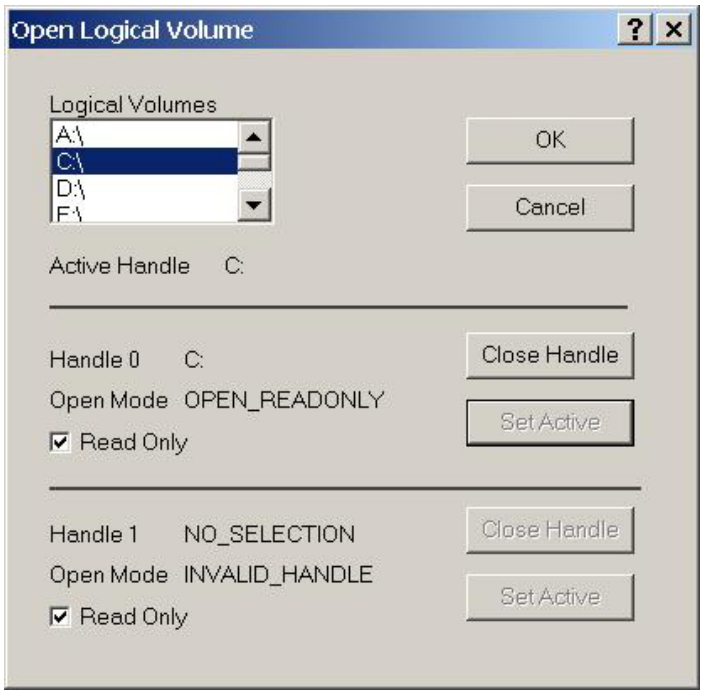
As mentioned previously, searching with Microsoft Disk Probe is very slow but it does run within Windows and it does understand the NTFS file system. Unfortunately, given a sector on a drive, it cannot tell you what file that sector belongs to.

1. Boot your Windows system into Safe Mode by pressing F8 during startup and selecting Safe Mode.

2. Run Disk Probe.

3. Choose the Drives, Logical Volumes command.

4. In the dialog box double click the drive containing problem text and click the Set Active button to make this volume active. Click OK

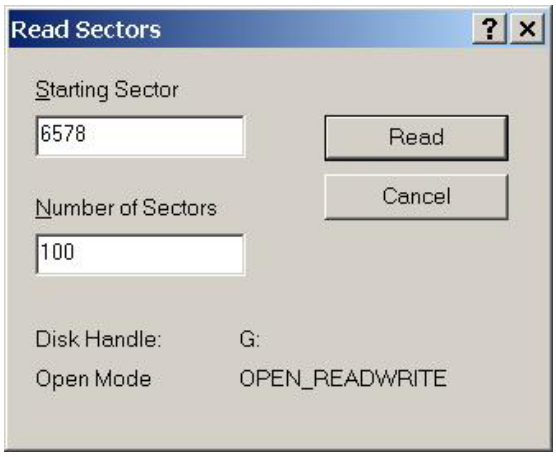


5. Choose the Tools, Search Sectors command. The default setting is to search all sectors in the drive. Set the **Search Type** to **Exhaustive search**, type the unique text into the box at the bottom, click ASCII or Unicode, and click Search.

6. When Disk Probe finds the text, it displays a dialog box containing the sector number. Record this number and continue searching.

7. Choose the Sectors, Read command.

8. Set the starting sector to be earlier than the detected sector and the number of sectors large enough to encompass the sector containing the problem text. Click Read.



9. Scroll to the sector where the problem text was found and verify that it is problem text. Unfortunately, Disk Probe cannot tell you what file the problem text is in, only the sector on disk.

Security Tip: If you don't know which file contains the problem text, you may be able to find it with the Search command on the Start menu. Do a **Search for Files or Folders** and search for the problem text.

10. Quit Disk Probe.

8.1.3 Searching for Text on a Macintosh System

Macintosh systems can have several file systems in use at the same time. The current version of Norton Utilities contains a Disk Editor that understands the different file systems but it must be run from an OS 9 or earlier system. It cannot work correctly under OS X.

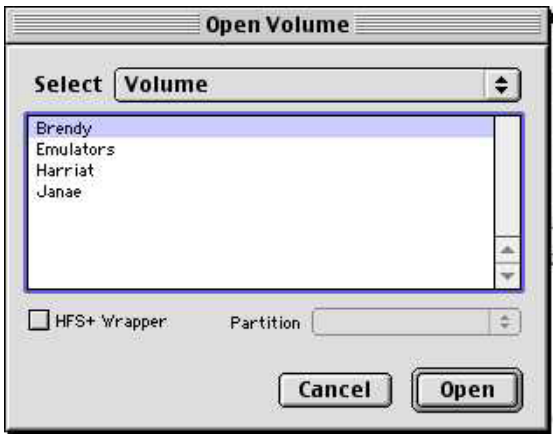
8.1.3.1 Viewing a File with Norton Disk Editor (Mac)

The Norton Disk Editor for Macintosh can view the contents of files and search for text on a sector by sector basis.

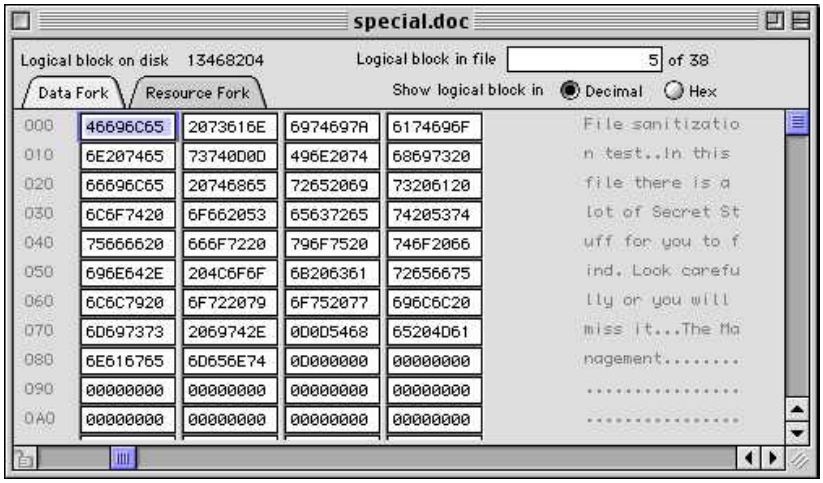
1. Boot the system with the Norton CD or an OS-9 floppy.

2. Start Norton Disk Edit.

3. As the program opens, select the drive you want to search in the dialog box.



4. Choose the File, Open File command and select the file containing the problem text. The raw contents of the file are displayed.



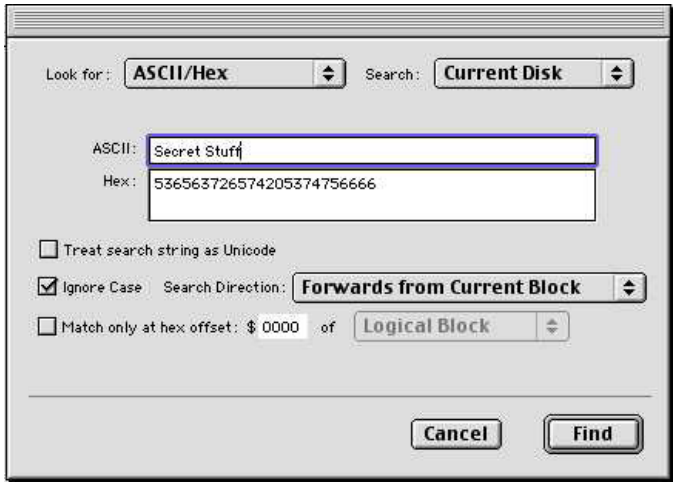
5. Scroll through the file and find a unique text string near the problem text and write it down.

8.1.3.2 Searching With Norton Disk Editor (Mac)

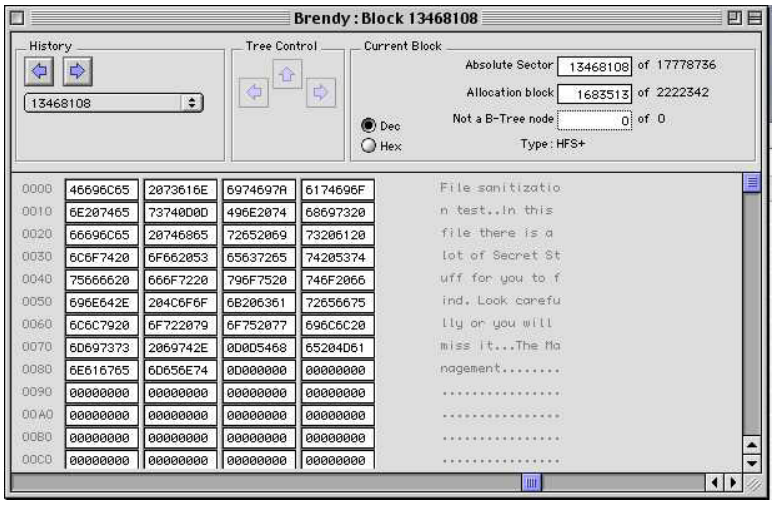
The Norton Disk Editor can also search a disk for different text.

1. Boot the system with the Norton CD or an OS-9 floppy.
2. Start Norton Disk Edit.

3. Choose the Edit, Find command and type the unique text into the text box. Click Find.



4. When Disk Edit finds the text, it displays the contents of the sector it found the text in. See that this is part of the problem data. Write down the sector number of the sectors that contain the problem text. A difficulty here is that this version of the Disk Editor does not tell you which file the found text is in, only the sector number.



5. Choose Edit, Find Again to search for another copy. Continue this until you have a list of all the sectors on the disk that need to be cleaned.

6. Quit the Disk Editor.

8.1.4 Searching for Text on a UNIX System

Searching for text on a Unix system (Solaris, Linux) can be done with the grep (or fgrep) command available on all Unix systems. Grep can search files for strings and can be used to search a disk for a string with a command like,

```
fgrep –r –s "string" /* | more
```

Here, -r makes it recurse down the subdirectories and –s makes it skip error messages. This will tell you which files the string appears in and include a little context for the string. The pipe to more should be safe as pipes do not generally write to disk. Do not redirect the output into a file. Redirecting it into a file can create more classified information on your computer and can overwrite a deleted copy of the classified information, making it impossible to find. You will need to take manual notes of any copies of the classified text you find.

> **Security Tip:** keep in mind that Unix file systems often contain multiple mount points where different disks and disk partitions are attached to the root file system. As you locate files containing classified information, you should also record which disk and partition they are in. A command like df can be used to list the different disks and mount points.

Searching for text in deleted files is problematic on Unix systems as there are no tools available to do that job in a way that prevents the spread of the classified files. The Coroners Toolkit is available but it copies the deleted sectors to another disk and turns them into a series of files. You then use Grep to find whatever text you are looking for. If you have classified information in the deleted sectors and you run the toolkit, you now have classified information on the new disk.

If you have a Linux system, you can boot it with a Windows or DOS floppy or CD and scan it with the same tools as are used to scan Windows systems. The biggest difference is that like scanning NTFS disks, programs like the Norton Disk Editor do not know anything about a Linux file system. It can show you the contents of sectors but you will not know which files those sectors belong to.

Another option is to move the disks to another system for scanning and sanitization. For example, a Sun computer cannot run any of the DOS based scanning tools. What you can do is to move the sun disks to a windows system that has a compatible disk drive card. You can then use the DOS tools to scan the disk.

8.2 PREPARING MAILBOX FILES FOR WIPING

Mailbox files on Windows and Macintosh systems are a special problem. One of the most common ways for classified information to get on an unclassified system is through the mail system. The classified information can be in either a mail message or in an attachment. Most mail readers store mail in Unix style mail files which are text files with each new mail message added to the end of the file. When a message is moved to another mail file or deleted, it is not really removed from the file but only from the mail index to that file. The problem is that you probably want to keep all the other e-mail in the mail

file. So what we need to do is to copy the good mail to another file so the contaminated file can be sanitized.

Another difficulty is mailbox compaction. As more mail messages are moved or deleted from a mail file, they become filled with deleted messages. Compaction rewrites these files, eliminating all the copies of deleted mail. We don't want this to happen as it may make it impossible to determine which sectors on a disk need to be sanitized.

The third thing to worry about is attachments. If the classified information is in an attachment rather than in the e-mail message itself, you must worry about where the attachment is. Some e-mail programs like Outlook Express leave the raw e-mail intact and place it in a mail file. In this case, the attachment is still part of the message and it is all in one place in the e-mail file. You must manually extract an attachment and save it to disk for it to appear elsewhere on your disk.

> **Security Tip:** Viewing an attachment in Outlook Express without manually saving it to disk still creates a copy on your disk in either the temp Directory or in one of the Internet temporary directories where it is opened by the program used to view it.

Other e-mail programs such as Eudora, extract attachments as soon as the e-mail is received, putting the attachment in an attachments directory and adding a link to the e-mail message that points to the attachment. The e-mail message without the attachment is then added to the mail file.

Presumably, at this point, you know that the classified information entered your system in an e-mail message. Otherwise, you don't need to follow these procedures. You need to know if the classified information is in the body of an e-mail message or in an attachment. If it is in an attachment, determine if you have a Eudora like or Outlook Express like e-mail program.

If the classified data is in the body of an e-mail message you need to clean the e-mail file and not worry about any attachment files.

If the classified data is in an attachment and you have a Eudora like mail reader, you need only worry about the attachment files and not about the e-mail files.

