MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

EFFECTIVELY IMPLEMENTING AND MANAGING ELECTRONIC DATA DISPOSAL AND DESTRUCTION

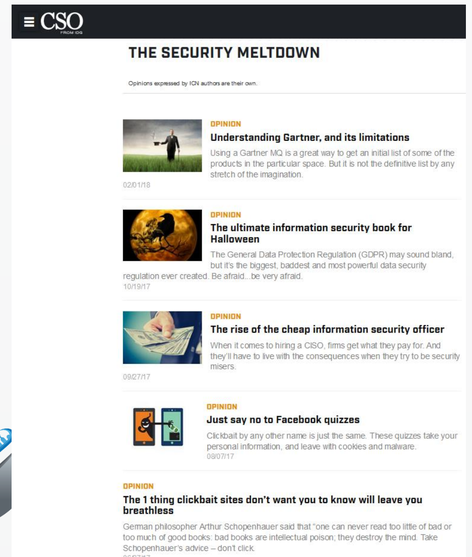
Ben Rothke, CISSP PCI QSA

Principal Security Consultant - Nettitude

@benrothke

ABOUT ME (SINCE YOU ASKED)

- Ben Rothke, CISSP + other certs
- Principal Security Consultant – Nettitude
- Author - Computer Security: 20 Things Every Employee Should Know
- Member: Cybersecurity Canon
  - https://www.paloaltonetworks.com/threat-research/cybercanon
- The Security Meltdown
  - https://www.csoonline.com/blog/the-security-meltdown



THE PROBLEM IS REAL – THERE IS NO FUD

Destroying digital footprints is an emerging business

January 11, 2014 10:57 PM

By Deborah M. Todd / Pittsburgh Post-Gazette

Calif. Assemblyman Mike Gatto Introduces Broad Government Data Privacy Bill

by **Christopher Simmons** on Tue, 14 Jan 2014

Like 1 Tweet 2 Pin it Share 3

SACRAMENTO, Calif. /California Newswire/ — Today, California Assemblyman Mike Gatto (D-Los Angeles) has introduced legislation to lessen the chances that government collection of "Big Data" jeopardizes the privacy of citizens. The broad mandate, AB 1442, would strengthen the notice requirements before the government gathers personal data and would require the prompt destruction of personal data when it is collected by a government entity.

Security gaps found in destruction of top-secret military data

Defence department overhauling policy on disposal of sensitive information after troubling audit

By Kathleen Harris, CBC News Posted: Jan 09, 2014 6:15 PM ET | Last Updated: Jan 09, 2014 6:15 PM ET

Footage released of Guardian editors destroying Snowden hard drives

GCHQ technicians watched as journalists took angle grinders and drills to computers after weeks of tense negotiations

- Watch the footage of the hard drives being destroyed

U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquires

Inspection Report

Internal Controls over Computer Hard Drives at the Oak Ridge National Laboratory

INS-O-10-03 August 2010

Police hard drive sold on eBay, secrets included

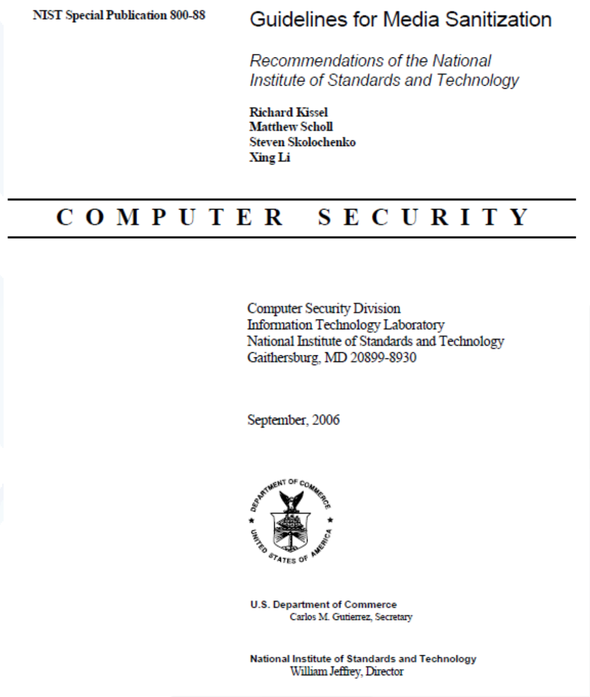
A computer hard drive, containing confidential data from the Brandenburg police in Germany, has been auctioned over eBay for €20, according to a report by Spiegel, one of Germany's leading weekly newspapers. It was bought by a student.

Hard disk drive data obliteration: has the data really been destroyed?

Data is harder to destroy from hard drives than you might think, warns Glyn Dodd, managing director at technology support specialist **Centrex Services**

A WORD ABOUT TERMS AND DEFINITIONS

- *Data destruction* is a generic term
- The industry users a number of terms including *data elimination*, *shredding*, *pulverizing,* and more.
- NIST Special Publication 800-88 uses the formal term *media sanitization*



NIST Special Publication 800-88

Guidelines for Media Sanitization

Recommendations of the National Institute of Standards and Technology

Richard Kissel
Matthew Scholl
Steven Skolochenko
Xing Li

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September, 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

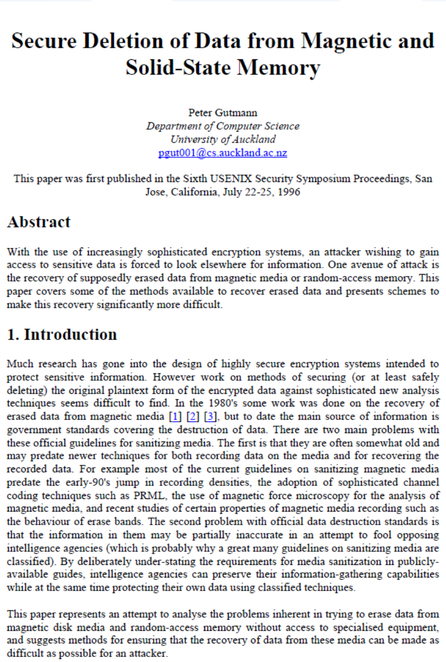
THIS IS NOT SUDDENLY A NEW ISSUE

Peter Gutmann

Secure Deletion of Data from Magnetic and Solid-State Memory - 1996

Simson Garfinkel

Remembrance of Data Passed: A Study of Disk Sanitization Practices - 2003



Secure Deletion of Data from Magnetic and Solid-State Memory

Peter Gutmann
Department of Computer Science
University of Auckland
pgut001@cs.auckland.ac.nz

This paper was first published in the Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996

Abstract

With the use of increasingly sophisticated encryption systems, an attacker wishing to gain access to sensitive data is forced to look elsewhere for information. One avenue of attack is the recovery of supposedly erased data from magnetic media or random-access memory. This paper covers some of the methods available to recover erased data and presents schemes to make this recovery significantly more difficult.

1. Introduction

Much research has gone into the design of highly secure encryption systems intended to protect sensitive information. However work on methods of securing (or at least safely deleting) the original plaintext form of the encrypted data against sophisticated new analysis techniques seems difficult to find. In the 1980's some work was done on the recovery of erased data from magnetic media [1] [2] [3], but to date the main source of information is government standards covering the destruction of data. There are two main problems with these official guidelines for sanitizing media. The first is that they are often somewhat old and may predate newer techniques for both recording data on the media and for recovering the recorded data. For example most of the current guidelines on sanitizing magnetic media predate the early-90's jump in recording densities, the adoption of sophisticated channel coding techniques such as PRML, the use of magnetic force microscopy for the analysis of magnetic media, and recent studies of certain properties of magnetic media recording such as the behaviour of erase bands. The second problem with official data destruction standards is that the information in them may be partially inaccurate in an attempt to fool opposing intelligence agencies (which is probably why a great many guidelines on sanitizing media are classified). By deliberately under-stating the requirements for media sanitization in publicly-available guides, intelligence agencies can preserve their information-gathering capabilities while at the same time protecting their own data using classified techniques.

