SMART™
HIGH RELIABILITY SOLUTIONS

Security Features for Solid State Drives in Defense Applications

SHRS-WP001 White Paper

Headquarters: T: (+1) 800.956.7627 • T: (+1) 510.623.1231 • F: (+1) 510.623.1434 • E: info@smarth.com

Customer Service: T: (+1) 510.624.5379 • F: (+1) 480.926.5579 • E: info@smarth.com

Europe: T: (+44) (0)1592.760426 • E: info@smarth.com

Asia/Pacific: T: (+65) 6232.2858 • F: (+65) 6232.2300 • E: info@smarth.com

Table of Contents

1. EXECUTIVE SUMMARY

There are various methods for data protection and elimination in Flash solid state drives (SSDs), depending on the security level required within each application. Security techniques can be divided into three categories:

1. Data protection
2. Data elimination
3. Media destruction

Methods of data protection include write protection, password protection and encryption. Password protection can be used in combination with a biometric key to implement a security scheme that is based on “what you have, what you know, who you are”.

Data elimination is handled by Clear and Sanitize procedures. Which method needs to be implemented depends on the security classification level of the organization in which the application resides. Typically, if the device will stay within the same security classification, a Clear procedure will suffice. If it is moved to a higher security classification level, the device needs to be entirely declassified, and a Sanitize procedure is needed. Moving the device to a lower security classification would require destruction of the drive.

Sanitizing a solid state drive is much faster and requires fewer cycles of the same procedure when compared to hard disk drives, since SSDs experience far lower levels of data remanence.

Complete media destruction can be a solution if a Sanitize procedure is too time consuming. However, incineration or disintegration can be expensive and impractical for many situations.

2. INTRODUCTION

In April 2001, a US Navy surveillance plane was intercepted by two Chinese F-8 fighter planes during a routine patrol flight over the Chinese South Sea[1]. The US plane was forced to make an emergency landing in China, after what officials described as a "minor" mid-air collision, occured with one of the Chinese planes.

The US crew had between 12 and 20 minutes in the air to destroy all classified material on board before making the emergency landing. In the final moments before the plane landed, the crew tried to destroy the hardware with hammers and axes. Just how much the crew was able to destroy is not public knowledge.

Figure 1: US Navy EP-3E ARIES before and after landing in China

This story illustrates the need for high-level security methods in defense systems, and in particular for the storage devices within these systems. This story is at the far end of the security spectrum; there are many systems that require lesser forms of security. For example, devices such as data recorders and ruggedized laptops that are used in training environments require a lower security implementation. Since these devices stay within the same security classification environment, fast elimination of mission data may be all that is required once a training mission has been completed. On the other hand, if the device is moved to an environment with a higher security classification, a complete Sanitize procedure per the specified defense department standard will be required. Moving the device to an environment with a lower security classification requires complete destruction of the device.

In general, defense storage system security levels are divided into three categories:

1. Data protection

2. Data elimination

3. Media destruction

The third method would have definitely been preferred in the case of the US surveillance plane, but, of course, it is impractical, if not impossible, to have incineration or disintegration equipment inside an aircraft.

SMART High Reliability Solutions (SMART HRS) designs and develops security functionality in accordance with commonly used military specifications. As a result of this focus, SMART HRS solid state drives find wide acceptance and deployment in defense applications.

This white paper discusses the various solid state drive data security methods that can be applied in defense applications and environments, and discusses Secure Data Elimination Technology (SDET) implemented within the solid state drive product line from SMART HRS.

3. SECURITY IN SOLID STATE DRIVES VS. HARD DISK DRIVES

Implementing security features that require data elimination or media destruction is far more complex for hard disk drives than solid state drives due to their underlying storage technology. For example, hard disk drives leave behind a much bigger "ghost-image" once data is written to them. This requires more complex and longer data elimination procedures than would be needed for solid state drives.