If the classified data is in an attachment and you have an Outlook Express like mail reader, you need to clean the mail file and any copies of the attachment you saved.

The steps are,

1. Is the classified information in the body of the e-mail message or is it in an attachment. If it is in both places, you will have to perform both branches of this procedure. If it is in the body, go to step 4. If it is in an attachment go to 2.

2. Do you have a Eudora like (attachments are extracted and put in an attachments folder) or Outlook Express like (attachments stay with the e-mail message) mail reader? If it is Eudora like you don't have to clean the mail files. Continue

sanitizing individual files, including the attachment file. If it is an Outlook Express like mail reader go to the next step.

3. The classified information is in an attached file that is part of an e-mail message. Note that you will not likely be able to see this text using a sector scanner because it is in rot64 format (binary characters have been converted into printable codes).

4. Boot your system in safe mode (Windows) or with extensions off (Macintosh).

5. Start your mail program.

6. Do not let your mail program compact mailboxes. In Outlook Express choose Tools, Options, Maintenance tab and uncheck Compact messages in the background. In Eudora, don't click the Special, Compact Mailboxes command.

7. Do not let your mail program automatically empty the trash. In Outlook Express choose Tools, Options, Maintenance tab and uncheck Empty messages from the Deleted Items folder on exit. In Eudora choose Tools, Options, Miscellaneous tab, and uncheck Empty trash when exiting.

8. You should know which mailboxes the e-mail containing the classified text is in. Most messages start in the IN box and may be filtered to other mailboxes or deleted and moved to the Trash mailbox. Do not delete any mailboxes.

Note: Different e-mail programs have different names for the IN and Trash mailboxes. Substitute the name your program uses for IN and Trash.

9. For each mailbox that contains the classified e-mail except for the Trash, create a new mailbox and copy all of the e-mail except for the classified one to the new mailbox.

10. Quit your mail program.

11. Make a list of all the mailbox files that contain the classified information. Include the Trash mailbox in this list. You will need to find where the mailbox files are stored on a system to get their real file name. They usually have the same name on disk as they have in the mail program with an extension like mbx (Eudora) or dbx (Outlook Express). Eudora's .toc files are the indexes to the mail box files. Outlook Express stores the index at the beginning of the mailbox file.

12. Add this list to the list of files you need to sanitize.

At this point, you will need to go to the section on sanitizing individual files and sanitize the mailbox files along with any other files you need to sanitize. After you have sanitized the system, open your mail program again and delete the sanitized mailboxes. You may need to designate a new IN box as you have likely deleted the existing IN box. Most mail programs should create a new IN box as soon as you try to download mail.

8.3 SANITIZING INDIVIDUAL FILES

One of the first things to check here is if the information is in a mailbox file. Assuming you want to save the other messages in your mailbox file, you will need to prepare those files first to separate the good data and the classified data into two different mailbox files. Go to *8.2 Preparing Mailbox Files for Wiping*.

On the other hand, if you don't care about the other messages in the mailbox files, go ahead and sanitize the whole file.

At this point, you have a list of the files that contain the classified data and you are ready to sanitize those individual files, plus the free space, and the swap space. You have two options here, to use a program to sanitize the file or to sanitize the problem sectors by hand. If you have only a few sectors of problem data, you can sanitize them by hand much faster than by sanitizing whole files with a program. A second benefit is that you do not need to know what file the classified information is in to be able to sanitize it. The only potential problem is that overwriting a sector in a file may damage that file, but then you are planning to delete the file anyway so it should not be a problem.

> **WARNING:** In most cases, problem text will be in document files however if a file name is classified you will find it in directory files and possibly in the registry. If you find the problem text in one of the registry files (**C:\windows\system.dat**, C**:\windows\user.dat**, **C:\windows\policy.dat**), wiping that file will make your system unstable and you may need to reinstall Windows to restore the file. Wiping a directory file will make all other files found in that directory inaccessible. Be sure to move those files out of that directory before wiping the directory file. If you wipe any system or directory like files, you should run a program like Norton's Disk Doctor to make sure things are still consistent after you are done.

8.3.1 Sanitizing Individual Files on a Windows System

Partial sanitization of Windows 95/98/ME systems can be achieved with either Norton Wipe Info or BCWipe. Either program provides sufficient capabilities to sanitize a file.

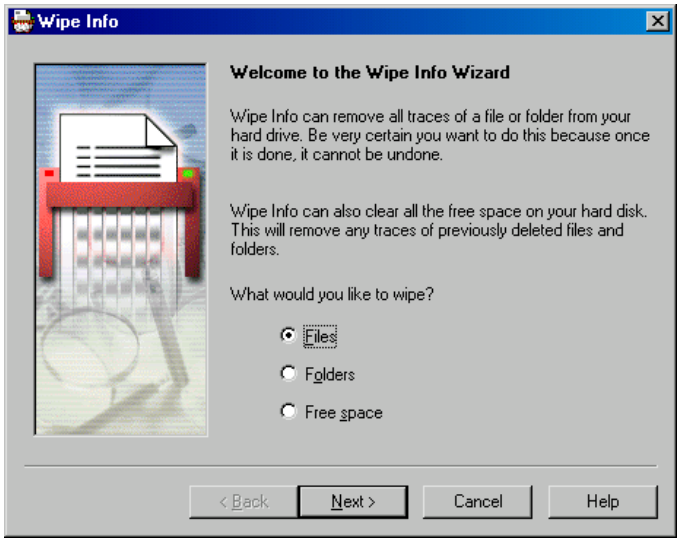
Partial sanitization of Windows NT/2000/XP systems precedes in much the same manner as for Windows 95/98/ME systems except that the Norton Disk Editor is not able to tell you which file owns a given sector. You have the same problem with Disk Probe as it can look at files or it can look at sectors but it cannot map between the two. If you know what file contains the classified data, you can use either Norton Wipe Info or BCWipe to sanitize the file. If you don't know which file contains the classified info, you may want to consider wiping the info by hand using the Norton Disk Editor. See *8.3.4 Sanitizing Individual Sectors With a Hex Editor*.

8.3.1.1 Sanitizing Individual Files with Norton Wipe Info

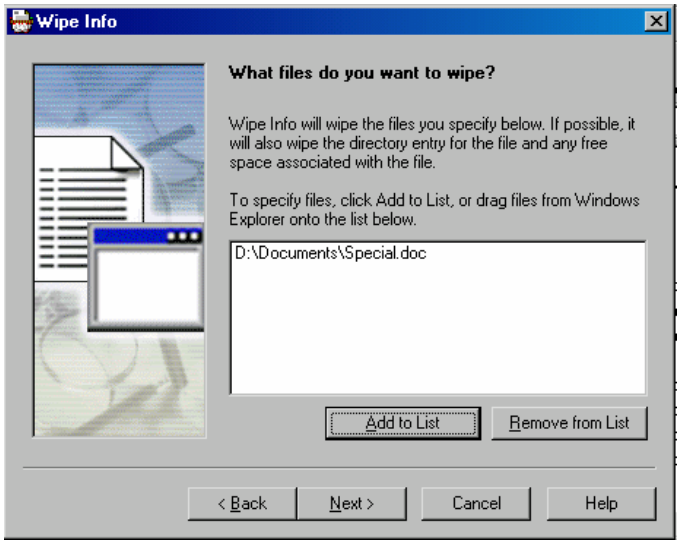
1. Boot your Windows system into Safe Mode by pressing F8 during startup and selecting Safe Mode.

2. Run Wipe Info in the Norton Utilities tools group.

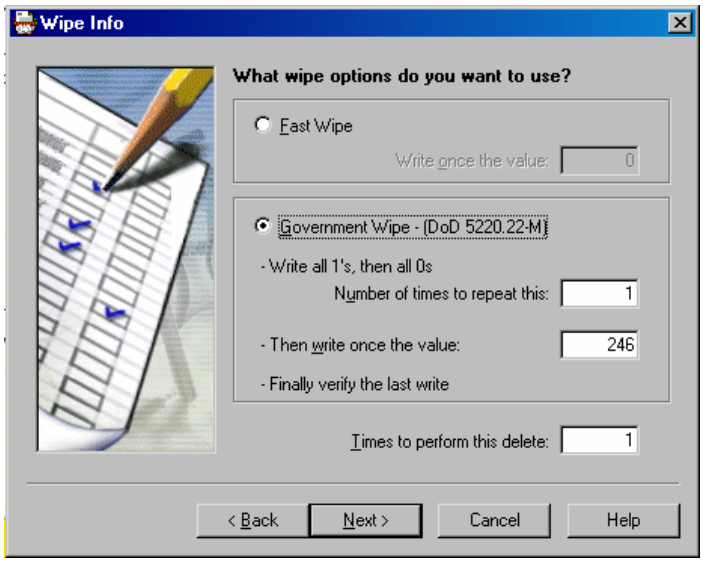
3. Choose the Files option in the dialog box and click Next.



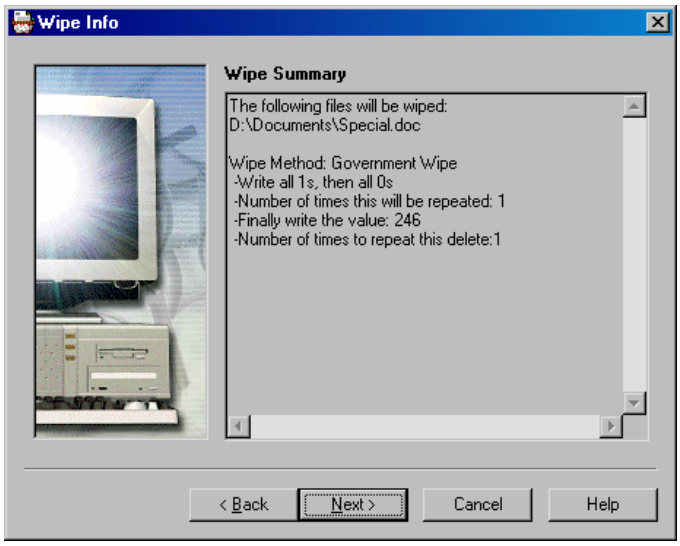
4. In the next dialog box select the files to wipe. Use the Add to List button to add files to be wiped. Insert all the files you know contain the classified text. Click Next when you are done.



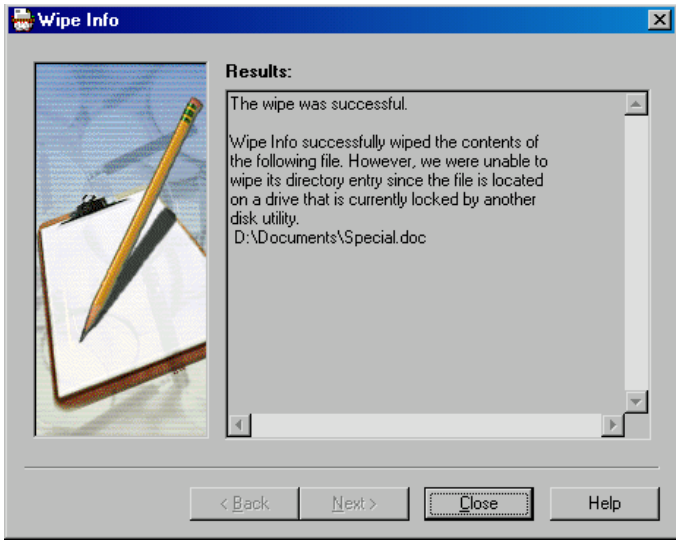
5. In the next dialog box, choose Government Wipe, with one iteration. For the **Then write once the value** option, type any value between 0 and 255. Click Next when done.



6. Click Next if the information is correct.



7. Click Next to wipe the files and wait while Wipe Info clears the file. The following dialog box appears if it was successful.



8. Quit Wipe Info.

9. Delete the wiped files and empty any trashcans and any deleted file savers such as Norton File Protect.

10. Start Wipe Info again and choose Wipe Free Space. Choose the drive that contained the problem files and use the same settings as for the files.

11. Wipe the free space.

12. Quit Wipe Info.

This completes wiping the info. Go next to *8.4 Searching for Missed Files* to check for any missed copies of the classified text.

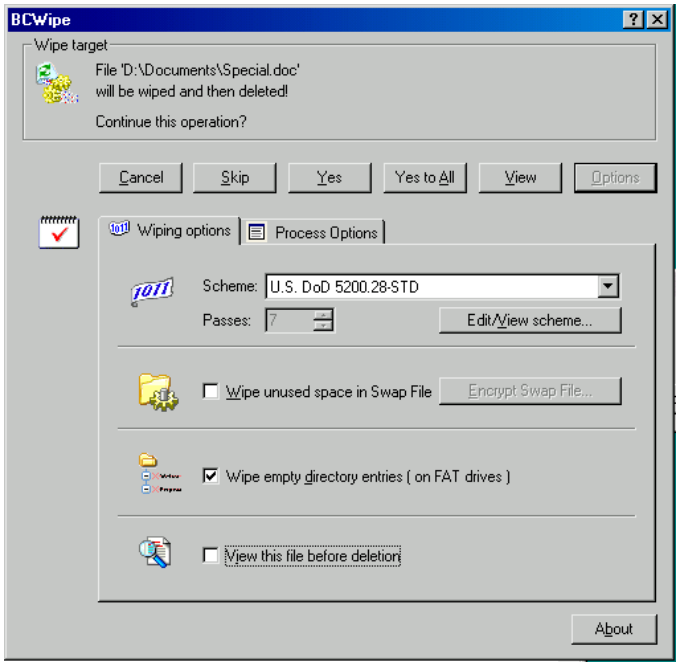
8.3.1.2 Creating a DOE Wiping Scheme in BCWipe

You can use the following procedure to create a wiping scheme in BCWipe that matches the DOE guidance. You only need to do this once in BCWipe as it will save the new scheme.