This paper represents an attempt to analyse the problems inherent in trying to erase data from magnetic disk media and random-access memory without access to specialised equipment, and suggests methods for ensuring that the recovery of data from these media can be made as difficult as possible for an attacker.

Open-Source Security

Remembrance of Data Passed: A Study of Disk Sanitization Practices

SIMSON L. GARFINKEL AND ABHI SHELAT
Massachusetts Institute of Technology

Many discarded hard drives contain information that is both confidential and recoverable, as the authors' own experiment shows. The availability of this information is little publicized, but awareness of it will surely spread.

A fundamental goal of information security is to design computer systems that prevent the unauthorized disclosure of confidential information. There are many ways to assure this information privacy. One of the oldest and most common techniques is physical isolation: keeping confidential data on computers that only authorized individuals can access. Most single-user personal computers, for example, contain information that is confidential to that user.

Computer systems used by people with varying authorization levels typically employ authentication, access control lists, and a privileged operating system to maintain information privacy. Much of information security research over the past 30 years has centered on improving authentication techniques and developing methods to assure that computer systems properly implement these access control rules.

Cryptography is another tool that can assure information privacy. Users can encrypt data as it is sent and decrypt it at the intended destination, using, for example, the secure sockets layer (SSL) encryption protocol. They can also encrypt information stored on a computer's disk so that the information is accessible only to those with the appropriate decryption key. Cryptographic file systems[1–3] ask for a password or key on startup, after which they automatically encrypt data as it's written to a disk and decrypt the data as it's read; if the disk is stolen, the data will be inaccessible to the thief. Yet despite the availability of cryptographic file systems, the general public rarely seems to use them.

Absent a cryptographic file system, confidential information is readily accessible when owners improperly retire their disk drives. In August 2002, for example, the United States Veterans Administration Medical Center in Indianapolis retired 139 computers. Some of these systems were donated to schools, while others were sold on the open market, and at least three ended up in a thrift shop where a journalist purchased them. Unfortunately, the VA neglected to sanitize the computer's hard drives—that is, it failed to remove the drives' confidential information. Many of the computers were later found to contain sensitive medical information, including the names of veterans with AIDS and mental health problems. The new owners also found 44 credit card numbers that the Indianapolis facility used.[4]

The VA fiasco is just one of many celebrated cases in which an organization entrusted with confidential information neglected to properly sanitize hard disks before disposing of computers. Other cases include:

- In the spring of 2002, the Pennsylvania Department of Labor and Industry sold a collection of computers to local resellers. The computers contained "thousands of files of information about state employees" that the department had failed to remove.[5]
- In August 2001, Doubtd auctioned off more than 100 computers from the San Francisco office of the Viant consulting firm. The hard drives contained confidential client information that Viant had failed to remove.[6]
- A Purdue University student purchased a used Macintosh computer at the school's surplus equipment exchange facility, only to discover that the computer's hard drive contained a FileMaker database containing the names and demographic information for more than 100 applicants to the school's Entomology Department.
- In August 1998, one of the authors purchased 10 used computer systems from a local computer store. The computers, most of which were three to five years old,

NETTITUDE

InfoSecWorld Conference & Expo 2018

NEAR INFINITE (AND VERY CHEAP) STORAGE – A PERFECT STORM

Dell Inspiron

- 1TB internal drive
- $349

Western Digital

- 20TB external hard drive
- $799
- 5.25 pounds / 6.30” x 3.94’’ x 7.09’’

These can store all the corporate data crown jewels

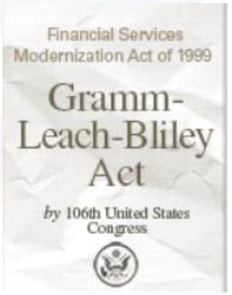
- Payroll, HR, R&D, financial, accounting, medical, company/trade secrets, tactical information, and much more
- Priceless, and expensive if lost

BUSINESS ISSUES AROUND SANITIZATION

- Every business has digital media (often petabytes) that must be sanitized
- Media sanitization is often overlooked
  - Failure to adequately sanitize media can have major and often catastrophic consequences to a business
  - financial loss
  - damage to a company’s reputation
  - regulatory violations
  - civil and criminal liability for directors and officers
  - especially since effective media sanitization is not rocket science

LEGAL AND REGULATORY DRIVERS

- GDPR, HIPAA, PCI, GLBA, Electronic Espionage Act, PIPEDA (Canada), FACTA Disposal rule, Check 21, FISMA, contracts, ICO (UK), Best Practices, and more to come
- regulatory and legal issues are extremely expensive
- even if you are found not at fault, you will have spent lots of money with nothing to show for it



DATA IS REMARKABLY RESILIENT

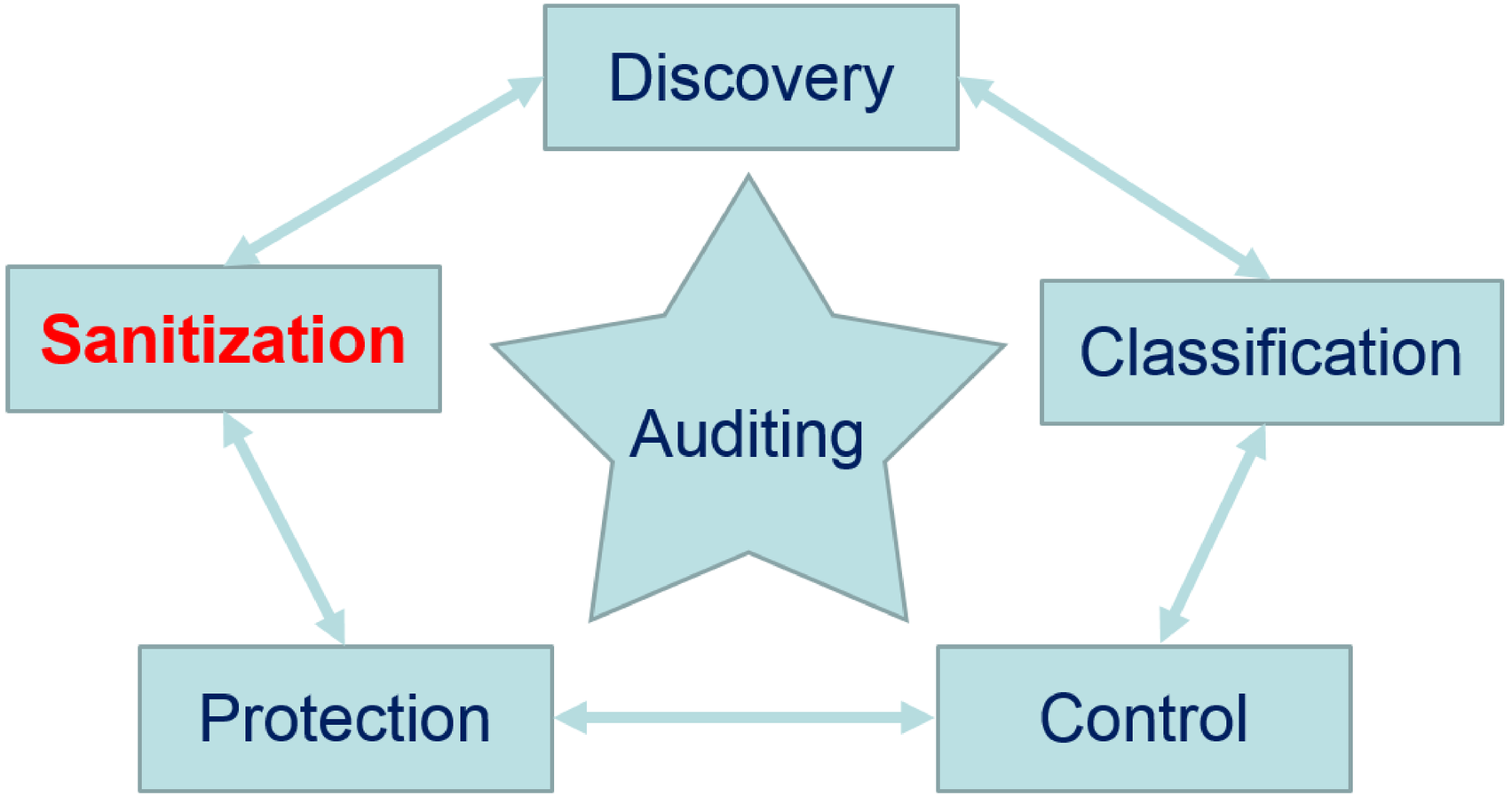
Fire - Found after fire destroys home – all data recovered