In general, the amount of data that could possibly remain after a simple erase on a particular storage medium dictates the complexity of the data elimination and media destruction techniques on that storage medium. The smaller the data remanence on the storage media, the more simple data elimination techniques can be implemented. The next sections review data remanence on hard disk drives and solid state drives.

3.1 Data Remanence in Hard Disk Drives

When data is written to a magnetic medium, the write head sets the polarity of most, but not all, of the magnetic substrate. This is partially due to the inability of the write head to write in exactly the same location each time, and partially due to the variations in media sensitivity and field strength among devices over time [4].

When a “1” is written to a disk, the media records a ”1”. When a “0” is written, the media records a ”0”. However, the actual effect is closer to obtaining a 0.95 when a “0” is overwritten with a “1” and a 1.05 when a “1” is overwritten with a ”1”. Deviations of the drive head from the original track may leave significant portions of the previous data along the track edge.

Normal disk circuitry is set up so that both these values are read as ”1”, but using specialized tools such as a magnetic force microscope, it is possible to read what previous layers contained. Using thesebspecialized tools, extracting so-called “ghost-images” becomes fairly easy.

To ensure a complete elimination of a “ghost-image” on a magnetic disk drive, two procedures can be followed:

- Degaussing the media by applying a reverse (coercive) magnetizing force in order to reduce the correlation between previous and present data to a point that there is no known technique for recovery of previous data [2].
- Overwriting the media multiple times with various patterns. A one-time erase of the media will not suffice and military standards specify up to four Sanitize cycles of erase and pattern-overwrite. However, according to industry recommendations [4], a pattern overwrite of up to 35 times is required to completely clear previously contained data from the media.

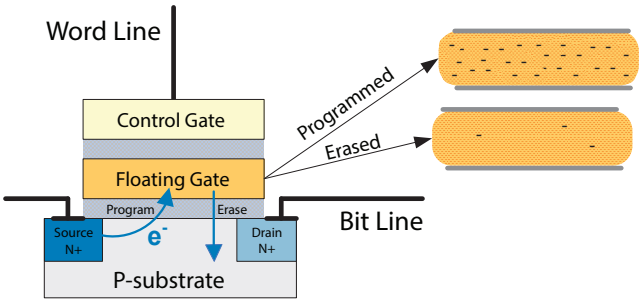
3.2 Data Remanence in Solid State Drives

Solid state drives use NAND Flash technology for data storage. Figure 2 below shows the internal structure of a NAND Flash cell, which uses a process known as Fowler-Nordheim tunneling to change the charge inside the floating gate [3].

Writing (programming) a “0” into a cell causes the accumulation of negative charges in the floating gate.

Writing a “1” into a cell does not change the cell’s content. To change the content of a cell from “0” to “1”, the cell must be erased in order to release the negative charges in the floating gate.

Figure 2: NAND Flash cell



Data remanence in NAND Flash is mainly caused by a so-called hot-carrier effect [3], where electrons get trapped in the gate oxide layer and can stay there as excess charge. The amount of trapped charge can be determined by measuring the gate-induced drain leakage current of the cell, or more indirectly by measuring the threshold voltage of the cell. The effect is more apparent in fresh cells, and becomes less noticeable after 10 program/erase cycles.

Erasing the cell will significantly reduce the amount of trapped electrons, making it extremely difficult to recover any data from the device after an erase cycle.

3.3 Flash SSD Data Abstraction Layers

An additional complexity to recovering data from a solid state drive (when compared to hard disk drives) arises from the fact that solid state drives contain additional data abstraction layers. In-depth knowledge would be required of the following layers to obtain a valid picture of the extracted data:

- File system: Each file system has its own method of mapping files, creating pointers, and storing tables. Knowledge of this would be required for both HDD and solid state drives when data is extracted
- Logical to physical mapping: Flash Management Systems map the logical file system sectors to physical locations on the Flash. Each solid state drive vendor implements a different Flash management algorithm for mapping sectors

- Solid state drive architecture: Each solid state drive vendor has a different architecture, and therefore it is hard to determine where in each Flash chip a logical block address ends up
- Flash cell architecture: Different Flash vendors have different Flash cell architectures with different sequences of discrete bits

The additional data abstraction layers in a solid state drive increase the complexity of reverse engineering, making it extremely difficult to extract sensible data.