1. BCWipe must be open. For example, right click on a file and select **Delete with wiping** from the drop down menu.

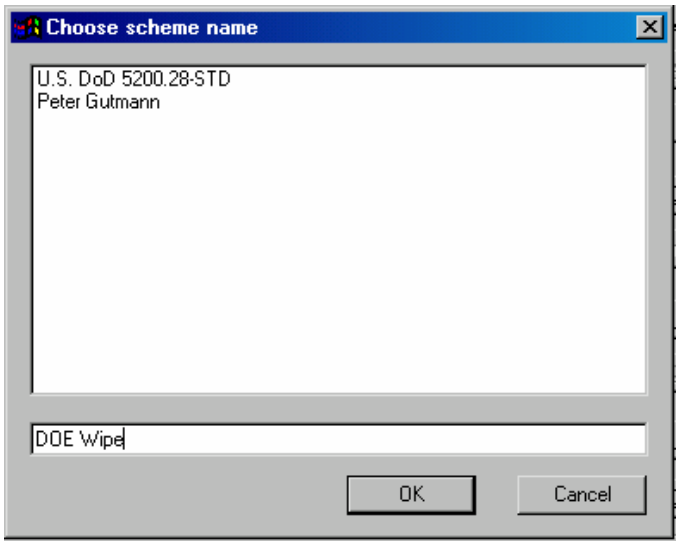
2. Click Options

3. Click the Edit/View scheme button.



4. In the Wiping Scheme Editor, click New.

5. Type a name for the new scheme ("DOE Wipe") and click OK.



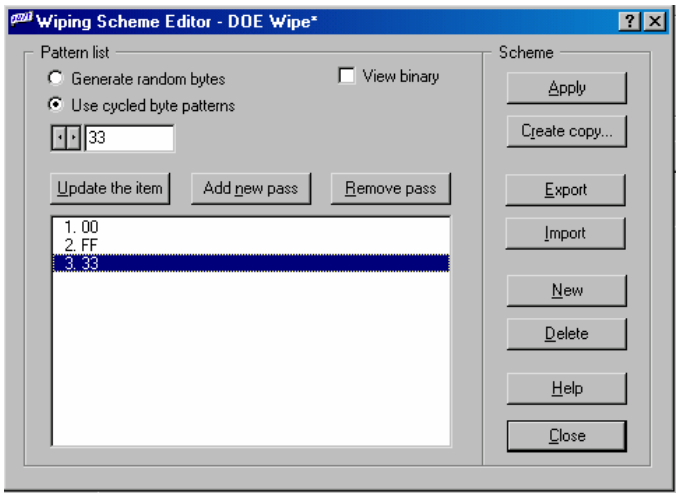
6. In the Wiping Scheme Editor click Use cycled byte patterns and set the pattern to any pattern from 00 to FF (hex). Here I chose 00. See Appendix C for a list of hex codes and their complements.

7. Click Add new pass.

8. Change the pattern to the complement of the first pattern. In this case, FF is the complement of 00 (See Appendix C).

9. Click Add new pass.

10. Change the pattern to any random character between the hex values 00 and FF and click Add new pass. Here, I chose a 33 hex which is the binary pattern 00110011.



11. Click Apply and then Close.

12. In the BCWipe dialog box make sure the new scheme is selected. Change the number of passes to 3 to match the three binary patterns you just defined to wipe the file.

8.3.1.3 Sanitizing Individual Files Using BCWipe

Sanitizing files with BCWipe is much like using WipeInfo.

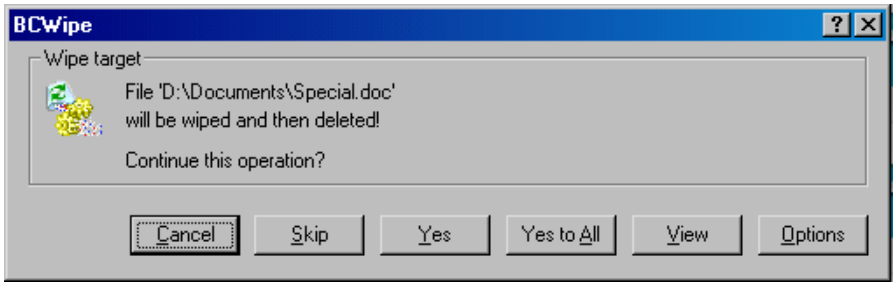
At this point, you have used the Norton Disk Editor to find where the problem text resides on the disk.

1. Boot your Windows system into Safe Mode by pressing F8 during startup and selecting Safe Mode.

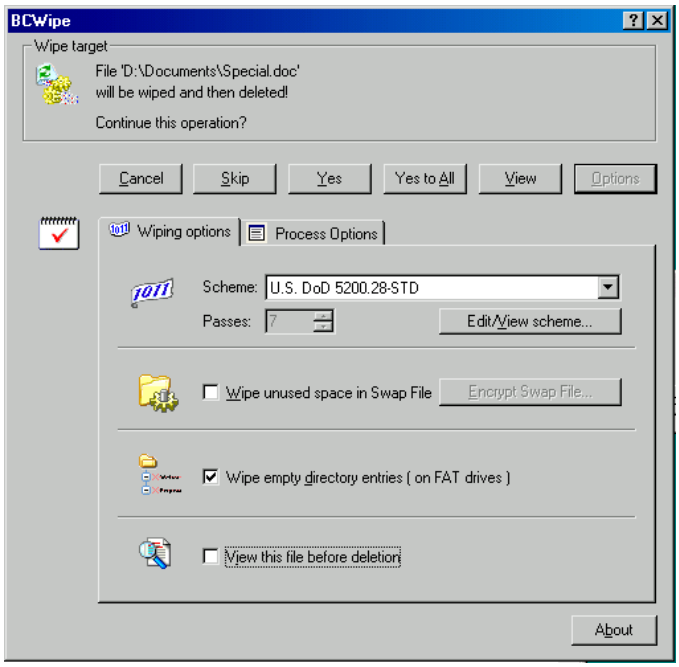
2. Open a Windows Explorer window and find the file that contains the problem text.

3. Right click on the file and select **Delete with wiping** from the drop down menu.

4. When the dialog box appears, click the Options button.

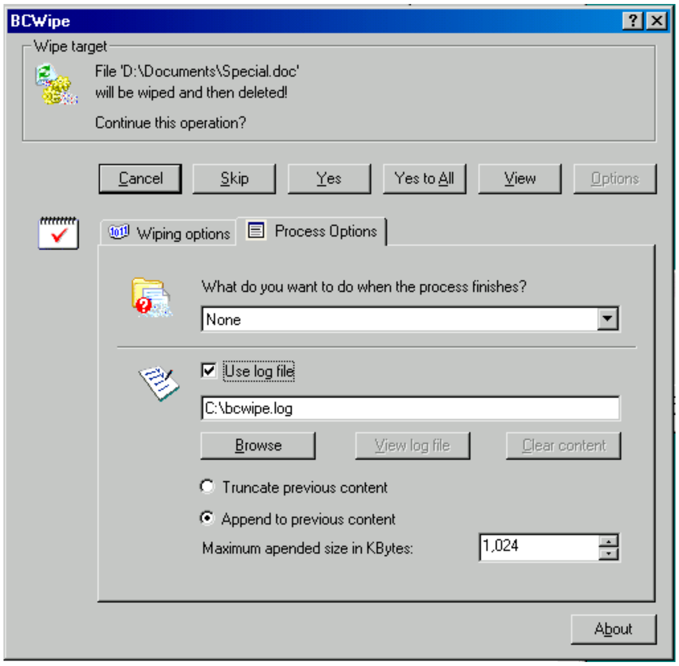


5. The default wipe is a DOD 7 pass wipe. This wipe is more than sufficient to wipe a file within the DOE. You may want to create a faster, three pass scheme that matches the DOE guidance (see 8.2.1.2 Creating a DOE Wiping Scheme in BCWipe). Select the wiping scheme to use.

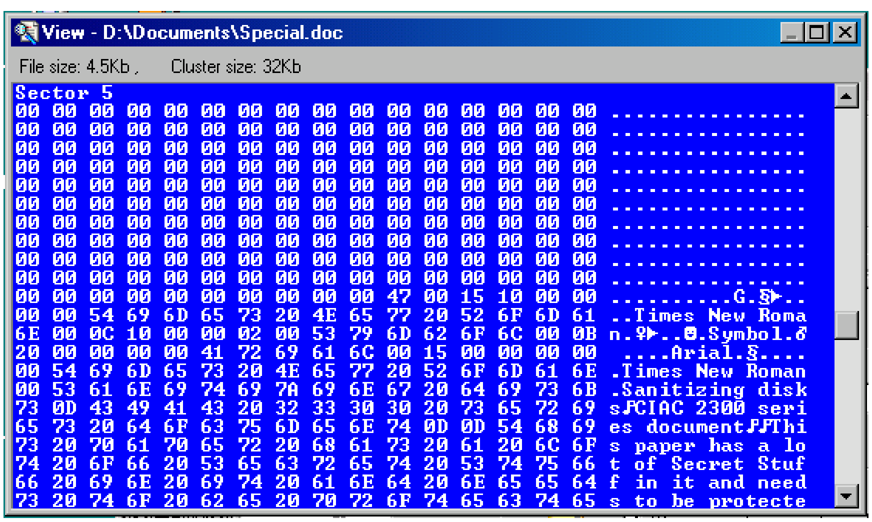


6. Check **Wipe unused space in Swap File** and **View this file before deletion**.

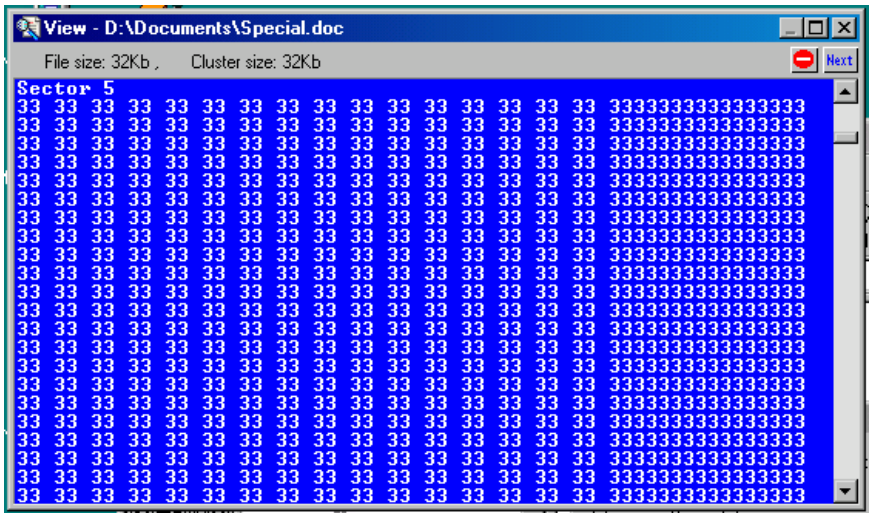
7. Click the Process Options tab and set **What do you wish to do when the process completes** to **Show report message**. Check **Use log file** and set a log file path and name.



8. At this point, you can view the file that is about to be wiped by clicking the View button. Scroll down the file until you find the problem text. Write down which sector it is in so you can go back and check it after wiping. In this case, it is in sector 5.



9. Click Yes and the file is sanitized with the three pass DOE Wipe scheme. When it completes, a file viewer opens so you can examine the file. If you scroll to sector 5 you see that the problem text has been overwritten.



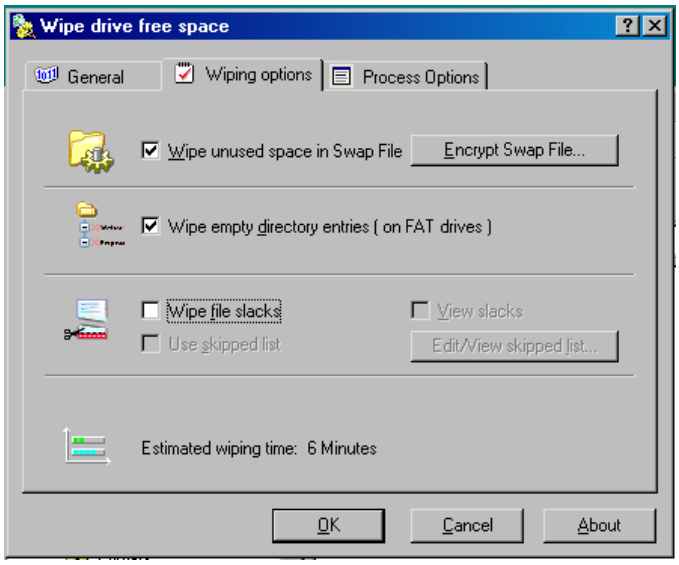
10. Click Next (top-right corner of the viewer) and the file viewer closes, the file is deleted, and the log file is displayed. Check the log for any problems.

