



## **Technical White Paper For Data Sanitization (eradication) of 3590, 9840, 9940 and LTO Cartridges**

### Government Recommendations

The (DoD) Department of Defense has been a standard for data centers and other companies when it comes to recommendations for protecting and destroying information that has been collected and stored on most forms of media.

The most recent DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) pertaining to magnetic media was updated and released January 1995. This document has just three classifications for Magnetic Tape.

### Type I

Is any magnetic tape that has a coercivity of 350 oersteds or less. This document states that Type I magnetic tape can only be sanitized for reuse by using approved degaussing equipment that erases the data on Type I tapes.

### Type II

Is any magnetic tape that has a coercivity between 351 and 750 oersteds. This document states that Type II magnetic tape can only be sanitized for reuse by using approved degaussing equipment that erases the data on Type II tapes.

### Type III

Is any magnetic tape that has a coercivity greater than 750 oersteds. This document states that Type III tape cannot be sanitized for reuse by degaussing but only sanitized thru destruction of the media. Destruction is further identified as crushing and/or incineration.

### What this meant for Data Centers

What this meant for most data centers at that time was, only open reel, 3480, 3490E, and some older versions of DLT tapes know as "TK" media could be reused (sanitized). This document excluded reusing many of the most popular tapes that were in use in 1995. For example DLT III, DLT IIIXT, DLT IV, 4mm, 8mm and many quarter inch (QIC) tapes were not addressed. This does not make sense due to the fact there was degaussing equipment available to sanitize (erase) these tapes. So data centers applied common sense to the DoD document to allow for situations that applied to their own media type being used.

The next major industry change included media types with a pre-written servo track(s) and/or prewritten header information. This changed the way tapes would or could be sanitized (erased) forever.

### Why is this an issue now?

A little history is necessary to understand the past and future technology. Prior to 1995, most large computer center tapes did not have prewritten servo tracks or prewritten information on tapes. This meant you could take a new tape or a previously used tape, completely degauss the tape (Graham's Tier 1 Eradication), mount it on a tape drive (initialize the tape if needed) and write data to the tape. This process could be repeated thousands of times without adversely affecting the media. At the same time tape libraries were continually increasing to satisfy the basic need for information, as well as new regulatory requirements. Data was being stored for longer periods of time. To help alleviate the ever growing library and data storage problem, a cry went out into the industry one more time asking for greater data density (store a lot more information in the same amount of space), faster transfer rates and better reliability. This essentially translated to many more (hundreds in some cases) tracks being written to that same basic half-inch tape. In order to accommodate that requirement, servo tracks were developed to electronically guide the tape across the write/read heads, as older mechanical methods were not effective with the number of tracks being used. As this occurred, enhanced electronic reconstruction of data was developed (often referred to as data correction) in order to maximize reliability.

The 3480 and 3490e data cartridges and drives had 18 and 36 tracks respectively. Then in 1995, IBM announced the 3590 cartridge and drive. This tape was different in that the tape had pre-written servo tracks from the factory. The first "3590 B" drive was capable of writing 128 tracks of data to a half inch 3590 tape. This was accomplished by writing 16 tracks at one time, making 8 passes up and down the tape in a parallel serpentine format following the three pre-written servo tracks. These servo tracks serve many purposes including calibration, timing, tape speed and the critical head alignment procedure. In a matter of speaking, the servo tracks became the nervous system of the 3590 tape cartridge. Without servo tracks the tape would cease to function. This is why warning labels arrived on and in the boxes of 3590 tapes stating that "degaussing of these cartridges would render them useless". Many data centers learned this lesson the hard way. As a manufacturer of 3590 cartridges, we would receive cases of tapes with the request to rewrite the servo tracks as someone had mistakenly degaussed (erased) them. At that time, this was not possible because the servo tracks are written in pancake form prior to the tape being loaded in the cartridges. Thousands of dollars of media had been rendered useless in a matter of seconds per tape until Graham Magnetics later developed an in-cartridge servo track writer. This same pre-written servo track technology is now used in most newer media products such as 9840, 9940, LTO, etc. in order to reach the recording levels demanded of them.

Now the dilemma: You have a tape that has 100's of gigabytes (GB) of sensitive data ranging from top-secret information to the company payroll containing names, addresses, phone numbers and Social Security numbers. The prior procedure to sanitize this information would render the cartridge useless but this is the only option according to the DoD because the tape coercivity is greater than 750 oersteds (3590 coercivity is 1600 Oe). The data center does not want to lose the investment they have made in the

cartridge (sometimes \$100.00 or more per tape). So they find in the DoD document that overwriting the entire tape was acceptable for Type II Magnetic Tapes and apply this same logic to Type III tapes. This is acceptable for many data centers and they have written this into their security procedures and policies (Graham's Tier 2 Eradication).