Crushed - Bus runs over laptop - all data recovered

Soaked - PowerBook underwater for 2 days - all data recovered

Fall from space - Hard drive recovered from space shuttle Columbia recovered from a dry river bed. 99% of 400MB data recovered

THE DATA LIFECYCLE



WHEN IS SANITIZATION NEEDED?

- Device is sold, donated, discarded, or recycled
- End of lease
- Storage decommissioning for data centers
- Sent to a manufacturer for warranty repair
- After severe malware/hacking/ransomware attack or attempt, for complete removal of offending code from infected storage device
- RAID or hot spare
  - Hot spare placed into service, then removed when faulty RAID drive was replaced
  - Hot spare should be sanitized, as well as the original failed RAID drive if the drive is still operational

DO YOU SEE DEAD MEDIA EVERYWHERE? YOU SHOULD

- IDC reported 405 million hard drives shipped in 2017
  - down from 425 million in 2016
- Thumb drives are everywhere
- How many multi-gig free USBs did you get at the expo?

IDC
Analyze the Future

MARKET FORECAST

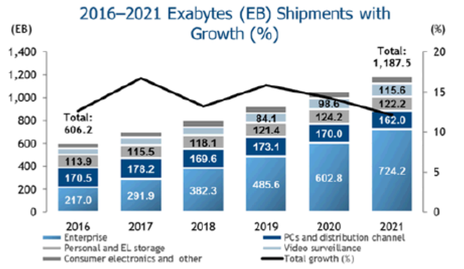
Worldwide Hard Disk Drive Forecast, 2017-2021

John Rydning

IDC MARKET FORECAST FIGURE

FIGURE 1

Worldwide Hard Disk Drive Exabyte Shipment Snapshot



Segment Shifts

Enterprise HDD EB shipments will grow at a 2016–2021 CAGR of 27.3%. In contrast, HDD EB shipments in all other market segments will grow at a 2016–2021 CAGR of 3.5%.

Source: IDC, 2017

NETTITUDE

DATA IS STORED IN COUNTLESS FORM FACTORS

- hard drives
- USB / thumb drives
- optical disks
- solid state storage
- flash
- VHS video
- floppies
- MFP
- back-up tapes
- copy machines
- DVD/CD
- GPS
- smart phones
- e-readers

NETTITUDE

HIPAA AND MEDICAL MEDIA

These media contain silver and are being recycled

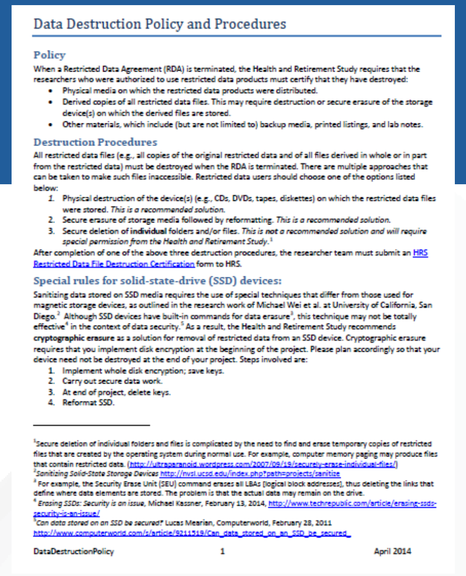
- x-ray
- microfilm
- Microfiche
- MRI
- CT scan
- imaging

EFFECTIVE SANITIZATION DEMANDS FORMAL PROCESSES

Formal system of information sanitization

- Based on risk factors specific to the organization
- in the event of a failure, plaintiff's lawyers will have much less to use, which could likely be judged positively by a jury
- must be policy based
  - detailed, explicit, auditable, and audited
- performed in a formal, consistent, documented manner
- done on a scheduled basis
- has quality control built in

POLICY



Data Destruction Policy and Procedures

Policy

When a Restricted Data Agreement (RDA) is terminated, the Health and Retirement Study requires that the researchers who were authorized to use restricted data products must certify that they have destroyed:

- Physical media on which the restricted data products were distributed.
- Derived copies of all restricted data files. This may require destruction or secure erasure of the storage device(s) on which the derived files are stored.
- Other materials, which include (but are not limited to) backup media, printed listings, and lab notes.

Destruction Procedures

All restricted data files (e.g., all copies of the original restricted data and of all files derived in whole or in part from the restricted data) must be destroyed when the RDA is terminated. There are multiple approaches that can be taken to make such files inaccessible. Restricted data users should choose one of the options listed below:

1. Physical destruction of the device(s) (e.g. CDs, DVDs, tapes, diskettes) on which the restricted data files were stored. *This is a recommended solution.*
2. Secure erasure of storage media followed by reformatting. *This is a recommended solution.*
3. Secure deletion of individual folders and/or files. *This is not a recommended solution and will require special permission from the Health and Retirement Study.*[1]

After completion of one of the above three destruction procedures, the researcher team must submit an HRS Restricted Data File Destruction Certification form to HRS.

Special rules for solid-state-drive (SSD) devices:

Sanitizing data stored on SSD media requires the use of special techniques that differ from those used for magnetic storage devices, as outlined in the research work of Michael Wei et al. at University of California, San Diego.[2] Although SSD devices have built-in commands for data erasure[3], this technique may not be totally effective[4] in the context of data security.[5] As a result, the Health and Retirement Study recommends **cryptographic erasure** as a solution for removal of restricted data from an SSD device. Cryptographic erasure requires that you implement disk encryption at the beginning of the project. Please plan accordingly so that your device need not be destroyed at the end of your project. Steps involved are:

1. Implement whole disk encryption; save keys.
2. Carry out secure data work.
3. At end of project, delete keys.
4. Reformat SSD.