11. Close the log file.

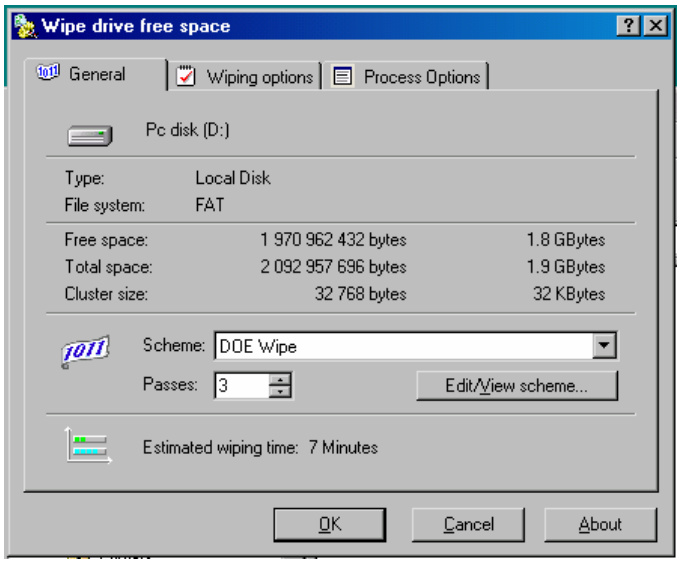
12. In a Windows Explorer window, right click on the disk drive that contained the problem text and choose **Wipe free space with BCWipe**.

13. Click the Process Options tab and set **What do you wish to do when the process completes** to **Show report message**. Check **Use log file** and set a log file path and name.

14. Click the Wiping Options tab and check **Wipe unused space in swap file** and **Wipe empty directory entries**.



15. Click the General tab and make sure that **DOE Wipe** and **3** passes are set.



16. Click OK to start the wiping process.

Security Tip: while the free space wiping is going on, Windows may complain that there is no space available on the drive. This is normal as you are intentionally filling all available space on the drive with the overwrite pattern. Click Cancel and let the process continue.

17. When the wiping process completes, click OK and the log file is displayed. Check the log file for any problems.

This completes wiping the info. Go next to *Searching for Missed Files* to check for any missed copies of the classified text.

8.3.2 Sanitizing Individual Files on a Macintosh System

Macintosh systems can be sanitized using Norton Wipe Info for the Macintosh. If you are using OS X, you must reboot your system in OS 9 as Wipe Info does not run under OS X.

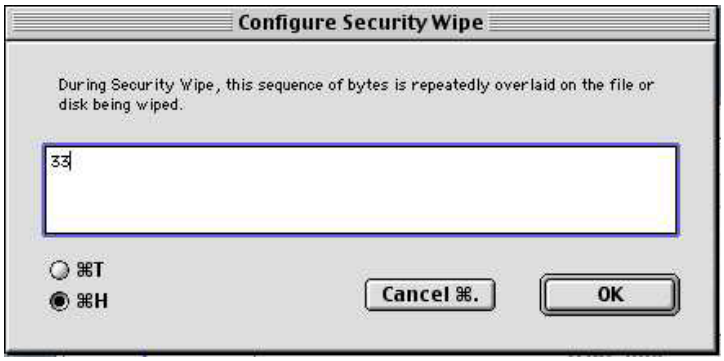
1. Start the Macintosh in OS 9 or earlier with extensions off (Hold down the shift key at boot) or boot the system from the Norton Utilities CD.

2. Run Wipe Info in the Norton Utilities folder.

3. Check the Options, Security Wipe command.

4. Choose the Options, Configure Security Wipe command.

5. In the text box, type the character to be used to overwrite the file (See Appendix C). The Macintosh version of Wipe Info wipes first with this character, then with its complement, and finally with 00.



6. Click the Wipe File/Folder button.

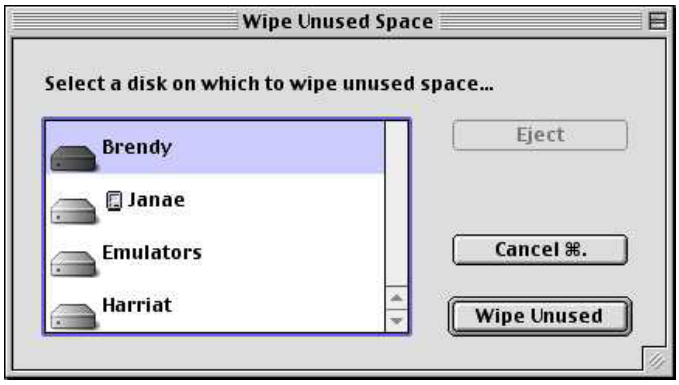
7. Select the file or folder to wipe and click Wipe and click Wipe again in the warning dialog.

8. The file has now been wiped. Continue wiping files in this manner until you have wiped all the known problem files.

9. Wipe the Sherlock Index file for the volume containing the problem text. The index file is either in the volume's root directory named, **.FBCIndex** or in a folder named, **TheFindByContentFolder** and is named: **TheFindByContentIndex**. You may have both of these files if you use both OS 9 and OS X. Wipe these files as before.

10. Click Wipe Unused.

11. Select the disk containing the problem text and click Wipe Unused and then Wipe Unused Space in the warning dialog.



12. When this completes, end Wipe Info.

13. Start Disk Edit and check the sectors where you previously found the problem text. See that it all contains the last character written by the wiping program (00).

14. Search for the problem text as before. If you find copies, you must figure out what files they are in and wipe those files. Continue until you no longer find the problem text.

Security Tip: If you are having trouble finding the files that contain the problem text you can use the Sherlock or Sherlock 2 application to search for files containing the search string. As you have wiped the index files, you must reindex the drive before you can search it.

Keep in mind that indexing may place problem words in the index file so you must sanitize the index file after locating the problem files. The index file contains only the words and the files they were found in. The index file is in the root directory of the indexed drive and is named **.FBCIndex** or in the folder, **TheFindByContentFolder** and is named: **TheFindByContentIndex**.

15. If you have indexed the drive to search for a file, be sure to sanitize the index files and free space again.

8.3.3 Sanitizing Individual Files on a UNIX System

UNIX type operating systems such as Solaris and Linux can be sanitized using the Scrub code. There is also a version of BCWipe for UNIX systems but it is still in development. As of this writing, BCWipe cannot sanitize the free space on a UNIX volume which is

necessary if a file has been deleted. Another difficulty with UNIX systems is that there is no way to search the raw sectors of the hard drive for the problem text. You must know what files it is in. It is possible to move a UNIX hard drive to a Windows or Macintosh system and to then examine and sanitize the hard drive there. You will not be able to determine what files contain the problem data but you can search for and sanitize the individual sectors.

For a Linux system or any system that runs on a PC, you can boot the system with a DOS or Windows 95/98/ME disk and then use the procedures for sanitizing a file on a Windows 95/98/ME system. The main difference is that you will have to sanitize the sectors as the Windows system will not know about the files in the UNIX system.

8.3.3.1 Sanitizing with Scrub.

You should have already installed scrub on your system. If not, install it on a different disk from the one that needs to be scrubbed.

1. Don't delete the file. It is much cleaner and easier to clean a system if the problem data is in a known place. You cannot easily search the raw sectors of a UNIX system to look for the problem data.

2. Login as root or boot the system in single user mode.

3. Mount the file system if it is not already mounted.

4. Use the following command to sanitize the files known or suspected to contain the problem data.

   scrub –r *filename*

   This command scrubs the file indicated by *filename* using the DOE wipe, including the random overwrite.

5. Use the following command to scrub any file names in case they are also a problem.

   scrub –D *filename*

   The file that was linked by the directory entry you just scrubbed will be saved in the root directory of the system with a name like UUUUUUUUUUU.

6. Delete the file in the root directory with the name like UUUUUUUUUU…

7. Delete all the sanitized files.

8. Scrub all free space with the following command.

   scrub –X *filename*

In this command, *filename* is the name of a dummy file that is somewhere in the volume whose free space you want to sanitize. If you have more free space than the maximum allowed file size, you will need to run this command more than once with different file names to completely sanitize a drive.

9. Continue running the last command with a different file name until you get the error that the file system is full or scrub hangs trying to write to the full file system. If Scrub hangs, end it with Ctrl-C.

10. Delete the dummy files created by scrub. Your system should now be clean.

8.3.4 Sanitizing Individual Sectors With a Hex Editor

If you are having trouble getting rid of all copies of some problem text because you cannot determine what file contains it, it is possible to do an overwrite using the disk editor. As you must realize, this only works for systems where there is a disk editor available that can both read and write to a sector. The disk editor for Windows 95/98/ME and Macintosh systems is the Norton Disk Edit. For Windows NT/2000/XP systems it is the Disk Probe program.

8.3.4.1 Sanitizing Individual Sectors with Disk Edit

Follow these steps to sanitize individual sectors using Norton's Disk Edit.

1. Start Disk Edit.

2. When Disk Edit starts, it is in Read-Only mode and cannot write to disk. You must first change to Read-Write mode.

3. Choose the Tools, Configuration command.

4. Uncheck the Read Only box and click Save.

5. Scroll to the first sector that needs to be overwritten.

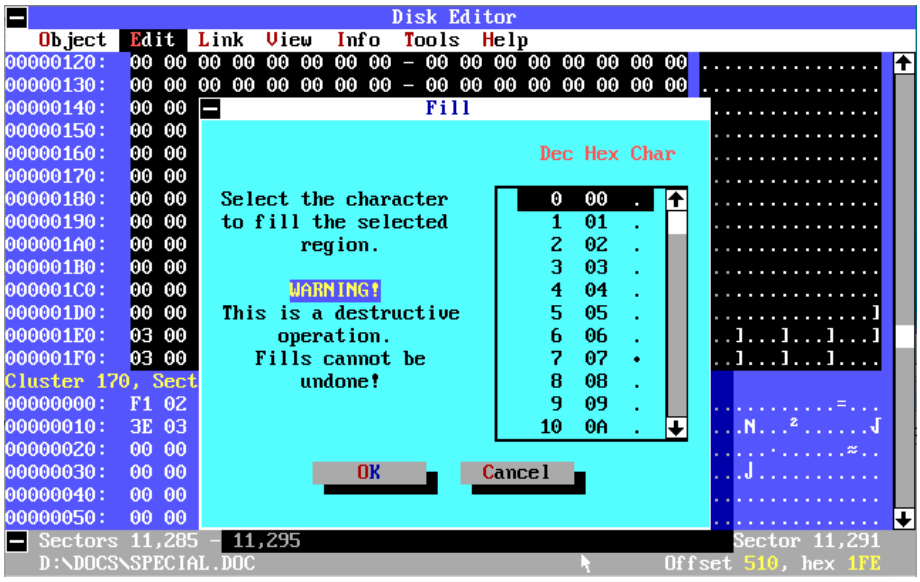
6. Scroll forward and backward around the sector you found to determine which sectors need to be sanitized. The sectors you pick are determined by how much of a file needs to be cleaned, a whole file or just a few paragraphs. List the sector numbers for all the sectors that must be sanitized.

7. Scroll to the first sector in your list.

8. Select the whole sector by clicking and dragging across the hex values.

9. Choose the Edit Fill command.

10. Select the first character to use as a fill character and click OK (See Appendix C for a list of characters and their complements).



11. Choose the Edit, Write Changes command.

12. Click Write. This completes the first overwrite of the first sector.

13. Choose the Edit Fill command.

14. Select the complement of the first character to use as the fill character and click OK.

15. Choose the Edit, Write Changes command.

16. Click Write. This completes the second overwrite of the first sector.

17. Choose the Edit Fill command.

18. Randomly select a character from the list as the fill character and click OK.

19. Choose the Edit, Write Changes command.

20. Click Write. This completes the third overwrite with a randomly selected character.

21. Scroll to the next sector in your list and repeat steps 7 through 20.

22. Repeat these steps for all the sectors in your list.

Note: You can speed this process a little by copying the filled sector and pasting it into all the sectors that must be overwritten. Then, go back and do the second overwrite to all the sectors and so on.

8.3.4.2 Sanitizing Individual Sectors on a Macintosh With Disk Edit +

1. Boot the Norton CD or boot the system with extensions off (Shift down at boot time).
2. Start Disk Edit +.
3. Scroll to the first sector that contains problem text.
4. Scroll forward and backward around the sector you found to determine which sectors need to be sanitized. The sectors you pick are determined by how much of a file needs to be cleaned, a whole file or just a few paragraphs. List the sector numbers for all the sectors that must be sanitized.
5. Scroll to the first sector on your list.
6. From Appendix C, pick a character for the first overwrite.
7. Fill that sector with the hex code for the selected character by typing it into each block.
8. Choose the Edit, Copy Sector command.
9. Choose the Disk, Write Sector command.
10. Scroll to the next sector on your list.
11. Choose the Edit, Paste Sector command.
12. Choose the Disk, Write Sector command.
13. Repeat the last three steps for all of the sectors on your list. This completes the overwrite.
14. Scroll back to the first sector on your list and fill it with the complement of the character you used for the first overwrite.
15. Choose the Edit, Copy Sector command.
16. Choose the Disk, Write Sector command.
17. Scroll to the next sector on your list.
18. Choose the Edit, Paste Sector command.

19. Choose the Disk, Write Sector command.

20. Repeat the last three steps for all of the sectors on your list. This completes the second overwrite with the first character's complement.

21. Scroll back to the first sector in your list. Choose a random hex character. Fill the sector with that character by typing it into each cell. For example, if you choose a hex F6, you would type **F6F6F6F6** into each cell.

22. Choose the Edit, Copy Sector command.

23. Choose the Disk, Write Sector command.

24. Scroll to the next sector on your list.

25. Choose the Edit, Paste Sector command.

26. Choose the Disk, Write Sector command.

27. Continue these three steps for all of the sectors on your list. This completes the overwrite with a randomly selected character.

28. Examine all the overwritten sectors again to be sure they contain the last character written (the randomly chosen character).