4. DATA PROTECTION

At the most basic level of data security, hardware and software applications achieve protection from viruses or hackers through write protection and password access protection. These isolate the Operating System (OS), applications, and critical data from corruption or infiltration by external sources. Write and password protecting a drive can be meaningful in applications where the end user is not allowed to tamper with the contents of the data.

4.1 Hardware Write Protection

Write protection prevents data modification on a storage device. It is typically enforced by the hardware through a jumper or switch and implemented through a hardware protection mechanism inside the controller of the SSD. In this case, a protection state machine inside the controller blocks writes to the media.

4.2 Software Write Protection

Software write protection can be implemented through the firmware of the storage device, whereby the host can set or remove the write protection via a host (vendor-unique) command to the drive. Software password protection is suitable when implementing a security scheme that is based on “what you have, what you know, who you are” [12]. For example, when only authorized personnel are allowed to download mission data from a data recorder, a combined password protection and biometric key would provide a secure identification scheme. In this case, the password would deliver the “what you know,” and a biometric key would cover the “what you have” and “who you are.”

4.2.1 Password Protection in SMART HRS Solid State Drives

The password protection feature on SMART HRS solid state drives is implemented through the standard ATA command set [5] and supports both a user and master password. When used for data logging purposes, the device can be locked or unlocked at boot time when used as the boot device, or once an application is loaded.

- Password protection during boot: When the SMART HRS solid state drive is used as the boot device, password protection is implemented in combination with the BIOS of the host system. The BIOS will need to incorporate the ATA commands that enable the usage of the password scheme. During the system boot process, the user must successfully enter a password to the system; otherwise the system will not continue booting.
- Password protection during operation: When the SMART HRS solid state drive is used for data logging purposes, standard ATA security commands are used for locking and unlocking the device.

After five unsuccessful attempts of entering a password, the drive will have to be rebooted before new attempts can be made. These include both user and master password attempts.

4.3 Encryption

Another form of data protection is encryption, whereby the original data, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext.

When using the most common encryption algorithms, such as RSA, AES and 3DES, it is virtually impossible to recover any data from a storage device, providing a high form of security. For example, to break an AES 128-bit encryption, a “brute-force” attack with a system that tries keys at the rate of one billion keys per second will take about 10,000,000,000,000,000,000,000 years to try all possible keys [6].

The main hurdle that has prevented encryption from being integrated full scale into host applications and storage devices is related to key management. Creating strong and secure keys appears to be surprisingly difficult. The challenge is that most systems are notoriously deterministic, but what is required of a good and strong key is the opposite – unpredictability and randomness. In addition, it is not a trivial matter to provide a secure method of key storage and distribution without running the risk of keys being tampered with or stolen.

Most modern SSDs incorporate some form of encryption on the data they write to the NAND Flash. Since the SSD internally manages all the elements of the encryption from the key generation, to the key storage, to key deletion, they are called Self-Encrypting Drives (SEDs). In itself, an SED does not offer much data protection except deleting the encryption key in milliseconds, but when combined with other data protection features such as passwords, it provides an additional layer of data protection.

5. DATA ELIMINATION

As the repository for data and programs, Flash solid state drives are critical electronic components in a defense computing system. For this reason, all branches of the military have spent significant time and effort developing standards for what has become known as Secure Erase features in data storage. These standards were originally set in two documents – the Department of Defense (DoD) 5200.28 and the National Security Agency (NSA) CSS 130-2, Media Declassification and Destruction Manual. Other branches of the US military have created other data elimination specifications drawn from the DoD and NSA instructions.