Other data centers like the solution, but they remember someone once said that even though the tape had been overwritten the data could be recovered from that tape. But, that is true only with older, low coercivity media where the signal did not saturate the media completely. This older low coercivity media also had other issues called "print through". This is when data written on adjacent layers or wraps on a reel of open reel tape affected the current layer of tape. This literally had the potential of changing the original data written to the tape and is part of why additional reliability was required in each new generation of media. With the higher coercivity tapes used now, the surfaces are completely saturated with a signal and adjacent layers have no effect on each other. So when the tape is being overwritten, all of the prior data is being completely eradicated. However, it should be noted that this only applies to the percentage of the tape that is actually being written to. Hence, the prior information written to a tape could be 10 GB of sensitive information but the next time the cartridge is used only 1 GB of information is written and 9 GB of the previous sensitive information is still unchanged on this tape. That data can be recovered by data recovery companies. This 9 GB of sensitive data can be and is a security issue to many data centers. Because of this, many companies cannot move tapes from one data center to another for fear that some of this sensitive data could fall into the wrong hands. As a result, millions of tapes have been destroyed because previous to Graham's process, data on these cartridges could not be effectively sanitized.

### Today's Environment

As was mentioned earlier each data center has a large investment in the media itself. When migrating to a different media, is that investment completely lost because of the security issues, or is there a way to sanitize the data and recover a part of that original investment in the media? With the new much higher cost of most new media, isn't there a better way for data centers to invoke "*Intelligent Asset Management*"?

Until earlier this year (2006), no one had an answer to this problem other than 100 percent over writing of the tape or destruction of the tape. Over writing the tape using the data center system could cost as much as the tape when new. A team of engineers at Graham Magnetics solved the problem by developing a system that completely eradicates the data tracks, leaving the original servo tracks untouched in a single pass using modified tape drives (the same drives that are used to write and read data to the tapes). This process not only sanitizes the data regions of the tape but also all other regions as well (information areas that the tape drive writes to that are only accessible to the tape drive). A 3590 "J" tape can be eradicated (sanitized) in under 5 minutes. A 9840 or LTO tape can be eradicated in under 2 minutes. All of this is done off line without the use of a computer (the modified drive only). After going through this eradication process tapes with servos can be moved and sent anywhere without the security danger, just like a new tape from the factory, making it possible, for the data center to utilize their investment in the media to their benefit. We call it "*Intelligent Asset Management*".

## Proven Sanitization Process

Many Graham customers have tested this process by providing Graham Magnetics with test sample of tapes. The tapes were processed through Graham's Tier 3 Eradication routine and returned to the customer for verification that the entire tape is now blank. When audit testing on their drives was conducted, the customers were unable to retrieve any of the data. The customers then sent the tapes to data recovery companies that specialize in difficult recovery projects, and once again, the tapes were determined to be blank. At least one company sent these tapes to Data Recovery International (DRI). They are known throughout the magnetic tape industry and data centers as one of the best data recovery companies. Bill King President of DRI commented, "I am impressed with this data eradication process because I can always find some data on the tape, but on these tapes not only did I find that data could not be recovered, it didn't even exist". Other data recovery companies have expressed the same results.

## Conclusion

Graham Magnetics has developed a new process using modified standard tape drives that set a new standard for data eradication, data sanitization and data destruction. This data eradication process and drives have been tested and validated by some of the largest financial data centers and data recovery companies in the world. These drives meet or exceed all requirements that could be imposed by the DoD and the NSA (National Security Agency) if these agencies were up to date.

## About the author:

Kevin Burton has over 30 years of experience with Magnetic Tape. He has worked for large data centers (Banks) in the mid-west, where he was in charge of improving system performance related to magnetic tape. He has been a Field Engineer repairing tape drives and related equipment. Kevin has traveled the world presenting technical seminars about magnetic tape technology, tape care and handling, disaster recovery and improving system performance. He has been in charge of data recovery projects involving thousands of tapes due to natural disasters (hurricanes and flooding), and ageing media problems from equipment failures. Kevin has been the Manager of Technical Services and is now the Manager over Quality Assurance and Engineering at Graham Magnetics. He has also served as a representative on the ANSI (American National Standards Institute) for the X3. (computer tape) committee.

November 21, 2006

## Definitions as they apply to computer tape

Coercivity, is the amount of work (force) necessary to change a bit (magnetizing force) from a one to zero on computer tape. The higher a magnetic tape's coercivity index, the more data it can store.

Oersted, is the unit of measurement of coercivity.

Sanitization, is the process of making sensitive information non-readable (overwrite the tape) and or eradicate the data to make it look like nothing was ever on the tape (degaussing, or erasing of the data on a tape).

Graham's Tier 1 Eradication: Completely degaussing the Media

Graham's Tier 2 Eradication: Over writing every possible bit position

Graham's Tier 3 Eradication: Completely eradicating the data tracks and leaving the original servo tracks untouched