29. Quit Disk Edit.

8.3.4.3 Sanitizing Individual Sectors with Disk Probe

Here we use Disk Probe to sanitize individual sectors on a Windows NT/2000/XP system.

1. Boot the system into safe mode by pressing F8 when the system starts to boot and selecting Safe Mode.

2. Start the Disk Probe program.

3. Choose the Drives, Logical Volumes command.

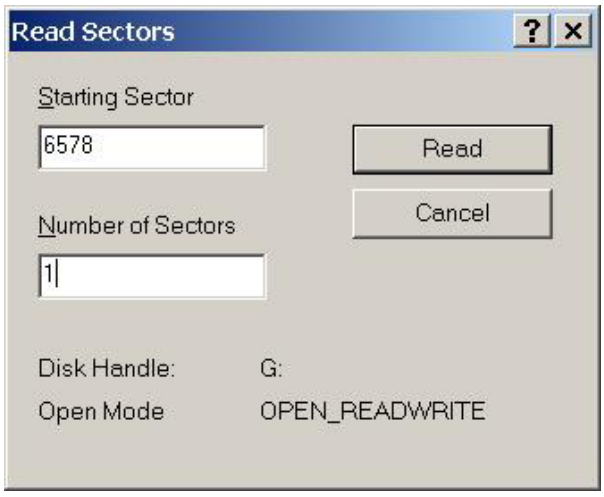
4. In the dialog box double click the drive containing problem text and click the Set Active button to make this volume active.

5. Uncheck the Read Only box for that drive and click OK

6. Scroll to the first sector that needs sanitizing.

7. Scroll forward and backward around the sector you found to determine which sectors need to be sanitized. Add these sectors to your list.

8. Choose the Sectors, Read command and set the **Starting Sector** value to the first sector that needs to be overwritten and the **Number of Sectors** to **1**. Click Read to read the sector.



9. Click on the first hex value in the sector and type a hex character between **00** and **FF** (See Appendix C for a list).

10. Continue typing that character until the whole sector is filled.

11. Choose the Sectors, Write command. Make sure the **Starting sector to write to** is the number of the first sector that needs to be overwritten.

12. Click Write It and Yes when it asks you if you really want to do this.

13. Choose the Sectors, Write command again. Change the **Starting sector to write to** to the next sector on your list, click Write It and Yes.

14. Continue writing sectors until you have overwritten all of the sectors on your list. This completes the first wipe.

15. Click in the first byte of the sector and type the complement of the first character used to overwrite the sectors. Fill the whole sector with that character.

16. Choose the Sectors, Write command, change the **Starting sector to write to** to the first sector in the list of sectors to be sanitized and click Write It and Yes.

17. Continue doing this to all of the sectors in the list. This completes the second wipe with a complement character.

18. Click in the first byte of the sector and type a random hex value between **00** and **FF**. Continue typing the value until the whole sector is filled with it.

19. Choose the Sectors, Write command, change the **Starting sector to write to** to the first sector in the list of sectors to be sanitized and click Write It and Yes.

20. Continue doing this to all of the sectors in the list. This completes the third wipe with a random hex value.

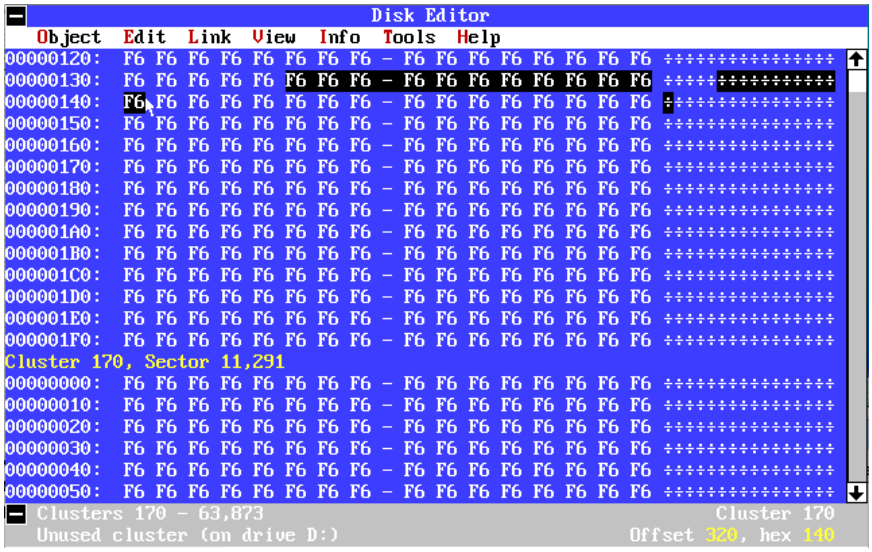
21. Choose the Sectors, Read command and read the sectors that contained the problem data. Check that they have all been overwritten with the last value you chose to overwrite with.

22. If everything is correctly overwritten, search again for the problem text. If none is found, you are done, otherwise continue overwriting sectors until you cannot find any more copies of the problem data.

8.4 Searching for Missed Files

The following steps are used to verify that all copies of the classified data have been cleaned off of a system. This is essentially the same as the initial search for the classified text plus a check of the known locations for the overwriting disk pattern.

Using the methods of section 8.1 for your particular operating system, first check the list of sectors where you know the problem text used to reside. Make sure those sectors are overwritten with the last character used to overwrite the sectors. For example, the following shows a sector overwritten with the hex character F6.



Next, search the whole disk for the problem text again as before. If you don't find the problem text and all known locations of the text are overwritten with the character you chose you are done, otherwise write down the locations that contain the problem text and wipe the file and free space again. Keep doing this until you can no longer find the problem text.

8.5 Sanitizing the Whole Drive and Putting the Files Back

You reach this point if you believe there are more copies of the classified text on the system but you don't know where they are because the space they used was overwritten by another file. While the problem sectors have been overwritten, they have not been overwritten by the required patterns the required number of times. As you cannot now find the sectors that contained the classified text so that you can overwrite it the required number of times, your only choice is to overwrite the whole disk (or disk partition).

> **Security Tip:** In some cases, it may be faster and easier to copy the good files to another disk, sanitize the whole drive, and then put the good files back.

As you do not want to lose all the unclassified files on the disk you are going to need to copy them off of the disk before you sanitize it. Because you do not want to copy the classified text onto your backup disk and then back onto the original disk, you are going to have to sanitize the original disk before moving the files off. You don't have to actually sanitize the disk here, just overwrite the problem data once so that it cannot be copied off of the disk. After the data you want to save is copied off, the disk, then you do the real drive sanitization.

Sanitizing and Replacing Files With Ghost

Norton Ghost can be used to copy all files off of a disk and then to restore that disk after it has been sanitized. Sanitizing can also be accomplished with the GDisk.exe utility included with Ghost. A nice feature of Ghost is that with its raw copy feature turned on (-ir) it can copy any file system that can be attached to your system.

A convenient way to use Ghost is to have a special system with a large hard drive and disk drive cards for all disks you use. A contaminated disk then can be attached to the system, ghost used to copy its files onto the large hard drive, Gdisk used to sanitize the disk, and Ghost used again to copy the files back onto the disk. This same system can also have the Norton Disk Editor and/or DIBS Mycroft programs for searching for contaminated sectors.

The large backup hard drive needs to be large enough to store the Ghost image for the disk you want to sanitize. For Windows and Linux disks, it needs to be larger than all the stored files on the system as Ghost copies Windows and Linux systems by files and directories. For other systems you must use the –ir switch to copy all sectors, in which case the backp disk needs to be larger than the disk you are backing up.

Go through the steps in section 8.1 for finding the classified information, 8.2 and 8.3 for sanitizing that data and 8.4 for checking that the data has really been cleared of off the original system. As mentioned above, a single overwrite is sufficient at this point to prevent the classified text from being copied onto the backup disk.

Use Norton Ghost to copy all the drive's contents onto backup media. Assuming you are backing up a Windows disk onto a file on a large hard drive, use a command like,

```
ghost.exe -clone,mode=create,src=2,dst=c:\backup\mydrv.gho
```

This command assumes the hard drive is the second hard drive on the system and it copies to the backup file c:\backup\mydrv.gho. If you are backing up a Macintosh disk or any disk that does not have a DOS style partition table, add the –ir switch to copy all sectors instead of just those that contain files.

Use the methods of section 7.3 to sanitize the whole original disk or disk partition. Here you can use GDisk to do the sanitization. Make sure you are sanitizing the right disk. Use gdisk alone to get a list of disks and gdisk *disknum* /status to get information about disk *disknum*.

```
gdisk.exe 2 /diskwipe /custom:3
```

This wipes the second disk using the DOE wipe (3 times overwrite).

Use Norton Ghost to copy the files back onto the original disk.

```
ghost.exe –clone,mode=restore,src=c:\backup\mydrv.gho,dst=2
```

This reverses the actions of the previous ghost command and copies the files from the mydrv.gho file back onto drive 2

Scan the disk one more time to make sure you have not accidentally copied the classified information back onto the disk.

9 DESTROYING DISKS

All classified disks that are going to leave a controlled area and be decommissioned must be destroyed. To insure that classified data does not leave a controlled area, sanitize the disks before sending them out to be destroyed. This is especially prudent if the drives leave the control of the organization that created the classified disks while on their way to be destroyed. This insures that even if they were to be diverted in some way that the diverted drives would still not yield any useful data.

Destruction methods consist of either destroying the whole drive by pulverizing, smelting, incinerating, disintegrating, or other mechanism that completely destroys the recording surfaces. Drives destroyed in this way do not generally need to be disassembled first unless the pulverizing machinery is not able to destroy the drive case.

Alternately, you can destroy a drive by removing the entire recording surface by sanding or by applying acid. Drives destroyed in this way must be disassembled first to get at the recording surface so you can sand it or dissolve it with acid.

10 REFERENCES

BCWipe – Jetico, Inc., http://www.jetico.com

Disk Probe – Microsoft, Part of Windows NT Resource Kit or in the Windows 2000 Support Tools (on the Windows installation CD), http://www.microsoft.com

DiskEdit – Symantec, part of Norton Utilities and Norton SystemWorks, http://www.symantec.com/nu/nu_9x/

DoD, DOE, CIA, NRC, *DoD 5220.22-m, National Industrial Security Program Operating Manual*, (January, 1995), http://www.dss.mil/isec/nispom.htm,

Gdisk – Symantec, part of Norton Ghost and Norton SystemWorks Pro, http://www.symantec.com/sabu/ghost/ghost_personal/

Peter Gutmann, *Secure Deletion of Data from Magnetic and Solid-State Memory*, Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996, http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Scrub –Lawrence Livermore National Laboratory, http://ciac.llnl.gov/ciac/ToolsUnixGeneral.html#scrub

Rob Sutton, Symantec, Symantec Ghost 7.5; Statement of conformance to DoD 5220.22-M, http://service1.symantec.com/SUPPORT/ghost.nsf/8f7dc138830563c888256c2200662ecd/dcb914b4f63d62d088256b5f007c0a2a/$FILE/Gdisk%20diskwipe.pdf

WipeInfo – Symantec, part of Norton Utilities and Norton SystemWorks, http://www.symantec.com/nu/nu_9x/

http://electron.mit.edu/~gsteele/mirrors/elchem.kaist.ac.kr/jhkwak/TopometrixWeb/datast4.htm

APPENDIX A – DOE N 205.12

Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware

Date 2/19/04

U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 205.12

Approved: 2-19-04
Expires: 2-19-05

SUBJECT: CLEARING, SANITIZING, AND DESTROYING INFORMATION SYSTEM STORAGE MEDIA, MEMORY DEVICES, AND OTHER RELATED HARDWARE

1. OBJECTIVES. To establish Department of Energy (DOE) policy requirements and responsibilities for clearing, sanitizing, and destroying DOE information system storage media, memory devices, and other related hardware.

   a. To provide instructions for sanitizing classified, nonremovable storage media that will be reused in controlled, unclassified environments.

   b. To provide instructions for sanitizing nonremovable storage media that has become partially contaminated with classified information.

   c. To ensure that no unauthorized information can be retrieved from unclassified DOE computer equipment that is to be transferred or declared surplus.

   d. To ensure that all DOE personnel are made aware of requirements for sanitizing information system storage media, memory devices, and related hardware.

   e. To fulfill the commitment to performance-based management of DOE contracts as outlined in Secretary Abraham's May 12, 2003, memorandum, Clarification of Roles and Responsibilities, by supporting to the "maximum extent practicable, the principle to apply performance-based contracting techniques under which the contract will define what is to be done, and not how it will be done."

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. DOE Organizations. Except for the exclusions in paragraph 3c, this Notice applies to Primary DOE, including National Nuclear Security Administration (NNSA), Organizations that own or operate DOE information systems or national security systems (see Attachment 1 for a complete list of Primary DOE Organizations). The attached list automatically includes any Primary DOE Organizations created after the Notice is issued.

   b. Site/Facility Management Contractors. Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Notice that will apply to site/facility management contractors whose contracts include the CRD.

(1) The CRD must be included in site/facility management contracts that provide automated access to DOE information systems (Site/facility management contractors to which the CRD applies are listed in Attachment 3).

(2) This Notice does not automatically apply to other than site/facility management contractors. Any application of requirements of this Notice to other than site/facility management contractors will be communicated separately.

(3) Lead Program Secretarial Officers are responsible for telling their appropriate contracting officers which site/facility management contractors are affected by this Notice. Once notified, contracting officers are responsible for incorporating the CRD into contracts of affected site/facility management contractors via the laws, regulations, and DOE directives clause of their contracts.