Sanitizing or Clearing a solid state drive provides a fast means for data declassification, without the need for degaussing or disk destruction as is the case with mechanical hard disk drives. A particular advantage of these operations in solid state drives is the ability to perform the operations without having physical access to the drive as is the case with degaussing or destruction of a hard disk drive. This makes the declassification procedures quicker, easier and more cost-effective for solid state drives.

A distinction has been made between a Clear operation and a Sanitize (or Purge) operation:

- Clear: Clearing is the process of erasing data on the media. In a Flash SSD, this is done be executing a block-by-block erase with or without verify. SMART HRS SDET implements that block-by-block erase on physical block level vs. logical block level.
- Sanitize (also known as Purge): Sanitizing is the process of declassifying the drive by executing an unrecoverable removal of all data on the media. In a solid state drive, this initiates a sequence of block-by-block erase, pattern write and pattern verify operations designed to eliminate any traces of the original data. Since data remanence in solid state drives is far less prevalent, a Sanitize procedure with few repeats will not leave a “ghost-image” behind on the drive, making it impossible to recover any data that was present on the drive.

Table 1 below provides an overview of the various military standards that define how data elimination is executed on a disk drive, regardless of the underlying media.

Table 1: Security Erase Military Standards

Procedure	Standard	Action
Clear		All data on the media is erased
Sanitize/ Purge	DoD (U.S. Department of Defense, National Security Program Operating Manual): DoD NISPOM 5220.22-M, January 1995	Erase the media and overwrite with single character, then erase again
Sanitize/ Purge	DoD (U.S. Department of Defense, National Security Program Operating Manual): DoD NISPOM 5220.22-M-Sup 1, February 1995	Erase the media and overwrite with single character, then erase again and overwrite with single character, then erase again and overwrite with random character, then erase again
Sanitize/ Purge	NSA (U.S. National Security Agency): NSA/CSS Manual 130-2, 10 November 2000	Erase the media and overwrite with random data 2 times, then erase and overwrite with a character
Sanitize/ Purge	NSA (U.S. National Security Agency): NSA/CSS Manual 9-12, December 2007	Erase the media and overwrite with known pattern
Sanitize/ Purge	U.S. Air Force: AFSSI-5220, 20 August 1996	Erase the media and overwrite with pattern, repeat 3 times
Sanitize/ Purge	U.S. Air Force: AFSSI-5020, 17 April 2003	Perform 6 passes of the following steps: erase the media and overwrite it with single character, erase the media, and overwrite it with the complement of the previous character, erase the media and overwrite it with a single character
Sanitize/ Purge	U.S Army: AR 380-19 15, 27 February 1998	Erase the media na doverwrite with random data, erase and overwrite with a character, then erase and overwrite with complement of the character
Sanitize/ Purge	U.S. Navy: NAVSO P-5239-26, September 1993	Erase the media and overwrite with random data, then erase again
Sanitize/ Purge	RCC-TG (Range Commanders Council Telemetry Group): IRIG 106-15, July 2015	Erase the media, overwrite with 0x55, erase, overwrite with 0xAA, and then erase again. Then fill the drive with a repeating string of Secure Erase
Fast Clear		All data on the media is erased simultaneously

5.1 Security Disposition

Depending on the security categorization of the organization where the solid state drive is deployed, the chosen procedure of data elimination or destruction can vary, as described below and shown in Figure 3:

- **Low Security Disposition:** If the security categorization is defined as CONFIDENTIAL, a Clear or Sanitize procedure is required. If the drive will leave the organization, it will be moved to a higher classification level (moving to a lower classification level is not allowed, unless the drive is destroyed) and as such, a full Sanitize procedure is required. If the drive stays within the organization and at the same classification level, a Clear procedure will suffice
- **Moderate Security Disposition:** If the security categorization is defined as SECRET, complete destruction of the media may be required, depending on whether the media needs to be reused or not. If the media is meant to be used again, a Clear or Sanitize procedure is required. If the drive is leaving the organization and moving to a higher classification level, a full Sanitize procedure is required. If the drive stays within the organization and at the same classification level, a Clear procedure will suffice
- **High Security Disposition:** If the security categorization is defined as TOP SECRET, complete destruction of the media may be required, depending on whether the media needs to be reused or not. If the media is meant to be used again, a Sanitize procedure is required. A Clear procedure is not recommended for High-Security Disposition.

