NATO STANDARD

AEDP-3

ADVANCED DATA STORAGE TECHNOLOGY
MEMORY SYSTEMS SANITIZATION GUIDANCE

Edition C Version 2
AUGUST 2016

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING DOCUMENTATION PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

© NATO/OTAN

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

16 August 2016

1. The enclosed Allied Engineering Documentation Publication AEDP-3, Edition C, Version 2, ADVANCED DATA STORAGE TECHNOLOGY MEMORY SYSTEMS SANITIZATION GUIDANCE, which has been approved by the nations in the Joint Capability Group on ISR (JCGISR) is promulgated herewith. The recommendation of nations to use this publication is recorded in STANREC 4750.

2. AEDP-3 Edition C, Version 2, is effective upon receipt and supersedes AEDP-3, Edition C, Version 1 which should be destroyed in accordance with the local procedure for destroying documents.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member nations or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1. FORWARD

This document was prepared by the NATO Advanced Data Storage Interface Custodial Support Team (NADSI CST) in response to user community requests for guidance on proper data purge and sanitization techniques for advanced technology memory systems. In particular, this document addresses Flash Memory, Solid State Disks (SSD) and advanced magnetic disks and disk array storage devices used in ISR systems. This information is provided as guidance and national requirements may supersede this document. This edition revises AEDP-3, edition 2 to address revised NATO directives and instructions, provide updated procedures for technology changes and to correct terminology.

This document provides sanitization procedures and defines sanitization levels for storage media used in ISR acquisition and ground systems. Sanitization is the technical basis for declassification. Declassification policies, directives and guidance are found in the referenced NATO INFOSEC documents.

Questions or comments should be directed to the Custodian of this document. The Custodian is also the Custodian for STANAG 4575. Inquiries can be addressed to:

Custodian, AEDP-3
SAF/AQIJ
1060 Air Force Pentagon
Washington D.C. 20330-1060
United States
Telephone: +1 571-256-0104
Telefax:

1.2. BACKGROUND

The NATO Advanced Data Storage Interface (NADSI) working group has identified the Sanitization of non-volatile solid state, high density magnetic disks, and RAID memory elements as an important issue in the ISR user community. Command infrastructure and functional capability to perform the necessary operations need to be included in any system that is required to sanitize data storage elements. Incorporating this capability during the system requirements definition and design phase is the most effective approach. Sanitization times for these technologies, which incorporate large storage capacities, can be significant and efficient means of sanitization should be addressed during the design process. This AEDP provides the sanitization guidelines for Solid State Recorder (SSR) flash memory, Solid State Disks (SSD), RAID, and magnetic hard disk data storage systems. This AEDP also provides Guidance for data encryption associated with cryptographic erase of memory modules.

1.2.1. Applicability

This document and the included procedures are applicable to Removable Memory Modules (RMM) which incorporate Solid State Recorder flash memory, Solid State Disks and RAID/magnetic Disk data storage systems that are used to store unexploited Intelligence, Surveillance, and Reconnaissance (ISR) data. ISR data has a high time value. This data is significantly different from general Computer Information System (CIS) data and the characteristics of ISR data have been considered in defining the included sanitization procedures. Sanitization is the technical basis for eliminating data from media in order to declassify it. In addition, NATO INFOSEC declassification directives and instructions apply to all classified data storage elements in the NATO environment and should be reviewed and applied as appropriate.

1.3. REFERENCES

1.3.1. Reference Terms

The following terms are defined for the purpose of clarity in this STANREC. Specific procedures and methods related to sanitization terms are provided in Chapter 3.

1. Advanced Data Storage Technology (ADST): Data storage technologies which may include magnetic, solid state, optical, molecular as well as future technologies.

2. Assurance Levels: High and low assurance levels relate to the confidence that data eliminated from an RMM is unrecoverable. High assurance generally relates to a “Purge” operation while low assurance relates to a “Clear” operation.

3. Removable Memory Module(s) (RMM). The RMM is the removable memory element of an ADST recorder which incorporates the STANAG 4575 interface in a STANAG 4575 compliant system

4. Clear: The process of removing information from a storage media, using a technologically appropriate procedure, such that it protects the confidentiality of data from being recovered using ordinary system commands or by data, disk or file recovery utilities.