(4) As the laws, regulations, and doe directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

(b) Contractors must not flow down requirements to subcontractors unnecessarily or imprudently. That is, contractors will—

1 Ensure that they and their subcontractors comply with the requirements of the CRD; and

2 incur only costs that would be incurred by a prudent person in the conduct of competitive business.

c. Exclusions.

(1) Consistent with the responsibilities identified in Executive Order (E.O.) 12344, dated February 1, 1982, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Notice for activities under the Deputy Administrator's cognizance.

(2) The requirements set forth in this Notice are not applicable to media that have been used to process Special Access Program information or Sensitive Compartmented Information.

4. REQUIREMENTS.

a. Implementation. Primary DOE Organizations must implement the requirements and meet the responsibilities defined in this Notice within 90 days of its issuance. Requirements and responsibilities will flow down from the heads of Primary DOE Organizations to all organizational levels.

b. Clearing. See Attachment 4 for definitions of terms used in this Notice.

(1) Depending upon authorized need to know, media that will be reused at the same or a higher classification level must be cleared.

(2) Overwriting is an acceptable method for clearing media. The approved procedure is to overwrite all locations three times—

(a) the first time with a character,

(b) the second time with its complement, and

(c) the third time with a random character.

(3) Only approved overwriting software that is compatible with the specific hardware intended for overwriting will be used. Use of such software will be coordinated in advance with the owner of the data.

(4) The designated approving authority (DAA) must approve all products used to perform overwrites.

(5) Cleared media that contained classified information must be protected by measures commensurate with the highest level of information it contained.

c. Sanitizing.

(1) Media that will be reused at a lower classification level or released from a classified environment must be sanitized.

(2) Media that will be released from a DOE-controlled environment must be sanitized.

(3) Individuals involved in clearing or sanitizing computer equipment must also certify that the process has been successfully completed by

affixing to the equipment a signed label verifying that the equipment has been sanitized. At minimum, labels must—

(a) describe the equipment;

(b) provide a statement indicating that the equipment has been cleared and/or sanitized in accordance with requirements of this Notice; and

(c) include the date, the printed name, and the signature of the certifier.

(4) The certifier must prepare separate documentation recording the same information and submit it to the Departmental element, which must maintain the documentation for a minimum of 5 years.

d. Destroying.

(1) Media that is no longer being used and that contains or did contain classified information must be destroyed.

(2) When classified matter is to be destroyed, it must be sufficiently destroyed to preclude any of the information it contained being recovered.

(3) Media which contained classified information must first be sanitized before being destroyed.

(4) Methods for destroying media are pulverizing, smelting, incinerating, disintegrating, applying acid solutions, etc., as approved by the DAA in accordance with national security policy.

e. Department of Energy Approved Procedures. DOE-approved procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and other related hardware that have been used to process, store, or contain classified information are listed in Appendix A of Attachment 2 to this Notice. Decisions to clear, sanitize, or destroy information system storage media, memory, and other related hardware should be based on cost-effectiveness.

f. Reusing Classified Media in Unclassified Environments. When nonremovable classified media (computer hard drives, etc.) are no longer required for use in classified environments (as determined by local site management), the media can be sanitized with specific overwrites and reused in unclassified environments within the same security area. This procedure is intended to be

used in conjunction with the accreditation of information systems at lower security levels.

(1) The unclassified media must be in a DOE-controlled environment.

(2) The media must not leave the controlled environment without first being destroyed.

(3) The decision to reuse media at a lower classification level may be acceptable if formal risk and cost analyses are conducted and the results of these analyses and testing of the implemented procedures verify that the national security of the United States is not adversely affected. Such analyses and decisions must be approved by heads of Departmental elements.

(4) Media are to be sanitized by overwriting using the three-step process described in Appendix A of Attachment 2.

(5) Sanitizing software must provide information about sectors overwritten and bad sectors that cannot be overwritten.

(6) The DAA must approve all products used to perform overwrites.[1]

(7) Media containing classified information designated for reuse by local site management must be sanitized. The information systems security officer (ISSO) or designee must approve overwrite methods and review the results of overwrites to verify that the method used completely overwrote all classified information.

(8) Once sanitized, media must be conspicuously marked to indicate that it once contained classified information. The media must be protected to ensure that it does not leave the controlled environment without first being destroyed.

(9) Personal computer diskettes or any other types of removable media that have contained classified information may not be reused in any unclassified system or environment.

g. Sanitizing Partially Contaminated Media.

(1) If nonremovable storage media operated in unclassified environments become contaminated with relatively small amounts of classified information (less than 20 kilobytes of information and less than 0.01

[1]The DOE Cyber Forensics Lab is available, at no charge, to assist with the verification of the sanitization of media.

percent of the capacity of the nonremovable media), the only the affected areas need to be sanitized using the process listed in Appendix A of Attachment 2.

(2) The DAA must approve all products used to perform overwrites.

(3) The ISSO or designee must approve overwrite methods and review the results of overwrites to verify that the methods used completely overwrote all classified information.

(4) If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, the media must be treated as if it had been used in classified environments, meaning that it must be completely sanitized in accordance with the procedures listed in Appendix A of Attachment 2.

(5) The programs used to overwrite contaminated media must overwrite all addressable locations, including temporary data file locations, file slack, free space, and directories and must provide confirmation of overwrite of specified areas and of successful completion.

(6) For networked systems that have become partially contaminated, the following requirements apply.

(a) If the contamination is less than 20 kilobytes of information and less than 0.01 percent of the capacity of the nonremovable media, then only the affected areas of the contaminated systems need to be sanitized using the process listed in Appendix A of Attachment 2.

(b) If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, then all affected systems must be completely sanitized in accordance with the procedures listed in Appendix A of Attachment 2.

(c) Personal computer diskettes or any other types of removable media that have become contaminated with classified information must be sanitized in accordance with the procedures listed in Appendix A of Attachment 2.

h. Clearing and Sanitizing Unclassified Computer Equipment.

(1) All Primary DOE Organizations must have plans to sanitize and clear DOE computer equipment and must define those plans in their respective program cyber security plans (PCSPs).

(2) All Primary DOE Organizations must describe the requirements for implementing their clearing/sanitizing plans in their respective cyber security program plans (CSPPs), including requirements for documented methods to independently verify clearing/sanitizing results.

(3) Before DOE-owned or DOE-managed hard drives or systems containing hard disks are transferred internally, they must be cleared. This requirement also applies to equipment used for DOE support.

(4) Systems or equipment declared surplus or donated to outside organizations must be sanitized.

(5) One-pass overwrites are sufficient for clearing unclassified computer media not containing sensitive information [e.g., Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), and Official Use Only (OUO)].

(6) A minimum of three-pass overwrites are required for sanitizing unclassified computer media which contained sensitive information (UCNI, NNPI, OUO).

(7) Overwritten hard drives intended for disposal, donation, or internal transfer must be sampled on a random basis to verify that the overwriting process has been successfully completed.

(a) Sampling/verifying must be conducted by trained individuals other than those who performed the overwrites.

(b) No fewer than 10 percent of all overwritten hard drives will be examined in the sampling process.

(c) Requirements for overwrite training, sampling overwritten hard drives, and verifying the overwriting process must be established in Departmental elements' PCSPs and CSPPs.

(8) Once computer equipment has been cleared and/or sanitized, the individuals performing the actions must prepare documentation that includes—

(a) descriptions of the media (serial numbers, makes, models),

(b) classification levels,

(c) purposes for clearing and/or sanitizing, and

(d) procedures used.

i. Training.

(1) All personnel from DOE organizations must be trained on the risks associated with disclosure of sensitive information and requirements for removing sensitive information from storage media, memory devices, and related hardware.

(2) All personnel who are responsible for clearing and sanitizing Federal information system storage media, memory devices, and other hardware must receive training in techniques to check, verify, and determine that procedures to remove the information were effective.

(3) Local sanitization awareness must be addressed in each Primary DOE Organization's computer security training and awareness program.

5. RESPONSIBILITIES.

a. Office of the Chief Information Officer (OCIO).

(1) Responsible for all cyber security Policies, Orders, Manuals, and guidelines.

(2) Develops and maintains Department-wide policy and guidance for clearing, sanitizing, and destroying storage media, memory devices, and other hardware.

b. Office of Security.

(1) Develops media sanitization procedures in coordination with the OCIO to enable a consistent approach to preventing unauthorized access or disclosure of the Department's sensitive and classified information.

(2) Maintains an on-request service to validate that no recoverable information resides on samples of a DOE organization's sanitized devices.

c. Heads of Primary DOE Organizations (see Attachment 1). Note that except for item (1) below, authority for these actions may be reassigned.

(1) Establish controls to ensure that requirements of this Notice are implemented.

(2) Ensure that plans and procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware are incorporated into the organization's PCSPs and site CSPPs in a manner consistent with paragraph 4 and the CRD for this Notice.

(3) Ensure that personnel receive adequate training in both requirements set forth in this Notice and local sanitization procedures. Training plans are to be documented in organization PCSPs.

6. REFERENCES. The following public laws and policies, national standards and guidelines, and DOE directives provide relevant processes and procedures for implementing cyber security program requirements and guidance that may be helpful in implementing this Notice.

a. Atomic Energy Act of 1954, as amended.

b. National Computer Security Center (NCSC) TG-025, *A Guide to Understanding Data Remanence in Automated Information Systems,* dated September 1991.

c. National Security Agency, Information Systems Security Products and Services Catalogue, Degausser Products List.

d. OMB Circular A-130, *Management of Federal Information Resources,* dated November 2000, Appendix III.

e. Memorandum from the Office of Safeguards and Security, to Distribution, Clarification to DOE M 5639.6-1A, *Clearing, Sanitization and Destruction of Automated Information Systems (AIS) Storage Media, Memory and Hardware,* dated 9-30-98.

f. DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03.

7. CONTACT. Questions concerning this Notice should be directed to the Office of the Chief Information Officer, Office of Cyber Security, at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

PRIMARY DOE ORGANIZATIONS TO WHICH DOE N 205.12 IS APPLICABLE

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Security
Office of Security and Safety Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Independent Oversight and Performance Assurance
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE N 205.12, *Clearing, Sanitizing, and Destroying Federal Information System Storage Media, Memory Devices, and Other Hardware*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) and National Nuclear Security Administration contractors, with access to DOE information systems. Contractors must comply with the requirements listed in the CRD.

This CRD supplements requirements contained in the CRD for DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03, including requirements for cyber resource protection, risk management, program evaluation and cyber security plan development and maintenance. The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD.

Regardless of the performer of the work, the contractor is responsible for complying with and flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

STORAGE MEDIA REQUIREMENTS.

The requirements set forth in this CRD are not applicable to media that have been used to process Special Access Program information or Sensitive Compartmented Information.

1. CLEARING.

   a. Dependent upon authorized need to know, media that will be reused at the same or a higher classification level must be cleared.

   b. Overwriting is an acceptable method for clearing media. The approved overwrite procedure is to overwrite all locations three times—

      (1) the first time with a character,

      (2) the second time with its complement, and

      (3) the third time with a random character.

   c. Only approved overwriting software that is compatible with the specific hardware intended for overwriting will be used. Use of such software will be coordinated in advance with the owner of the data.

d. The designated approving authority (DAA), who must be a Federal employee, must approve all products used to perform overwrites.

e. Cleared media that contained classified information must be protected using measures commensurate with the highest level of information it contained.

2. SANITIZING.

a. Media that will be reused at a lower classification level or released from a classified environment must be sanitized.

b. Media that will be released from a DOE-controlled environment must be sanitized.

c. Individuals involved in clearing/sanitizing computer equipment must also certify that the process has been successfully completed by affixing to the equipment a signed label verifying that the equipment has been sanitized. At a minimum, the labels must—

(1) describe the equipment;

(2) provide a statement indicating that the equipment has been cleared and/or sanitized in accordance with this DOE N 205.12; and

(3) the date, the printed name, and the signature of the certifier.

d. The certifier must prepare separate documentation recording the same information and the contractor must maintain this documentation for a minimum of 5 years.

3. DESTROYING.

a. Media that is no longer being used and that contains or did contain classified information must be destroyed.

b. When classified matter is to be destroyed, it must be sufficiently destroyed to preclude any of the information it contained being recovered.

c. Media which contained classified information must first be sanitized before being destroyed.

d. Methods for destroying media are pulverizing, smelting, incinerating, disintegrating, applying acid solutions, etc., as approved by the DAA in accordance with national security policy.

4. DEPARTMENT OF ENERGY-APPROVED PROCEDURES. DOE-approved procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware that have been used to process, store, or contain classified information are listed in appendix a of this CRD. Decisions to clear, sanitize,

or destroy information system storage media, memory, and other related hardware should be based on cost effectiveness.

5. REUSING CLASSIFIED MEDIA IN UNCLASSIFIED ENVIRONMENTS.

When nonremovable classified media such as computer hard drives is no longer required for use in classified environments (as determined by local site management), the media can be sanitized with specific overwrites and reused in unclassified environments within the same security area. This procedure is intended to be used in conjunction with the accreditation of information systems at a lower security level.

a. The unclassified environments must be in a DOE controlled environment.

b. The media must not leave the controlled environment without first being destroyed.

c. The decision to reuse media at a lower classification level may be acceptable if formal risk and cost analyses are conducted and the results of these analyses and testing of the implemented procedures verify that the national security of the United States is not adversely affected. Such analyses and decisions must be approved by heads of Departmental elements. Media are to be sanitized by overwriting the entire media using the three-step process described in paragraph 1a(2) of this CRD.