[1] Secure deletion of individual folders and files is complicated by the need to find and erase temporary copies of restricted files that are created by the operating system during normal use. For example, computer memory paging may produce files that contain restricted data. (http://ultrageneral.wordpress.com/2007/08/19/securely-erase-individual-files/)
[2] *Sanitizing Solid-State Storage Devices* http://nvsl.ucsd.edu/index.php?path=projects/sanitize
[3] For example, the Security Erase Unit [SEU] command erases all LBAs [logical block addresses], thus deleting the links that define where data elements are stored. The problem is that the actual data may remain on the drive.
[4] *Erasing SSDs: Security is an issue*, Michael Kassner, February 13, 2014, http://www.techrepublic.com/article/erasing-ssds-security-is-an-issue/
[5] *Can data stored on an SSD be secured?* Lucas Mearian, Computerworld, February 28, 2011 http://www.computerworld.com/s/article/9211519/Can_data_stored_on_an_SSD_be_secured_

Policy is dependent on a number of factors including:

- age and interface type of the storage technology
- classification of the data residing on the device
- environment in which the device had been used

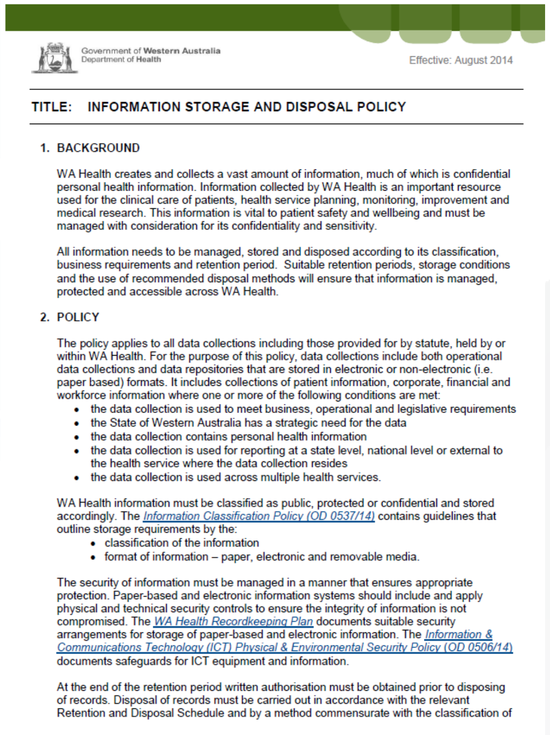
One policy does not fit all

- If device was used to store public data, but used in a SCIF that handles top secret information; the drive, since it was used in a SCIF, is likely classified at the highest level of classification
  - **S**ensitive **C**ompartmented **I**nformation **F**acility - enclosed area within a building that is used to process sensitive compartmented information

POLICY

Create a responsible policy

- must encompass all types of storage hardware and information classifications
- employ a responsible sanitization practice using both in-house and if required external services/resources



Government of Western Australia
Department of Health

Effective: August 2014

TITLE: INFORMATION STORAGE AND DISPOSAL POLICY

1. BACKGROUND

WA Health creates and collects a vast amount of information, much of which is confidential personal health information. Information collected by WA Health is an important resource used for the clinical care of patients, health service planning, monitoring, improvement and medical research. This information is vital to patient safety and wellbeing and must be managed with consideration for its confidentiality and sensitivity.

All information needs to be managed, stored and disposed according to its classification, business requirements and retention period. Suitable retention periods, storage conditions and the use of recommended disposal methods will ensure that information is managed, protected and accessible across WA Health.

2. POLICY

The policy applies to all data collections including those provided for by statute, held by or within WA Health. For the purpose of this policy, data collections include both operational data collections and data repositories that are stored in electronic or non-electronic (i.e. paper based) formats. It includes collections of patient information, corporate, financial and workforce information where one or more of the following conditions are met:

- the data collection is used to meet business, operational and legislative requirements
- the State of Western Australia has a strategic need for the data
- the data collection contains personal health information
- the data collection is used for reporting at a state level, national level or external to the health service where the data collection resides
- the data collection is used across multiple health services.

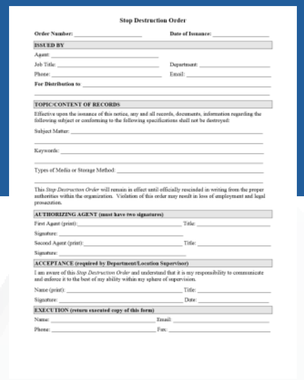
WA Health information must be classified as public, protected or confidential and stored accordingly. The *Information Classification Policy (OD 0537/14)* contains guidelines that outline storage requirements by the:

- classification of the information
- format of information – paper, electronic and removable media.

The security of information must be managed in a manner that ensures appropriate protection. Paper-based and electronic information systems should include and apply physical and technical security controls to ensure the integrity of information is not compromised. The *WA Health Recordkeeping Plan* documents suitable security arrangements for storage of paper-based and electronic information. The *Information & Communications Technology (ICT) Physical & Environmental Security Policy (OD 0506/14)* documents safeguards for ICT equipment and information.

At the end of the retention period written authorisation must be obtained prior to disposing of records. Disposal of records must be carried out in accordance with the relevant Retention and Disposal Schedule and by a method commensurate with the classification of

SANITIZATION MORATORIUM



Stop Destruction Order

Order Number: _____ Date of Issuance: _____

ISSUED BY

Agent: _____

Job Title: _____ Department: _____

Phone: _____ Email: _____

For Distribution to: _____

TOPIC/CONTENT OF RECORDS

Effective upon the issuance of this notice, any and all records, documents, information requiring the following subject or conforming to the following specifications shall not be destroyed:

Subject Matter: _____

Keywords: _____

Types of Media or Storage Method: _____

This *Stop Destruction Order* will remain in effect until officially rescinded in writing from the proper authorities within the organization. Violation of this order may result in loss of employment and legal prosecution.

AUTHORIZING AGENT (must have two signatures)

First Agent (print): _____ Title: _____

Signature: _____

Second Agent (print): _____ Title: _____

Signature: _____

ACCEPTANCE (required by Department/Location Supervisor)

I am aware of this *Stop Destruction Order* and understand that it is my responsibility to communicate and enforce it to the best of my ability within my sphere of supervision.

Name (print): _____ Title: _____

Signature: _____ Date: _____

EXECUTION (return executed copy of this form)

Name: _____ Email: _____

Phone: _____ Fax: _____

Often called a Litigation Hold or Legal Hold

- organization must **stop** its data sanitization activities
- sanitization activities must immediately be placed on hold until legal department determines whether these sanitization activities jeopardize sought-after data
- doesn't just mean when there is a lawsuit
  - can be regulatory investigation, internal investigation for workplace misconduct, preservation because a client or vendor is in litigation
  - while you aren't technically part of it, you may have data material to the matter they are involved in

RECYCLING IS GREEN, BUT IT'S *NOT* SANITIZATION

Microstar

Home | About Us | Sell Hard Drives | Sell RAM | Sell Motherboards | Contact Us | Our eBay Store

Sell RAM Memory, Sell used RAM, Sell used Memory

We buy ram memory of all major brands like Crucial, SanDisk, Kingston, Dell, Apple, HP and other major brands. Branded RAM gives you higher value. If your RAM memory still have sticker on that, then you are at luck, we can provide you better pricing. We accept DDR2 and DDR3 types of RAM Memory. We also accept RAM memory from old Mac computer and laptops. You can sell us RAM in bulk quantity as well. We are buying server RAM memory also. Just fill the form on bottom of this page and we will get back to you as soon as possible.

Why you choose Microstar?

- We are eBay Power Seller.
- We are in this industry more than 3 decades.
- We pay you most of your RAM memory.
- We buy RAM memory from computer, laptop and server of all types.
- We process your payment fast.

We accept DDR2 and DDR3 RAM Memory of following brands:

Oracle-Sun Microsystems	Samsung	Dell	Crucial
Micron	IBM	Hynix	HP
Edge	Corsair	Cisco	All other brands

Hard Drive Disposition Services and Data Center Value Recovery | (800) 700-7683 | sales@webuyusedharddrives.net | follow us

We Buy Used Hard Drives

IT Asset Recovery | About | Blog | Contact | FREE QUOTE

Servers, Desktop Hard Drives and Laptop Hard Drives have significant value. Send us the details about your Hard Drives and get a maximum offer.

Get a quote today!