5. Cryptographic Erase (CE): Leverages the encryption of target data by enabling sanitization of the target data’s encryption key. Elimination of the key leaves only the ciphertext on the media, effectively sanitizing the data.

6. Declassify: The procedure used to cancel the security classification of an item of classified matter or material. (See AAP-6(V)) Declassification includes the removal of data from the media, verification of data removal and the removal of all classified labels, markings and the completion of appropriate documentation.

7. Delete: To remove data from the media.

8. Destroy: Physical destruction of the media rendering it unusable and un-readable and rendering the stored data unrecoverable by any means.

9. Downgrade: To reduce the security classification of a classified document or an item of classified matter or material. (APP-6(V)).

10. Enhanced Secure Erase (ESE): A positive command that results in the automatic overwriting of all data on magnetic disks with an acceptable pattern, including areas that have been previously mapped out of active memory.

11. Erase: The elimination of existing data in preparation for re-use of the media element. Erasure is accomplished by a technologically appropriate procedure for a given memory technology.

12. Overwrite: Recording of data over all previously recorded user data within a storage media using a known pattern such as PRD.

13. PRD: Pseudo-Random-Data sequence such as a 2e23-1 bit sequence.

14. Purge: The process of removing information from a storage media, using a technologically appropriate procedure, that makes data recovery impossible by any known means.

15. Sanitize: The deliberate, permanent elimination of stored data, or destruction of a media element, such that data recovery by any known technique is prevented.

16. Secure Erase (SE): A positive command that initiates a procedure, resulting in the automatic overwriting of all user data on magnetic disks with an acceptable pattern.

17. Self-Encrypting Drives (SED): Storage devices with integrated encryption and access control capability which features always-on encryption. It allows the use of cryptographic erase that can be accomplished very quickly and substantially reduces the likelihood of unencrypted data being retained on the device.

18. Trusted Security Group: TCG Opal SSC and the TCG Enterprise SSC are referenced in this document and represent the Security Subsystem Class for encryption and cryptographic erase. The TCG maintains the recommended standards for these security classes.

1.3.2. Reference Documents

The following reference documents provide policy and guidance for declassification of storage media:

1. #AC/35-D/2002-REV2 - Directive on the SECURITY of INFORMATION

2. #AC/35-D/2005 - INFOSEC MANAGEMENT DIRECTIVE FOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

3. AAP-6(V) –NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH)

4. STANAG 4575-NATO ADVANCED DATA STORAGE INTERFACE (NADSI)

5. NIST special Publication 800-38A, Media Encryption

6. NIST Special Publication 800-88 –Revision 1, Guidelines for Media Sanitization

7. NIST Special publication 800-90, Cryptographic Key Generation

CHAPTER 2 CONSIDERATIONS FOR SANITIZATION OF ADST MEMORY SYSTEMS

2.1. SANITIZATION PROCEDURE GUIDANCE

This AEDP provides the technical procedures for Sanitization of SSR, SSD and Magnetic Disk media used in ISR tactical applications. Specific sanitization steps are given for Flash solid state, solid State Disk and magnetic disk based media used to store unexploited ISR data. System specific criteria and procedures for Sanitization must be established and documented in accordance with NATO and Country directives and policies. Normal erase and re-initialization procedure for the media (i.e. CLEAR, which is generally considered low assurance level) is recommended as a minimum for normal storage, handling, and reuse of ADST memory devices. Users of STANAG 4575 and related standards, AEDPs, and handbooks may reference these Sanitization recommendations.

2.2. ADST MEMORY ACQUISITION CONSIDERATIONS

Acquisition managers should insure that the interfaces, control options, command structure, OS, and/or BIOS of procured data storage devices are capable of supporting the sanitization requirements of this AEDP in their systems. A positive means to identify, verify, and document that the procedures were followed and the expected level of sanitization was performed to completion, on the data storage device/media, is required in order to reduce the risk of releasing classified data. This capability should be incorporated into devices and systems that use the ADST memory device. In addition to addressing the sanitization of ADST memories, a physical or logically set “Record Inhibit” function should be considered for incorporation into the RMM’s NADSI port, to prohibit the recording of any data when the RMM is connected to a classified ground system via the NADSI port for data download, so that unclassified RMM memories remain unclassified. Also, it is recommended that the desirable functionality of identifying and addressing failed bytes and sectors during sanitization be incorporated into the system requirements when practical. The media type incorporated into the RMM must also be considered when incorporating and/or approving specific sanitization techniques.