(1) Sanitizing software must provide information about sectors overwritten and bad sectors that cannot be overwritten.

(2) The DAA must approve all products used to perform overwrites.[1]

d. Media containing classified information, designated for reuse by local site management, must be sanitized. The contractor's lead system security officer must approve overwrite methodologies and review the results of overwrites to verify that the methodology used completely overwrote all classified information.

e. Once sanitized, media must be conspicuously marked to indicate that they once contained classified information and be protected to ensure the media do not leave the controlled environment without first being destroyed.

f. Personal computer diskettes or any other type of removable media that have contained classified information may not be reused in any unclassified system or environment.

[1]The DOE Cyber Forensics Lab is available, at no charge, to assist with the verification of the sanitization of media.

6. SANITIZING PARTIALLY CONTAMINATED MEDIA.

a. If nonremovable storage media operated in unclassified environments become contaminated with relatively small amounts of classified information (less than 20 kilobytes of information and less than 0.01 percent of the capacity of the nonremovable media), the affected areas may be sanitized using the three-step process described in paragraph 1a(2) of this CRD.

b. The DAA must approve all products used to perform overwrites.

c. The contractor's lead system security officer must approve overwrite methods and review the results of overwrites to verify that the method used completely overwrote all classified information.

d. If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, the media must be treated as if it had been used in classified environments, meaning that it must be completely sanitized in accordance with the procedures listed in Appendix A of this CRD.

e. The programs used to overwrite contaminated media must overwrite all addressable locations, including temporary data file locations, file slack, free space, and directories, and provide confirmation of overwrite of specified areas and of successful completion.

f. For networked systems that have become partially contaminated, the following requirements apply.

(1) If the contamination is less than 20 kilobytes of information and less than 0.01 percent of the capacity of the nonremovable media, then the affected areas of the contaminated systems may be sanitized using the three-step process listed in paragraph 1a(2) of this CRD.

(2) If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, then all affected systems must be sanitized in accordance with the procedures listed in Appendix A of this CRD.

(3) Personal computer diskettes or any other type of removable media that have become contaminated with classified information must be sanitized in accordance with the procedures listed in Table 1 of Appendix A.

7. CLEARING AND SANITIZING UNCLASSIFIED COMPUTER EQUIPMENT.

a. The contractor must describe the requirements for implementing their clearing/sanitizing plans in their respective cyber security program plans (CSPPs),

including the requirement for documented methods for independently verifying the clearing/sanitizing results.

b. Before any DOE-owned or DOE-managed hard disks or systems containing hard disks are transferred internally, they must be cleared. This requirement also applies to equipment used for DOE support.

c. Systems or equipment declared surplus or donated to outside organizations must be sanitized.

d. One-pass overwrites are sufficient for clearing unclassified computer media not containing sensitive information [e.g.; Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), and Official Use Only (OUO)].

e. A minimum of three-pass overwrites are required for sanitizing unclassified computer media which contained sensitive information (UCNI, NNPI, OUO).

f. Overwritten hard drives intended for disposal, donation, or internal transfer must be sampled on a random basis to verify that the overwriting process has been successfully completed.

(1) Sampling/verifying must be conducted by trained individuals other than the ones who performed the overwrites.

(2) No fewer than 10 percent of all overwritten hard drives will be examined in the sampling process.

(3) Requirements for overwrite training, sampling overwritten hard drives, and verifying the overwriting process must be established in the contractor's CSPP.

g. Once computer equipment has been cleared and/or sanitized, the individuals performing the actions must prepare documentation that includes—

(1) descriptions of the media (serial numbers, makes, models),

(2) classification levels,

(3) purposes for clearing and/or sanitizing, and

(4) procedures used.

8. TRAINING.

a. All contractor personnel must be trained on the risks associated with disclosure of sensitive information and requirements for removing sensitive information from storage media, memory devices, and related hardware.

b. All contractor personnel who are responsible for clearing and sanitizing Federal information system storage media, memory devices, and other hardware must receive training in techniques to check, verify, and determine that procedures to remove the information were effective.

APPENDIX A

TABLE 1. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZING, AND DESTROYING STORAGE MEDIA*

MEDIA TYPE†	CLEARING‡	SANITIZING‡	DESTROYING‡
Magnetic Tapes			
Type I	1 or 2	1 or 2	4
Type II	1 or 2	2	4
Type III	1 or 2	X	4
Magnetic Disks			
Floppies, Zip drives	1, 2, or 3	X	4
Bernoulli Boxes	1, 2, or 3	X	4
Removable Hard Disks	1, 2, or 3	1, 2, or 3	4 or 5
Nonremovable Hard Disks	3	1, 2, or 3	4 or 5
Optical Disks			
Magneto-optical: Read Only	X	X	4
Write Once, Read Many (WORM)	X	X	4
Read Many, Write Many	3	X	4
Other			
Floptical	X	X	4
Helical-scan Tapes	X	X	4
Cartridges	X	X	4
Optical	X	X	4

*Procedures listed are for storage media that have been used to process and/or store/contain classified information.

†Program offices are responsible for developing cleaning, sanitizing, and destroying procedures for media types not listed.

‡Numbers in the table refer to the procedures listed

§All degaussing products used to clear or sanitize media **must** be certified by the National Security Agency (NSA) and be listed on the Degausser Products List of the NSA *Information Systems Security Products and Services Catalogue*.

Procedures: †

1. Degauss with a Type 1 degausser.§
2. Degauss with a Type 2 degausser.§
3. Overwrite all locations with a character, its complement, then with a random character.
4. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
5. Remove the entire recording surfaces by sanding or applying acid.

X. No procedure authorized.

TABLE 2. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZING, AND DESTROYING ELECTRONIC MEMORY DEVICES*

MEDIA TYPE†	CLEARING†	SANITIZING‡	DESTROYING‡
Magnetic Bubble Memory	3	1, 2, or 3	11
Magnetic Core Memory	3	1, 2, or 3	11
Magnetic Plated Wire	3	3 and 4	11
Magnetic-Resistive Memory	3	X	11
Read-Only Memory (ROM)	X	X	11 (see 12)
Random Access Memory (RAM) (Volatile)	3 or 5	5, then 10	11
Programmable ROM (PROM)	X	X	11
Erasable PROM (UV PROM)	6	7, then 3 and 10	11
Electrically Alterable PROM (EAPROM)	8	8, then 3 and 10	11
Electrically Erasable PROM (EEPROM)	9	9, then 3 and 10	11
Flash Erasable PROM (FEPROM)	9	9, then 3 and 10	11

*The procedures listed are for electronic memory devices that have been used to process and/or store/contain classified information.

†Program offices are responsible for developing cleaning, sanitizing, and destroying procedures for media types not listed.

‡Numbers refer to the numbers in the procedures listed.

§All degaussing products used to clear or sanitize media **must** be certified by the National Security Agency (NSA) and be listed on the Degausser Products List of the NSA *Information Systems Security Products and Services Catalogue*.

Procedures:‡

1. Degauss with a Type 1 degausser. §
2. Degauss with a Type 2 degausser.§
3. Overwrite all locations with a character, its complement, then with a random character.
4. Sanitization is not authorized if data resided in same location for more than 72 hours; sanitization is not complete until each overwrite has resided in memory for a period longer than the classified data resided in memory.
5. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.
6. Perform an ultraviolet erase according to manufacturer's recommendation.
7. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
8. Pulse all gates. 9. Perform a full chip erase (see manufacturer's data sheet for procedure).
9. Check with ISSO or designee to determine whether additional procedures are required.
10. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
11. Destruction required only if ROM contained a classified algorithm or classified data.

X. No procedure authorized.

TABLE 3. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZING, AND DESTROYING HARDWARE*

MEDIA TYPE†	CLEARING‡	SANITIZING‡	DESTROYING‡
Printer Ribbons	1	1	6
Platens	X	2	6
Toner Cartridges	3	3	X
Laser Drums	4	3	6
Cathode-Ray Tubes (If there is Classified Burn-In)	X	X	6
Fax Machines	5	5	6

*The procedures listed are for hardware that have been used to process and/or store/contain classified information.
†Program offices are responsible for developing cleaning, sanitizing, and destroying procedures for media types not listed.
‡Numbers refer to the numbers in the procedures listed.

Procedures: †

1. Overwrite at least five consecutive times with unclassified data.
2. Chemically clean so no visible trace of data remains.
3. Print at least five pages of randomly generated unclassified data. The pages should not include any blank spaces or solid black areas.
4. Print three blank copies. If unable to get a clean output, print an unclassified test pattern or black copy; then run three blank copies.
5. For fax machines that have memory and other storage media incorporated, treat each component per procedures listed in tables 1 and 2 of this appendix.
6. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media is physically destroyed.

X. Not applicable.

Note: All copies printed for clearing and sanitization purposes must be destroyed as classified waste.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The Contractor Requirements Document for DOE N 205.12 is intended to apply to the site/facility management contracts applicable to the following sites/facilities.

Lawrence Berkeley National Laboratory

Pacific Northwest National Laboratory

Brookhaven National Laboratory

Sandia National Laboratories

National Renewable Energy Laboratory

Stanford Linear Accelerator Center

Bettis Atomic Power Laboratory

Argonne National Laboratory

Idaho National Engineering & Environmental Laboratory

Thomas Jefferson Nat'l Accelerator Facility

Ames National Laboratory

Oak Ridge National Laboratory

Knolls Atomic Power Laboratory

Lawrence Livermore National Laboratory

Los Alamos National Laboratory

Savannah River Site

Princeton Plasma Physics Laboratory

Fermi National Accelerator Center

West Valley Project

Strategic Petroleum Reserve

Oak Ridge Y-12 National Security Complex

Pantex Plant

Waste Isolation Pilot Plant

Nevada Test Site

Kansas City Plant

National Civilian Radioactive Waste Program (Yucca Mountain)

Hanford Environmental Restoration

Oak Ridge Environmental Management

Mound Environmental Management Project

Project Hanford

River Protection Project Tank Farm Management

Rocky Flats

Fernald Environmental Management Project

Grand Junction Technical & Remediation Services

Grand Junction Facilities & Operations Services

Oak Ridge Institute of Science & Education

Occupational Health Services at the Hanford Site

DEFINITIONS

Clearing. The process of eradicating data on media before reusing it in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory will be cleared to effectively deny access to previously shared information.

Degauss. To reduce magnetic induction to 0 (zero) by applying a reverse magnetizing field.

Degausser. A device that removes data from a storage medium by removing magnetism.

DOE-controlled environment. An area within DOE-controlled premises or within DOE contractor-controlled premises.

Internally transferred. Computer equipment that is to be transferred within DOE, but outside the direct line of authority (i.e., outside of an organizational department). For example, a computer with a hard disk in the Office of Cyber Security may be transferred to another person within the Office of Cyber Security without being cleared, but if it were to be transferred to someone in DOE but outside of the Office of Cyber Security, it must be cleared first.

Nonremovable media. Fixed storage devices, such as hard drives, which provide internal information/data storage.

Removable media. Media that is not attached to information systems via the internal buss of the information system.

Overwriting. A procedure to destroy data from storage media by recording patterns of meaningless data over that which is stored on the media. The approved overwrite procedure is to overwrite all locations three times—the first time with a character, the second time with its complement, and the third time with a random character. For example, overwrite first with "00110101," followed by "11001010," and then "10101101."

Sanitization. The process of removing the data from media before it is reused in an environment that does not provide an acceptable level of protection for the data that was stored in the media before sanitizing. Information system resources will be sanitized before they are released from classified information controls or released for use at lower classification levels.

APPENDIX B – GLOSSARY

allocation block – When space on a disk is allocated to a file, it is not allocated sector by sector but in a larger quantity called the allocation block. Allocation blocks consist of some even number of sectors. When a file is created it is given one allocation block. When it fills that allocation block it is given another.

ASCII – A 256 character code set for representing printed characters. The first 128 characters consist of the upper and lower case Arabic letters, numbers, punctuation, and control codes. See also UNICODE.

bad sector – A sector that cannot be reliably written and read on the disk. Bad sectors are either marked by the drive so they cannot be used or marked by the system so it will not attempt to use them. Many drives remap bad sectors found after the drive was formatted to spare sectors on the drive.

BCWipe – A commercial program from Jetico, Inc. for sanitizing disk drives. See References.

clearing – Erasing the data so that it cannot be retrieved by keyboard commands, such as running an "undelete" program. Clearing protects information from a keyboard attack but not a laboratory attack.

complement of a character – A complement of a character is a character where the binary 1s and 0s are reversed. For example, the letter A is represented in most systems as the hex character 41. The binary representation of a 41 is 0100 0001. The complement is, 1011 1110, which is the hex character BD. Thus, hex characters 14 and BD are complements of each other. The hex character BD has no letter equivalent. The hex characters range from 00 (binary 0000 0000) through FF (1111 1111).

DAA – See Designated Approving Authority.

degaussing – Passing a strong magnetic field through magnetic media to change the alignment of magnetic domains and erase any information contained in that magnetic alignment. Two types of degaussing are DC and AC. DC degaussing uses a strong, fixed magnetic field to make all the domains align in the same direction. AC degaussing uses an alternating field to scramble the magnetic domains in all different directions.

Designated Approving Authority – A DOE person who may accredit an information processing system as being in compliance with the DOE orders.

destruction – Physically destroying the magnetic recording medium such that there is no possibility of recovering the data by any means. Destruction assures you that there is no way that information could ever be recovered from the drive.

directory or directory file – A file on disk that contains the names of files, information about the file and a pointer to the block on disk that is the first block in the file.