Get A Quote | 239.596.2254 | Serving All States

exIT technologies

R2 Responsible Recycling | We Buy: Servers | Processors | Memory | Networking | Storage

ITAD Services | Data Center Services | Colocation Services | Industries | Contact Us | Blog | About

DTC Computer Supplies

DTC Computer Supplies
Serving I.T. Departments & Saving Budgets for Over 40 Years!

Call Us!
(800) 700-7683 – Toll-Free
(909) 466-7680 – Local
E-mail Us!
contact@dtc1.com

Home | Products | Services | Computer Repair | Printer Repair | Service Area | About Us | Contact Us

Home › Services › Sell Your Backup Media

We Buy Used Tapes, Disks, and All Other Types of Backup Media

Have you thought about selling your Magnetic Media? Do you need an environmentally responsible way to reduce expenses and make a positive influence to your organization's bottom line? Cash in your surplus, used, obsolete and unused tapes. DTC makes top offers for all types of data tape, cartridges, and other media. We guarantee your data is securely and completely eradicated. Our processes comply with all government agency and industry specific regulations. Data Destruction Certificates are provided to document your transaction and comply with your organization's recycling and data eradication processes.

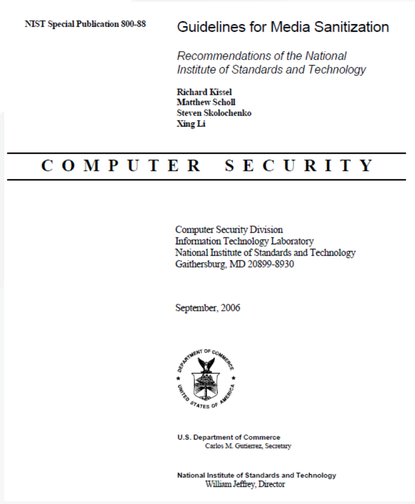
NETTITUDE

InfoSec World Conference & Expo 2018

NIST SP 800-88

Guidelines for Media Sanitization

- General process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed
- assists with decision-making when media require disposal, reuse, or will be leaving the effective control of an organization
- develop and use local policies and procedures in conjunction with 800-88 to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information


NIST Special Publication 800-88

Guidelines for Media Sanitization

Recommendations of the National Institute of Standards and Technology

Richard Kissel
Matthew Scholl
Steven Skolochenko
Xing Li

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September, 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

SANITIZATION TYPES

Clearing

- Protects confidentiality of data against keyboard attack
- Overwriting

Purging

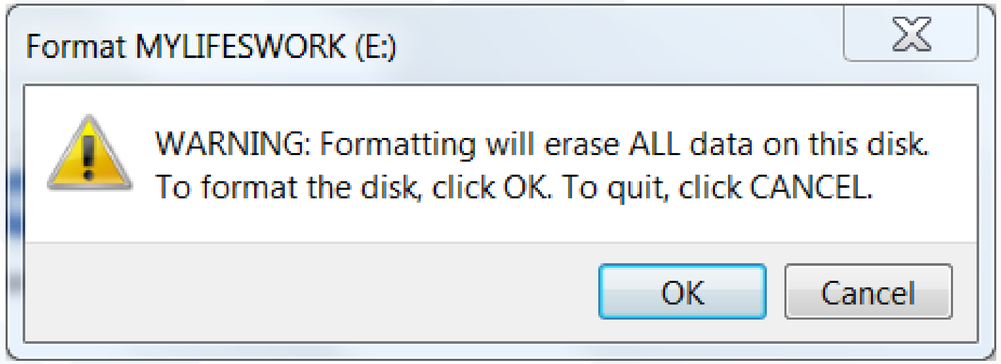
- Protects the confidentiality of information against a laboratory attack (use of special equipment by trained recovery technicians)
- Secure Erase, degaussing

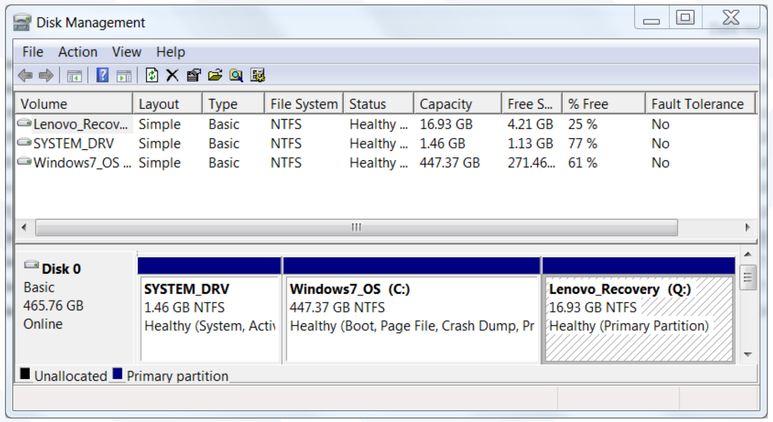
Destroying

- Absolute destruction
- Hard drive shredding, smelting, disintegration

UNACCEPTABLE SANITIZATION PRACTICES

- File deletion
- Drive formatting
- Disk partitioning
- Encryption / key destruction





M&A planned activity for 2Q2018.pptx	2/21/2018 11:11 PM	PGP Zip	1,236 KB
US financial projections 2018.xls	2/21/2018 11:12 PM	Application	175 KB
Internal data breaches 2017 - CONFIDENTIAL.docx	2/21/2018 11:11 PM	PGP Zip	122 KB
Executive's salaries 2017 – USA & EMEA.pdf	2/21/2018 11:13 PM	PGP Zip	31 KB

SOFTWARE BASED SANITIZATION

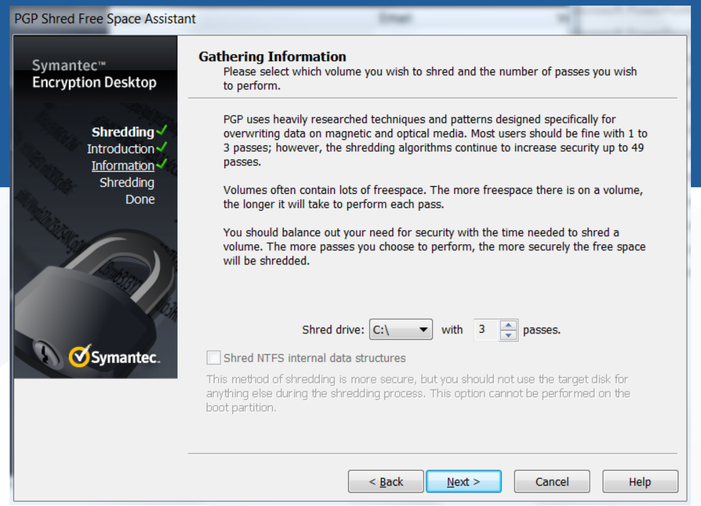
Advantages

- single pass is adequate (as long as all data storage regions can be addressed)
- cost-effective and easily configurable sanitization solution
- can be configured to clear specific data, files, partitions or just the free space
- erases all remnants of deleted data to maintain ongoing security
- green solution

Disadvantages

- requires significant time to process entire high capacity drive
- may not be able to sanitize data from inaccessible regions
- inconsistent data logging, audit trails or certification labels
- no security protection during the erasure process / subject to intentional or accidental parameter changes
- may require separate license for every hard drive
- ineffective without QA processes
- not scalable

SINGLE PASS VS. MULTIPLE PASSES



DoD standard 5220.22-M (1995)

- required at least 3 passes required

NIST Special Publication 800-88, section 2.3

- replaces 5220 which is retired
- for ATA disk drives manufactured after 2001
- clearing by overwriting the media once is adequate against both keyboard and laboratory attack
- single pass is adequate only if able to access the entire data storage region of the media surface