Figure 3: Security disposition flow chart

5.2 IRIG 106-15

The DoD and NSA defined the security erase standards for storage devices in an era where hard disk drives were the main storage media. Hence, the standards focused on declassification of standard disk and other conventional memory technologies. With the advent of advanced, high-density memory technologies, such as NAND Flash, new standards were required.

The Inter Range Instrumentation Group (IRIG) is the standards body of the Range Commander Council (RCC). The Telemetry Group of the Range Commander Council specified a new standard, called IRIG 106-15, chapter 10.8 [8] to define the operation and interfaces for digital flight recorders. It specifically addresses NAND Flash architecture and data structures, defines for bad block handling, and allows for reviewing the secure erase results to verify that all classified data has been eliminated. SDET embedded within certain enabled SMART HRS solid state drives, is fully compliant to the IRIG 106-15 standard.

5.3 SMART HRS Secure Data Elimination Technology (SDET)

SMART HRS Secure Data Elimination Technology (SDET) provides fast Clear and Sanitize options for any capacity solid state drive. Clear and Sanitize provide different levels of data security and performance, and thus provide different levels of protection against compromising sensitive data.

SDET operates on a physical block level as opposed to logical block level. This means that all Erase Blocks within the drive, including those that contain data structures, mapping tables or any other blocks used for flash management purposes, are erased during an SDET operation. To return the drive to a state that it can be reused after an SDET procedure, the drive must undergo an Initialize Drive operation. SDET supports the following data elimination procedures:

- **SDET Fast Clear:** This is the fastest level of data elimination. It performs a single erase of the data from the solid state drive, followed by an automatic initialization drive procedure. The drive is completely reusable at the end of this procedure.

- **SDET Clear:** This is the second fastest level of data elimination. It performs a single erase of the data from the solid state drive, after which the drive is completely reusable following an initialization drive procedure. The initialization procedure is not executed automatically and must be called through a host command.
- **SDET Sanitize:** Typically, each Flash array inside the solid state drive is simultaneously cleared of data and then overwritten one or more times, using one of several pre-programmed procedures or a customized Sanitize procedure. After a Sanitize procedure, the solid state drive is reusable following an Initialize Drive procedure. Depending on the chosen SDET procedure, Sanitization of the drive can take minutes to hours.

SDET complies with all military standards shown in Table 1, including full support for IRIG 106-15, chapter 10.8. In addition, SDET supports a custom-defined procedure with up to 30 steps.

An SDET operation can be triggered by either a software host command or a hardware input. It is possible to connect a pushbutton or other actuator to manually initiate a configured SDET procedure.

Once the command is issued, the SDET-enabled solid state drive indicates progress through an LED status notification. In addition, it is possible to track the progress (percent of completion) of the secure erase operation through an ATA command.

If an SDET procedure is interrupted by removing power to the drive (or any other means), the built-in Auto-Resume feature ensures that the SDET procedure automatically resumes at the same point when power is restored to the drive. This is accomplished by storing various “save points” at key steps in the SDET procedure. When the SDET-enabled solid state drive reboots, the controller resumes the SDET procedure at the last step indicated by the save point.

Note: Please refer to SMART HRS SDET Programmer’s Guide [9] for full details on the SDET command set and configuration.