Disk Probe – A commercial program from Microsoft for reading and searching a drive sector by sector. See References.

DiskEdit – A commercial program from Norton for reading and searching a drive sector by sector. See References.

Double Deletion – Deleting a file and emptying the trash. This process does not clear the contents of a file from a drive.

end-of-file marker – A number stored in a file that indicates where in the last block of a file the last piece of data was written. It actually points to the byte that is one beyond the last byte written to the file. See also slack space.

FAT – See file allocation table.

FAT12, FAT16, FAT32 – The file system used on DOS and Windows 95/98/ME systems. It was designed for a single user system and has no built-in file protections. See also NTFS.

file allocation table – A table on a disk that keeps track of which allocation blocks are used and which are available to be allocated to new files.

free space – The space on a disk drive that is not allocated to any file. That is, it is free to be used by any file that needs it. The blocks used by deleted files become part of the free space.

Gdisk – A commercial program from Norton for sanitizing whole disk drives. Part of the Norton Ghost package. See References.

government overwrite – This overwrite depends on whose definition you are using. DOE, DoD, NSA, all specify slightly different combinations of overwriting. The most common is to do a three times overwrite using a character, the character's complement, and another character. DOE specifies hex 00 and hex FF as the character and its complement and a randomly chosen character for the last overwrite. DoD specifies a randomly chosen character and its complement with hex 00 used for the last overwrite. Some DoD specs also say to use three characters and their complements and then a sequence of random characters for a total of seven overwrites.

Gutmann overwrite – An overwrite method based on the work of Peter Gutmann (see References). It is a 35 times overwrite with different characters, patterns and random characters and represents about the theoretical best you can do by overwriting.

hex characters – Base 16 numbers that correspond to one byte characters. One byte is coded as two hex digits between 00 and FF. For example, hex 61 is the letter "a" and hex 3F is the question mark "?". These one byte characters are how computers store text. A one byte character can code up to 255 distinct alphabetic characters, numbers, and punctuation. ASCII character coding defines the first 128 characters as the standard alphabetic characters in upper and lower case, the 10 numeric digits, punctuation, and control characters. Other codings generally use the ASCII standard for the lower 128 characters but code different characters with the second 128 codes. An extension of this to two byte characters is called Unicode and is needed for many Asian languages that have more than 255 characters.

hibernation file – A disk file where a computer stores the contents of memory when it changes into hibernation mode.

hibernation mode – A method by which a computer (usually a laptop) saves power by stopping execution, writing the contents of memory to a disk file, and then turning off. When a hibernating system wakes up, it copies the data back into memory and resumes where it left off.

index tracks – Special tracks written on one platter of a disk drive to guide the other heads on the drive to the data. Tracks are placed so closely together on a modern drive that the drive's heads need to be actively aligned to keep them on the data. Some modern drives use one head and one side of one platter to do the alignment that keeps all the other heads aligned with the tracks. Index tracks are generally not written by a drive but are created at the factory when a drive is built. If the index tracks are erased a drive cannot be used.

ISOM – Information Systems Security Operations Manager. A person at a DOE area office who is in charge of classified information systems under the control of that area office.

ISPM – Information Systems Security Program Manager. A person at DOE headquarters who is in charge of classified information systems throughout DOE.

ISSM – Information Systems Security Site Manager. A person who is in charge of classified information systems at a single DOE site.

keyboard attack – An attempt by an unauthorized person to obtain information from a system using only keyboard commands.

laboratory attack – An attempt by an unauthorized person to obtain information from a hard drive where the hard drive can be removed from the system and special electronics and other devices can be used to extract the information.

magnetic media – media that stores information using magnetic recording methods such as hard drives, floppy drives, and magnetic tape.

make – A UNIX utility for compiling and linking a program.

mu metal – A special metal that strongly attracts magnetic fields. Magnetic fields pass through metals like aluminum with little distortion. Mu metal pulls magnetic field lines into the metal instead of letting them pass through and is used for magnetic shielding. Mu-metal is a nickel-iron alloy (77% nickel, 15% iron, plus copper and molybdenum).

Naval Nuclear Propulsion Information (NNPI) – Any information concerning the design, manufacture, use, repair, etc. of naval nuclear propulsion systems.

NNPI – See Naval Nuclear Propulsion Information.

NTFS – The file system used on Windows NT/2000/XP systems. It was designed for a multi-user system and has built-in file protections that key to the authenticated user.

Official Use Only (OUO) – A broad category of unclassified information based on the exemption categories in the Freedom of Information Act including: personnel data (Social Security numbers and home phone numbers), medical data, financial data, CRADA information, proprietary data, and export controlled data.

OUO – See Official Use Only

overwriting – The act of writing new data on top of the old data on a hard drive to replace that old data and make it unrecoverable. Also known as scrubbing or wiping though scrubbing and wiping may include more than one pass of overwriting.

page file – A file used to store programs that are not currently running so that programs that are running have more memory to use. Also called a swap file.

pass – overwriting data one time.

RAID - Redundant Array of Independent Disks. This was originally known as Redundant Array of Inexpensive Disks. RAID is a method of combining multiple disks into what appears to be a single large disk. Data written to the RAID disks is spread across the multiple disks to increase the speed at which data can be transferred. RAID can also contain redundant copies of the data to make it possible to quickly and automatically recover information that was on a failed disk.

sanitizing – Erasing the data such that it cannot be recovered by any means without actually destroying the media. Note that some media, such as hard drives, cannot be sanitized without damaging the drive. Sanitization protects information from a laboratory attack but you cannot be absolutely assured that you have gotten every bit of classified information.

Scrub – A utility program written by the Lawrence Livermore National Laboratory for sanitizing disk drives on UNIX type operating systems. See References.

scrubbing – see overwriting.

sectors – A piece of a track on a disk drive. The smallest chunk of data that can be written or read from a disk drive. Data is not read or written to a disk drive a byte at a time but is done in chunks called sectors. To write less than a sectors worth of data you write the data into a sector sized buffer in memory and then write the whole buffer to the disk drive. The normal size of a sector is 512 bytes of data plus some header information.

slack space – The part of a file in the last allocation block between the file's end-of-file marker and the end of the last block in the file. Slack space generally contains whatever was on the disk before that space was allocated to the file. It could contain the contents of a previous file that was deleted.

swap file – see page file.

UCNI – see Unclassified Controlled Nuclear Information.

Unclassified Controlled Nuclear Information (UCNI) – Information concerning the production and protection of controlled nuclear material, and the design, production, and use of unclassified nuclear weapons components.

UNICODE – A two byte code for representing printed characters. The original, one byte ASCII code can only represent 256 characters which is insufficient for most printed Asian languages. UNICODE extends ASCII to allow it to handle more languages. The first 128 UNICODE characters are the one byte ASCII character codes followed by zeros.

WipeInfo – A commercial program from Norton for sanitizing disk drives.

wiping – see overwriting.

APPENDIX C TABLE OF HEX CODES AND THEIR COMPLEMENTS.

The following table contains the decimal and hexadecimal values for single byte codes and their complements for use in the overwriting programs. Most overwrite schemes require you to pick a value and its complement as two of the overwrites.

Character		Complement	
Decimal	Hex	Decimal	Hex
0	00	255	FF
1	01	254	FE
2	02	253	FD
3	03	252	FC
4	04	251	FB
5	05	250	FA
6	06	249	F9
7	07	248	F8
8	08	247	F7
9	09	246	F6
10	0A	245	F5
11	0B	244	F4
12	0C	243	F3
13	0D	242	F2
14	0E	241	F1
15	0F	240	F0
16	10	239	EF
17	11	238	EE
18	12	237	ED
19	13	236	EC
20	14	235	EB
21	15	234	EA
22	16	233	E9
23	17	232	E8
24	18	231	E7
25	19	230	E6
26	1A	229	E5
27	1B	228	E4
28	1C	227	E3
29	1D	226	E2
30	1E	225	E1
31	1F	224	E0
32	20	223	DF
33	21	222	DE
34	22	221	DD

Character		Complement	
Decimal	Hex	Decimal	Hex
35	23	220	DC
36	24	219	DB
37	25	218	DA
38	26	217	D9
39	27	216	D8
40	28	215	D7
41	29	214	D6
42	2A	213	D5
43	2B	212	D4
44	2C	211	D3
45	2D	210	D2
46	2E	209	D1
47	2F	208	D0
48	30	207	CF
49	31	206	CE
50	32	205	CD
51	33	204	CC
52	34	203	CB
53	35	202	CA
54	36	201	C9
55	37	200	C8
56	38	199	C7
57	39	198	C6
58	3A	197	C5
59	3B	196	C4
60	3C	195	C3
61	3D	194	C2
62	3E	193	C1
63	3F	192	C0
64	40	191	BF
65	41	190	BE
66	42	189	BD
67	43	188	BC
68	44	187	BB
69	45	186	BA

Character		Complement	
Decimal	Hex	Decimal	Hex
70	46	185	B9
71	47	184	B8
72	48	183	B7
73	49	182	B6
74	4A	181	B5
75	4B	180	B4
76	4C	179	B3
77	4D	178	B2
78	4E	177	B1
79	4F	176	B0
80	50	175	AF
81	51	174	AE
82	52	173	AD
83	53	172	AC
84	54	171	AB
85	55	170	AA
86	56	169	A9
87	57	168	A8
88	58	167	A7
89	59	166	A6
90	5A	165	A5
91	5B	164	A4
92	5C	163	A3
93	5D	162	A2
94	5E	161	A1
95	5F	160	A0
96	60	159	9F
97	61	158	9E
98	62	157	9D
99	63	156	9C
100	64	155	9B
101	65	154	9A
102	66	153	99
103	67	152	98
104	68	151	97
105	69	150	96
106	6A	149	95
107	6B	148	94
108	6C	147	93
109	6D	146	92
110	6E	145	91
111	6F	144	90
112	70	143	8F

Character		Complement	
Decimal	Hex	Decimal	Hex
113	71	142	8E
114	72	141	8D
115	73	140	8C
116	74	139	8B
117	75	138	8A
118	76	137	89
119	77	136	88
120	78	135	87
121	79	134	86
122	7A	133	85
123	7B	132	84
124	7C	131	83
125	7D	130	82
126	7E	129	81
127	7F	128	80
128	80	127	7F
129	81	126	7E
130	82	125	7D
131	83	124	7C
132	84	123	7B
133	85	122	7A
134	86	121	79
135	87	120	78
136	88	119	77
137	89	118	76
138	8A	117	75
139	8B	116	74
140	8C	115	73
141	8D	114	72
142	8E	113	71
143	8F	112	70
144	90	111	6F
145	91	110	6E
146	92	109	6D
147	93	108	6C
148	94	107	6B
149	95	106	6A
150	96	105	69
151	97	104	68
152	98	103	67
153	99	102	66
154	9A	101	65
155	9B	100	64

Character		Complement	
Decimal	Hex	Decimal	Hex
156	9C	99	63
157	9D	98	62
158	9E	97	61
159	9F	96	60
160	A0	95	5F
161	A1	94	5E
162	A2	93	5D
163	A3	92	5C
164	A4	91	5B
165	A5	90	5A
166	A6	89	59
167	A7	88	58
168	A8	87	57
169	A9	86	56
170	AA	85	55
171	AB	84	54
172	AC	83	53
173	AD	82	52
174	AE	81	51
175	AF	80	50
176	B0	79	4F
177	B1	78	4E
178	B2	77	4D
179	B3	76	4C
180	B4	75	4B
181	B5	74	4A
182	B6	73	49
183	B7	72	48
184	B8	71	47
185	B9	70	46
186	BA	69	45
187	BB	68	44
188	BC	67	43
189	BD	66	42
190	BE	65	41
191	BF	64	40
192	C0	63	3F
193	C1	62	3E
194	C2	61	3D
195	C3	60	3C
196	C4	59	3B
197	C5	58	3A
198	C6	57	39

Character		Complement	
Decimal	Hex	Decimal	Hex
199	C7	56	38
200	C8	55	37
201	C9	54	36
202	CA	53	35
203	CB	52	34
204	CC	51	33
205	CD	50	32
206	CE	49	31
207	CF	48	30
208	D0	47	2F
209	D1	46	2E
210	D2	45	2D
211	D3	44	2C
212	D4	43	2B
213	D5	42	2A
214	D6	41	29
215	D7	40	28
216	D8	39	27
217	D9	38	26
218	DA	37	25
219	DB	36	24
220	DC	35	23
221	DD	34	22
222	DE	33	21
223	DF	32	20
224	E0	31	1F
225	E1	30	1E
226	E2	29	1D
227	E3	28	1C
228	E4	27	1B
229	E5	26	1A
230	E6	25	19
231	E7	24	18
232	E8	23	17
233	E9	22	16
234	EA	21	15
235	EB	20	14
236	EC	19	13
237	ED	18	12
238	EE	17	11
239	EF	16	10
240	F0	15	0F
241	F1	14	0E

Character		Complement	
Decimal	Hex	Decimal	Hex
242	F2	13	0D
243	F3	12	0C
244	F4	11	0B
245	F5	10	0A
246	F6	9	09
247	F7	8	08
248	F8	7	07

Character		Complement	
Decimal	Hex	Decimal	Hex
249	F9	6	06
250	FA	5	05
251	FB	4	04
252	FC	3	03
253	FD	2	02
254	FE	1	01
255	FF	0	00

Department of Energy

CIAC

Computer Incident Advisory Capability

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551