Overwriting Hard Drive Data: The Great Wiping Controversy

http://privazer.com/overwriting_hard_drive_data.The_great_controversy.pdf

ABSOLUTE DESTRUCTION

- Process must ensure that data on the media surface can’t be recovered using any technology now available or in the future
- Grinding media to a particle size smaller than the smallest recoverable unit, sector, or melting the media to slag, etc., to assure data can never be recovered

- Ryk Edelstein – CEO Cicada Security

CICADA
Security Technology

NETTITUDE

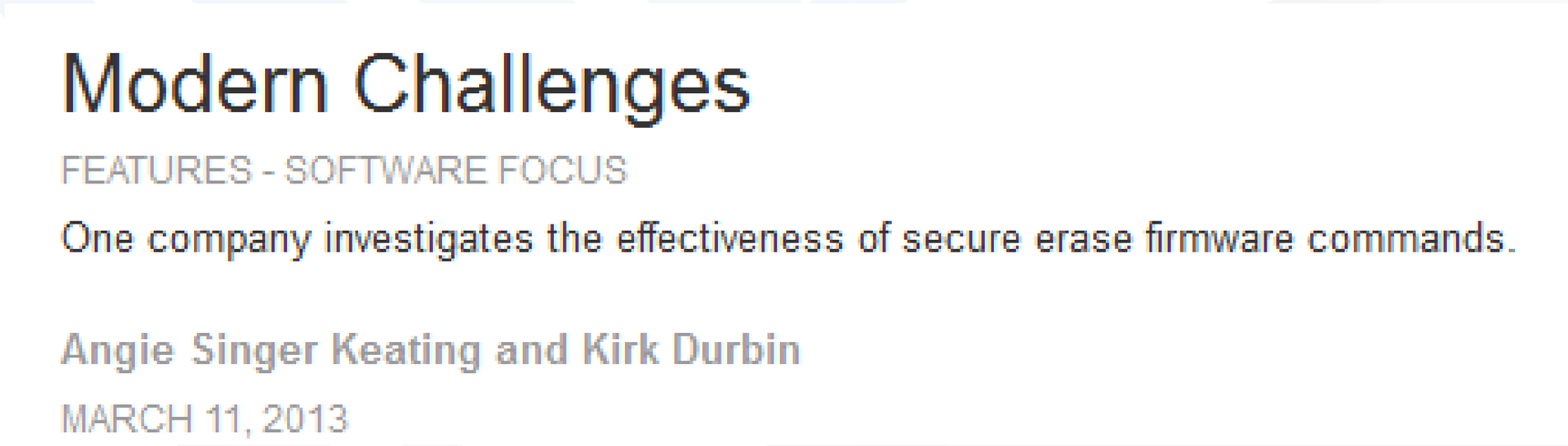
SECURE ERASE SANITIZATION STANDARD

- From drive manufacturers & Center for Magnetic Recording Research
- component of the ANSI ATA Specification
- optional inclusion for use in SCSI as *Secure Initialize*
- embedded in the firmware of all standards compliant ATA hard drives manufactured since 2002
- highly effective and very fast
- validated and certified by various governing bodies
- most individuals and companies don’t know it exists
- HDD manufacturers scared of irate help-desk calls
- inhibited by most PC manufacturers to protect from the potential exploitation by virus / malware

HOW SECURE IS SECURE ERASE?

Keating and Durbin research on effectiveness of Secure Erase

- Secure Erase doesn’t always successfully execute on all hard drives
- Weakness: no output of status code or statistics. When command is executed, only return from the application is that it completed
- NIST to deal with it in a revision to 800-88



Modern Challenges

FEATURES - SOFTWARE FOCUS

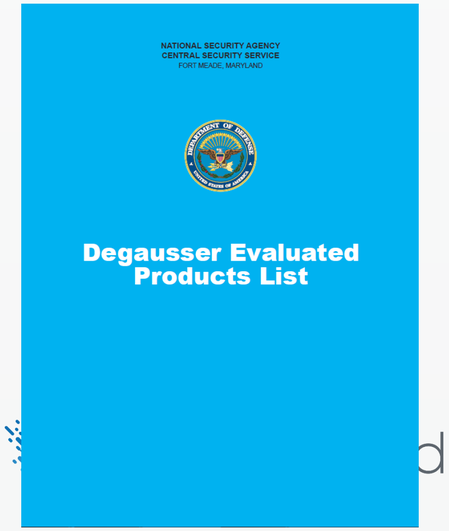
One company investigates the effectiveness of secure erase firmware commands.

Angie Singer Keating and Kirk Durbin

MARCH 11, 2013

HARDWARE BASED - DEGAUSSING

- Removal of data by exposing data storage bits on media surface to a magnetic field of sufficient strength to achieve coercion of the bit
  - ensure degausser on NSA *Degausser Evaluated Products List*
  - non-EPL listed devices will be cheaper
- Destructive process
  - creates irreversible damage to hard drives
- destroys the special servo control data on the drive, which is meant to be permanently embedded on the hard drive
- once the servo is damaged, the drive is unusable
- if you plan to reuse the drive, don’t degauss it



CHOOSING A DEGAUSSER

Cycle time – time it takes to complete the erasure

Heat generation – may generate significant heat. Need to cool down

- if you need to degauss many drives, downtime can be an issue

Wand or cavity style – hand wands models are generally cheaper, but may lack certain power features

- cavity style enables you to place the entire unit into the degausser

Size – smaller and portable, or larger more powerful?

- some powerful models require wheels - can weigh 400 pounds

NETTITUDE

DEGAUSSING DOESN'T WORK ON ALL MEDIA

Degaussing will eliminate data on:

- nearly all magnetic-based hard drives
- backup tapes (DLT, SDLT, LTO, QIC, DAT, Travan, AIT, 8mm)
- removable: floppy, ZIP, JAZZ, REV, Syquest
- audio tapes: cassette, mini/micro, cassette, reel-to-reel
- video tapes: VHS, Beta, SVHS, Mini DV, 8mm

Degaussing will not eliminate data on:

- Solid state drives (SSD)
- USB thumb, compact flash, optical (CD, DVD), smartphones

DEGAUSSER ENVIRONMENTAL CONSIDERATIONS

- Should be installed in a location that will not interfere with equipment or cause risk to operator or the public
- Caution must be taken so that the strong electromagnetic fields created by the degausser don’t produce collateral damage to other susceptible equipment nearby
- Must not impose potential health risk
  - Consideration for interference with those who have pacemakers

PHYSICAL DESTRUCTION

- Shredding
- Disintegration
- Bending, breaking or mangling the hard drive
  - drive is easily distinguishable from unprocessed drives - ensuring the disposal of the correct drive
- Absolute destruction required?
  - grind to diameter smaller than single data block (512KB), require particle size less than 1/250 inch

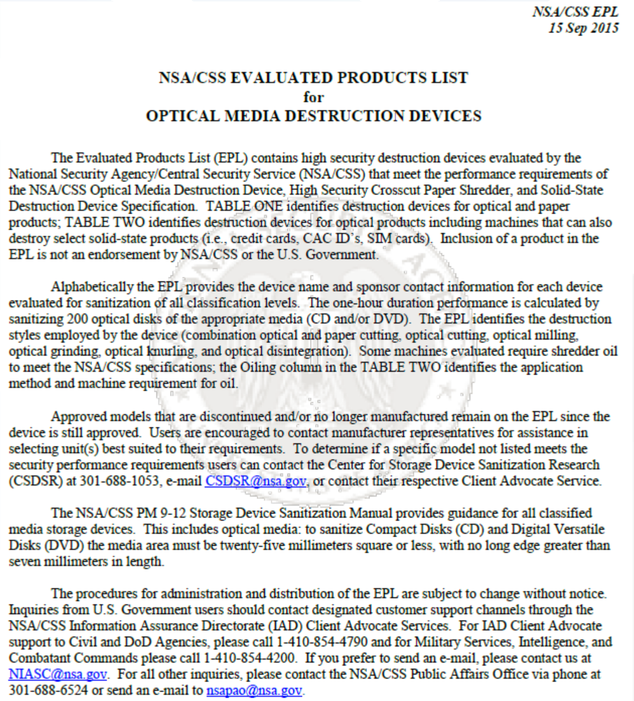
SECURE ERASE VIA HARDWARE

Enables the native Secure Erase command

- overcomes host limitations to effectively launch Secure Erase
- maintains internal audit log
- issues destruction certificate upon successful completion