5.4 SDET Block Management

An Erase Block of 4MBytes is the minimum unit of data that can be erased. NAND Flash is shipped by Flash manufacturers and can contain bad Erase Blocks – areas on the Flash that cannot be used for read/write operations. Additional Bad Blocks are accumulated during standard read/write operations. In order to provide complete Sanitize capabilities, solid state drive vendors must effectively manage Bad Blocks that may contain sensitive data.

Flash management algorithms assign Erase Blocks for different purposes and containing different types of data, as described in Table 2 below.

Table 2: Block Definition

Block	Usage	Content
User Data plus Overpro-visioned Space	Write and read areas for the user. Equals the available capacity on the solid state drive and additional blocks which could be old-stale user data, or erased waiting to hold new user data	Contains user data
Failed	Retired User Data block. Also known as accumulated Bad Block	Can contain old user data
Factory Defect	Marked by Flash chip manufacturer as non-functional. Also known as Bad Block	Never used by SDET solid state drive, and does not contain data
Buffer	Erased blocks that accept new user data. The content is later merged with User Data block and is not part of the solid state drive capacity	Contains new user data
Reserved	Holds control and configuration information for each Flash controller	Contains firmware and control structures, but no user data

Any SDET sanitize procedure erases and overwrites all of the above mentioned block types, and keeps track of the erase status of each block through an Erase Block database. If an Erase Block fails to erase or write during a Sanitize process, it will be processed outside of the standard flow.

5.4.1 Implementing and Verifying EraSure

As mentioned in section 5.3, SDET procedures can be triggered via a software host command or a hardware input. Regardless of the trigger method, the OEM host computer requires a device driver to support the following functionality:

1. Program the selection for the desired SDET procedure. May be done real time or prior to a mission
2. Trigger the pre-selected SDET procedure by software command or hardware trigger
3. Issue commands to verify the execution of the SDET procedure
4. Issue a command that reinitializes the drive after an SDET procedure

Note: Please refer to SDET Programmer's Guide for full details on the command set. To verify the validation of an SDET procedure during design stage, the following steps are recommended:

1. Interrupt the power during the SDET procedure to validate the recovery and continuation of the process (SDET will resume the procedure when power is restored)
2. Validate the non-stop progress by attempting to interrupt and stop the procedure
3. Verify the absence of all known data within all the Erase Blocks, as defined in Table 2. This can be done through the host computer interface (SDET command) or by removing the Flash chips to independently verify the data content.

6. MEDIA DESTRUCTION

Different military specifications call for different media destruction procedures. The NSA 130-2 specification [2] requires the use of degaussers for magnetic disk drives, after which the drives can be disposed of through shredding or burning. It does not specify anything for solid state drives and refers to Clear and Sanitize procedures to ensure complete data elimination.

A more stringent specification is the NAVSO P-5239-26 standard [10], which calls for a variety of hard disk drives destruction techniques, ranging from degaussing to sand blasting or chemically destroying the disk. Besides the common Sanitize techniques, no specification is provided for media destruction of solid state drives.

In certain cases, standard sanitization techniques are not adequate for the application due to timing constraints. If the data must be eliminated in a matter of seconds, other methods, such as physical destruction of the media, may be applied. These media destruction methods are not practical to deploy on mobile military vehicles, such as planes, tanks, and boats; therefore, media destruction is generally performed in laboratory environment.

7. CHOOSING THE RIGHT SECURITY TECHNOLOGY

Choosing the correct SDET procedure depends on many factors. Two illustrative examples are presented below.

7.1 Data Recorder in a Tank

The solid state drive inside the data recorder of a tank captures data during training sessions at a military base inside neutral territory. Once the training session is over, the tank commander takes the drive out of its enclosure inside the tank and returns it to a secure place on the base.

The data that is captured during the session needs to be declassified, although the highest security level is not required as the drive remains inside the premises of the base. Since the tank commander does not want to wait hours for the drive to be declassified, a Fast Clear procedure, where the data on the drive is erased and the drive is reformatted in a matter of seconds, will suffice.