2.3. OPTIONAL NADSI COMMANDS

The NADSI STANAG provides a list of both required (minimum) and allowed SCSI and iSCSI commands. Systems using the NADSI interface may implement any of the allowed commands via the NADSI interface, the system interface, or both. The native system interface should provide for the use of all commands that allow Sanitization of the ADST memory device. The sanitization of a storage media may be accomplished using multiple methods. Since there is no single “Sanitize” command that addresses these sanitization guidelines for all media types, a multi-step process, which is controlled by the data storage device or system, may be used; along with provisions for producing the appropriate overwrite data patterns and verifying successful sanitization. Commands used for sanitizing media may include “Format”, “Secure Erase”, “Enhanced Secure Erase” “Erase”, “Record”, “Write” or “Overwrite” commands used in an appropriate sequence, if supported by the RMM. In addition, a separate controller or work station, connected directly to the RMM’s native interface, could be used to implement the data purge function, which would not require the use of the native/primary data recording or reconstruction system.

2.4. MEDIA SANITIZATION APPROACHES

2.4.1. Sanitization Command Definitions

The sanitization command definitions are provided in Table 1.

Table 1: Sanitization Command Definitions

Command	*Definition*
Overwrite	Writing one or more patterns of data on top of the physical location of data stored on the media. May be performed through manual operations or automatically.
Cryptographic Erase	A method of Sanitization in which the Media Encryption Key (MEK) for the encrypted Target Data is sanitized, making recovery of the decrypted Target Data infeasible.
Erase	Process intended to render magnetically stored information irretrievable by normal means.
Sanitize Command	A command in the ATA and SCSI standards that leverages a firmware-based process to perform a Sanitization action. If a device supports the sanitize command, the device must support at least one of three options: overwriting, block erase (usually for flash-based media), or crypto scramble (Cryptographic Erase). These commands typically execute substantially faster than attempting to rewrite through the native read and write interface. The ATA standard clearly identifies that the Sanitization operations must address user data areas, user data areas not currently allocated (including “previously allocated areas and physical sectors that have become inaccessible”), and user data caches. The resulting media contents vary based on the command used. The overwrite command allows the user to specify the data pattern applied to the media, so that pattern (or the inverse of that pattern, if chosen) will be written to the media (although the actual contents of the media may vary due to encoding). The result of the block erase command is vendor unique, but will likely be 0s or 1s. The result of the crypto scramble command is vendor unique, but will likely be the ciphertext of the encrypted data (except for areas that were not encrypted, which are set to the value the vendor defines).
Secure Erase Command	An overwrite command in the ATA standard (as ‘Security Erase’) that leverages a firmware-based process to overwrite the media. This command typically executes substantially faster than attempting to rewrite through the native read and write interface. There are up to two options, ‘normal erase’ and ‘enhanced erase’. The normal erase, as defined in the standard, is only required to address data in the contents of LBA 0 through the greater of READ NATIVE MAX or READ NATIVE MAX EXT, and replaces the contents with 0s or 1s. The enhanced erase command specifies that, “…all previously written user data shall be overwritten, including sectors that are no longer in use due to reallocation” and the contents of the media following Sanitization are vendor unique. The actual action performed by an enhanced erase varies by vendor and model, and could include a variety of actions that have varying levels of effectiveness. The secure erase command is not defined in the SCSI standard, so it does not apply to media with a SCSI interface.

2.4.2. Self-Encrypting Drives (SED):

Many storage manufacturers have released storage devices with integrated encryption and access control capabilities, also known as Self-Encrypting Drives (SEDs). SEDs feature always-on encryption that substantially reduces the likelihood that unencrypted data is inadvertently retained on the device after Cryptographic Erase. Cryptographic erase provides a method for quick sanitization. The end user cannot turn off the encryption capabilities which ensure that all data in the designated areas is encrypted. A significant additional benefit of SEDs is the opportunity to tightly couple the controller and storage media so that the device can directly address the location where any cryptographic keys are stored, whereas solutions that depend only on the user access interface to the key through software may not be able to directly address those areas. SEDs typically encrypt all of the user-addressable area, with the potential exception of clearly identified areas dedicated to the storage of pre-boot applications and associated data.