OPTICAL MEDIA SANITIZATION

- Securely and permanently eradicates digital data on DVD, CD-ROM & other optical media
  - grinds the information layer off media
- Ensure device meets requirements of NSA/CSS *Evaluated Products List For Optical Media Destruction Devices*



NSA/CSS EPL
15 Sep 2015

NSA/CSS EVALUATED PRODUCTS LIST
for
OPTICAL MEDIA DESTRUCTION DEVICES

The Evaluated Products List (EPL) contains high security destruction devices evaluated by the National Security Agency/Central Security Service (NSA/CSS) that meet the performance requirements of the NSA/CSS Optical Media Destruction Device, High Security Crosscut Paper Shredder, and Solid-State Destruction Device Specification. TABLE ONE identifies destruction devices for optical and paper products; TABLE TWO identifies destruction devices for optical products including machines that can also destroy select solid-state products (i.e., credit cards, CAC ID's, SIM cards). Inclusion of a product in the EPL is not an endorsement by NSA/CSS or the U.S. Government.

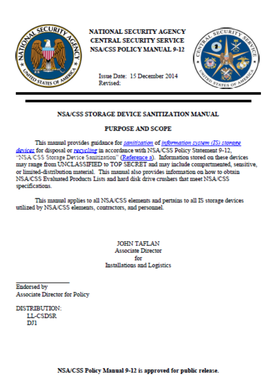
Alphabetically the EPL provides the device name and sponsor contact information for each device evaluated for sanitization of all classification levels. The one-hour duration performance is calculated by sanitizing 200 optical disks of the appropriate media (CD and/or DVD). The EPL identifies the destruction styles employed by the device (combination optical and paper cutting, optical cutting, optical milling, optical grinding, optical knurling, and optical disintegration). Some machines evaluated require shredder oil to meet the NSA/CSS specifications; the Oiling column in the TABLE TWO identifies the application method and machine requirement for oil.

Approved models that are discontinued and/or no longer manufactured remain on the EPL since the device is still approved. Users are encouraged to contact manufacturer representatives for assistance in selecting unit(s) best suited to their requirements. To determine if a specific model not listed meets the security performance requirements users can contact the Center for Storage Device Sanitization Research (CSDSR) at 301-688-1053, e-mail CSDSR@nsa.gov, or contact their respective Client Advocate Service.

The NSA/CSS PM 9-12 Storage Device Sanitization Manual provides guidance for all classified media storage devices. This includes optical media: to sanitize Compact Disks (CD) and Digital Versatile Disks (DVD) the media area must be twenty-five millimeters square or less, with no long edge greater than seven millimeters in length.

The procedures for administration and distribution of the EPL are subject to change without notice. Inquiries from U.S. Government users should contact designated customer support channels through the NSA/CSS Information Assurance Directorate (IAD) Client Advocate Services. For IAD Client Advocate support to Civil and DoD Agencies, please call 1-410-854-4790 and for Military Services, Intelligence, and Combatant Commands please call 1-410-854-4200. If you prefer to send an e-mail, please contact us at NIASC@nsa.gov. For all other inquiries, please contact the NSA/CSS Public Affairs Office via phone at 301-688-6524 or send an e-mail to nsapao@nsa.gov.

SOLID STATE DRIVES (SSD)



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY MANUAL 9-12

Issue Date: 15 December 2014
Revised:

NSA/CSS STORAGE DEVICE SANITIZATION MANUAL

PURPOSE AND SCOPE

This manual provides guidance for sanitization of information system (IS) storage devices for disposal or recycling in accordance with NSA/CSS Policy Statement 9-12, "NSA/CSS Storage Device Sanitization" (Reference a). Information stored on these devices may range from UNCLASSIFIED to TOP SECRET and may include compartmented, sensitive, or limited-distribution material. This manual also provides information on how to obtain NSA/CSS Evaluated Products Lists and hard disk drive crushers that meet NSA/CSS specifications.

This manual applies to all NSA/CSS elements and pertains to all IS storage devices utilized by NSA/CSS elements, contractors, and personnel.

JOHN TAFLAN
Associate Director
for
Installations and Logistics

Endorsed by
Associate Director for Policy

DISTRIBUTION:
LL-CODIR
DJ1

NSA/CSS Policy Manual 9-12 is approved for public release.

- Degaussing is not effective on SSD media
- Software overwrite is not foolproof
- Physical destruction remains the only fail-safe method to date, but in order to be effective, even shredding and crushing require a different approach than for standard HDDs.
- NSA/CSS 9-12 storage device sanitization manual approved methods:
  - Disintegration - into particles that are 2mm edge length
  - Incineration - material must be reduced to ash
  - Power removal - removing the power, including backup batteries
  - Strip shredding or cutting - strip shredder with a maximum width of 2 millimeters

WHICH IS THE BEST METHOD?

For most unclassified media, physical destruction is acceptable.

- physical damage is so considerable, it's almost impossible to recover the data; except for a nation state, or MacGyver

For highly classified data, degauss then physically destroy the media

- that two-step approach is DoD mandated for classified data

Ultimately, the best method is what meets **your** specific requirements to mitigate your specific risks

THREAT AND RISK MATRIX

ADISA risk level	Threat actor and compromise methods
1 – Very Low	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilizing freeware, OS tools and COTS products
2 – Low	Commercial data recovery organization able to mount non-invasive and non-destructive software attacks and hardware attacks
3 – Medium	Commercial computer forensics organization able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilizing COTS products
4 – High	Commercial data recovery and computer forensics organization able to mount both non-invasive/nondestructive and invasive/non-destructive software and hardware attack, utilizing both COTS and bespoke utilities
5 – Very High	Government-sponsored organizations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitized data

IN-HOUSE DATA SANITIZATION

Advantages

- Media never leaves your location, no risk of loss in transit
- Full control
- Data is destroyed by your own trusted staff
- Recommended that all destruction activities be carried out under the office of the CISO, and by a trained and trusted technology support technician

Disadvantages

- Destruction systems can be expensive
- Low volume = longer time for ROI
- Staff with other duties may miss devices
- Must manage internal personnel and technology changes
- Lack of space and/or resources for proper segregation between destroyed and non-destroyed units
- Still must have a qualified vendor to deal with residual waste and/or drives that fail sanitization/wiping process
- Disposal of residual material
- Technicians will miss drives
- Requires good QC process

IN-HOUSE DATA SANITIZATION

- Quality control is crucial
- If your organization is going to do any of its own data sanitization, it **must** have quality control mechanisms
  - Separation of duties - one tech removes hard drives while another is assigned to verify the drives have been removed, document the verification, and replace the cover
- Wiping - assign a separate tech to take a random sample of at least 10% (depending on quantity) and attempt to recover data with a COTS data recovery tool