The situation would change if the drive were to be transferred to another program or military base, and would have to undergo a more stringent declassification procedure. In that case, a Sanitize procedure, according to IRIG 106-15, would be more appropriate. Since this procedure takes a few hours, it should only be implemented only for occasions like this.

As can be seen from the above example, the drive would have to support two different procedures in order to support two different usage scenarios.

Figure 6: Tank commander

8. CONCLUSION

Various methods exist for data protection and elimination depending on the security level required within an organization. Many defense applications require the functionality provided by SMART HRS Secure Data Elimination Technology (SDET).

Securing confidential data in emergency situations is essential. The damage that may result if confidential information falls into the wrong hands can be devastating. Sanitizing mechanical hard disks is an arduous process, requiring special degaussers, stable power conditions during the process, and ample time, all of which may be lacking during an emergency. Solid state Flash drives are better suited for this task, and can be erased in seconds using Clear procedures. When the drive is used in a medium-to-high security categorization, a Sanitize procedure may be required. Depending on the military specification that is implemented, declassifying a solid state drive in a Sanitize procedure can take minutes to hours.

The Clear and Sanitize commands implemented within SMART HRS SDET-enabled solid state drives provide the performance and erase levels required by all U.S.A. defense organizations.

9. REFERENCES

[1] www.cnn.com, U.S. surveillance plane lands in China after collision with fighter, April 1, 2001.

[2] NSA/CCS Manual 130-2, Media Declassification and Destruction Manual.

[3] Peter Gutmann. Data remanence in Semiconductor Devices, proceedings of USENIX Security Symposium, Washington DC, August 2001

[4] Peter Gutmann. Secure Deletion of Data from Magnetic and Solid State Memory, proceedings of USENIX Security Symposium, San Jose, CA, July 1996

[5] ATA/ATAPI-7, 1410D Volume 2, Revision 0, 5 November 2001, section 2.7

[6] About AES – Advanced Encryption Standard, A short introduction, August 2007, Svante Seleborg, Axantum Software AB

[7] http://www.taonline.com/securityclearances/, Types of Security Clearance.

[8] RCC Document 106-15, Telemetry Standard, Chapter 10.8, Digital Recording Standard, July 2015

[9] Adtron EraSure Data Security, Secure Erase Programmer's Guide, November 2007

[10] NAVSO P-5239-26, Information Systems Security (INFOSEC) Program Guidelines, Naval Information Systems Management Center, http://www.fas.org/irp/doddir/navy/5239_26.htm

[11] Failure Analysis Report H09154, MEFAS Lab, Lake Forest, CA

[12] www.computer.org, Biometric Authentication, Alfred C. Weaver, University of Virginia, Feb 2006.

SMART High Reliability Solutions

SMART High Reliability Solution (SHRS) is a market pioneer of secure, ruggedized SSDs and continues to be a technology leader employing current and next-generation defense focused designs backed with proven world-class support of its solid state drives. Utilizing Flash technology, SHRS designs and manufactures high performance military and industrial SSDs with additional attributes such as encryption, secure data elimination and write-protect features. SHRS understands and solves customers' key requirements, leveraging its long heritage of established, generational SSD design. SMART High Reliability Solutions is part of the SMART family of global companies.

Learn more about SMART HRS at www.smarth.com

Headquarters: T: (+1) 800.956.7627 • T: (+1) 510.623.1231 • F: (+1) 510.623.1434 • E: info@smarth.com

Customer Service: T: (+1) 510.624.5379 • F: (+1) 480.926.5579 • E: info@smarth.com

Europe: T: (+44) (0)1592.760426 • E: info@smarth.com

Asia/Pacific: T: (+65) 6232.2858 • F: (+65) 6232.2300 • E: info@smarth.com

10.02.17/SecurityFeaturesForSSDs_WhitePaper/Rev.2