OUTSOURCED DATA SANITIZATION

Advantages

- No initial capital investment required
- handles varying destruction needs (disintegration, degaussing, etc.)
- can handle varying volume needs
- experts utilizing best practices
- may have higher security standards than your location
- no need to manage personnel and technology changes
- regulatory compliant residual disposal
- if litigated, professional secure destruction services destruction documentation is more credible than internally generated processes

Disadvantages

- No direct control of vendor employees
- may be transported outside of your location
- possible security concerns with off-premise transportation and handling
- may get locked into a bad contract
- may require minimums greater than your needs
- data is handled/destroyed by non-employees
- if hardware is not disposed of properly, you could be included in a pollution liability case
- **Given these disadvantages, special emphasis should be placed on vendor selection criteria that specifically address these issues**

OUTSOURCED DATA SANITIZATION – ASK LOTS & LOTS OF QUESTIONS

- What type of insurance coverage do they have?
  - professional liability (sometimes called Errors & Omissions)
  - pollution / environmental liability
  - demand to see certificate of insurance demonstrating coverage for both
- what processes do they follow from receipt of asset through disposition?
- what are their security procedures?
- how do they sanitize data?
- are they NAID certified for digital data destruction?
- how do they verify data is eradicated?
- do they do full background checks?
- what are financial capabilities?
- if private, where do they get their funding? How stable is source?
- can they provide customer references?
- do they have the necessary state and local permits?
- do they export e-waste overseas?
- can they handle all or most of the locations for which you will require services?
- do they have processes around chain of custody?
- will they agree to the SLA's that you have created?
- do they barcode items?

OUTSOURCING - CAVEAT EMPTOR

- Certificate of destruction and a contract assuring responsibility of the process mean very little in the real world
- If a device is lost or data is exposed, it will be the owner of the data who will be getting the penalty and making the mandatory disclosure
- The service provider will be little more than a footnote in the disclosure

DATA MEDICS

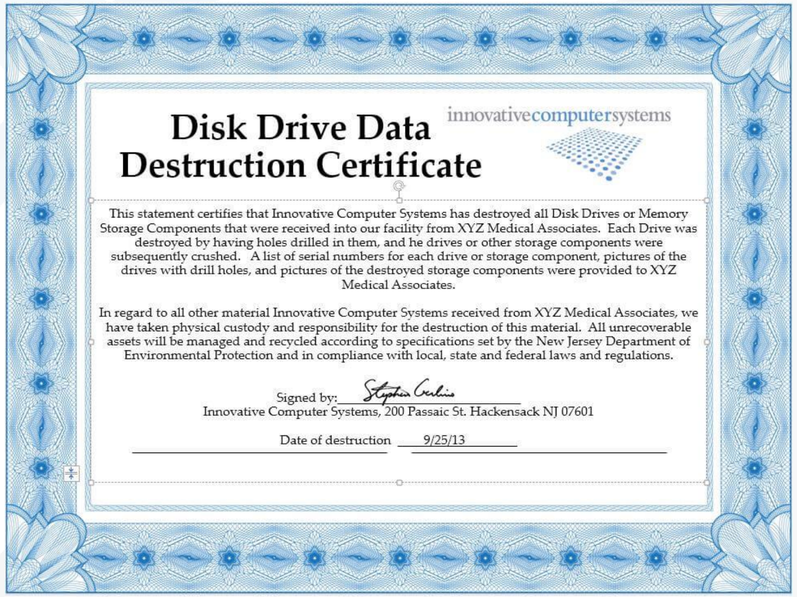
Certificate of Destruction

The hard drive appearing to the right
serial #S0DEJ1KL806379

Was securely wiped using the following method:
D.o.D. Three Pass Psudo-random

At the following times:
Start: 4/20/2015 1:31 p.m.
End: 4/20/2015 2:39 p.m.
Technician: Jared Palmer

Jared Palmer



Disk Drive Data Destruction Certificate

innovativecomputersystems

This statement certifies that Innovative Computer Systems has destroyed all Disk Drives or Memory Storage Components that were received into our facility from XYZ Medical Associates. Each Drive was destroyed by having holes drilled in them, and he drives or other storage components were subsequently crushed. A list of serial numbers for each drive or storage component, pictures of the drives with drill holes, and pictures of the destroyed storage components were provided to XYZ Medical Associates.

In regard to all other material Innovative Computer Systems received from XYZ Medical Associates, we have taken physical custody and responsibility for the destruction of this material. All unrecoverable assets will be managed and recycled according to specifications set by the New Jersey Department of Environmental Protection and in compliance with local, state and federal laws and regulations.

Signed by: Stephen Gerbino
Innovative Computer Systems, 200 Passaic St. Hackensack NJ 07601

Date of destruction 9/25/13

TAKING SANITIZATION SERIOUSLY

Segregation

- separate all storage devices and media from others to be disposed of materials.
- specifically remove all hard drives from to-be-disposed-of PCs, laptops and servers

Inventory

- establish the chain of possession of the data storage device
- best practice - establish the connection of a particular storage device to the unit it was removed from and use internal asset management records to track the device back to the actual user

TAKING SANITIZATION SERIOUSLY

Isolation

- using secure collection containers, isolate inventoried data storage devices to prevent unauthorized removal.
- avoid warehousing – media must be processed frequently as to avoid warehousing of drives containing confidential data.

Hard drives in an unsecured storage room at the Oak Ridge National Laboratory

http://energy.gov/sites/prod/files/igprod/documents/INS-O-10-03.pdf

NAID

National Association for Information Destruction

- International trade association for companies providing information destruction services
- Mission: to promote the information destruction industry and the standards and ethics of its member companies
- NAID certified companies audited annually
  - by an independent 3rd-party and subject to unannounced audits
- www.naidonline.org

FOR MORE INFORMATION

Center for Magnetic Recording Research
http://cmrr.ucsd.edu

Australian Department of Defence Information and Communications Technology Security Manual
https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf

Can Intelligence Agencies Read Overwritten Data?
www.nber.org/sys-admin/overwritten-data-gutmann.html

Storage & Destruction Business Magazine
http://www.recyclingtoday.com/magazine/code/sdb/

ICO - IT asset disposal for organisations
https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

FOR MORE INFORMATION

National Association of Corporate Directors

- Record Retention and Document Destruction Policy

https://www.nacdonline.org/files/NACDGovernanceDocuments/RecordRetention051023.pdf?navItemNumber=1785

Remembrance of Data Passed: A Study of Disk Sanitization Practices

http://cdn.computerscience1.net/2006/fall/lectures/8/articles8.pdf

Best Practices for the Destruction of Digital Data

https://www.amazon.com/Best-Practices-Destruction-Digital-Data-ebook/dp/B008UZHQA4

Hard Drive Disposal: The Overlooked Confidentiality Exposure

http://www-03.ibm.com/financing/pdf/sg/Hard_Drive_Disposal_The_Overlooked_Confidentiality_Exposure_AP.pdf

SOFTWARE AND HARDWARE VENDORS

DestructData
www.destructdata.com

Security Engineered Machinery
www.semshred.com

Ontrack Eraser
www.krollontrack.com

CPR Tools
www.cprtools.net

Ensconce Data Technology
www.deadondemand.com

Garner Products
www.garner-products.com

Darik’s Boot And Nuke
www.dban.org

CONCLUSION / ACTION ITEMS

- **Management awareness**
  - management must be aware of the risks
  - must ensure formal sanitization processes are developed
- **Develop strategies** on media sanitization
- **Review security procedures** for adequacy, completeness, scope and failure analysis
- Develop an **information lifecycle audit program**
  - Follow a life cycle approach to IT risk management that includes making an explicit decision about data destruction
- **Implement** sanitization process
- Ensure **quality control** is built into the process

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Ben Rothke, CISSP PCI QSA

Principal Security Consultant - Nettitude

@benrothke