2.4.3. Cryptographic Erase (CE)

Cryptographic Erase leverages the encryption of target data by enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data. As a result, sanitization of the target data is reduced to sanitization of the encryption key(s) used to encrypt the target data. Thus, with CE, sanitization may be performed with high assurance much faster than with any other sanitization techniques. The encryption itself acts to sanitize the data, subject to constraints identified in the referenced NIST 800-88 guidelines document.
Federal agencies must use FIPS 140 validated encryption modules in order to have assurance that the conditions stated above have been validated for the SED.
Typically, CE can be executed in seconds. This is especially important as storage devices get larger, resulting in other sanitization methods taking much more time. CE can also be used as a supplement or addition to other sanitization approaches. CE should only be used when all data on an RMM has been automatically encrypted.

2.4.4. Encryption and Cryptographic Erase (CE) Requirements

In order to use CE for sanitization, both the encryption and the CE shall meet the requirements of NIST 800-88. These requirements include media encryption, Key generation and key level wrapping. An example of the requirement is media encryption with AES 256 media encryption in CBC mode as described in NIST SP800-38A and key generation as specified in NIST SP800-90. An example of the key sanitization technique would be overwrite of the key three times with a pattern that is inverted between passes and then verification of the overwrite.

2.4.5. Verification of Sanitization

Verifying the sanitization process is an essential step in maintaining confidentiality and is always a required step in the PURGE procedures. Two types of verification should be considered. The first is full media verification. The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action or executed by an approved software tool. See Paragraph 3.4 for verification procedures.

NOTES:

1. Verification Considerations

   a. Verification of the sanitization process is not the only assurance required by the organization. If the organization is using sanitization tools (e.g., a dedicated workstation), then equipment testing, and scheduled calibration and maintenance, is also needed.

   b. Verification of Personnel Competencies
   Another key element is the potential training needs and current expertise of personnel conducting the sanitization. Organizations should ensure that equipment operators are properly trained and "certified" to perform sanitization functions.

2.4.6. Partial Sanitization

Partial sanitization is the removal of specific files from the media while leaving others. Due to the difficulty in reliably ensuring that partial sanitization effectively addresses all sensitive data it should not be used.

2.5. FAILED DATA CELLS

It is not the intent of this document to limit the manufacturer's methods of providing error free data to the user. It is necessary for a program to provide, and the security officer to evaluate, the capability to make residual data unusable or valueless to an adversary. In the case of failed data blocks, "bad block mapping", "Error Correction Coding", "randomization", or other methods may be incorporated into the manufacturer's design of the ADST memory system and be employed in normal data recording operation, regardless of the technology used. Each of these design elements should be considered when establishing sanitization procedures since their incorporation makes recovery of any data difficult or impossible from failed cells.

It is recommended that all data in the memory element be overwritten during sanitization, including bad blocks. However, the security officer must evaluate the risk of ignoring bad blocks during sanitization procedures, based on the technology used and the data stored. This risk is likely to be low in ISR RMMs that incorporate both randomization and encoding.

The security officer must consider the impact of failed Bytes, Blocks and Sectors when determining the declassification requirements for an RMM. This includes data type, time value of the data, recording techniques (including encoding and error detection encoding and the type of storage media incorporated). When the storage blocks are small and the data is in large segments (i.e. Imagery Data on an ADST memory device), and the failed data block is uncorrectable and unrelated to other data stored in adjacent blocks or elsewhere in the RMM, the failed blocks would be useless for imagery reconstruction. Failed bytes which have been made inactive due to failed bit cells are unlikely to contain any recoverable data. In these cases, subsequent recovery of corrupted bytes would not allow any data reconstruction and the risk of ignoring them is very low.

2.6. SECURITY OFFICER ASSESSMENT

Situational analysis by Security Officers and Program Managers is required to determine how to best apply the sanitization guidance in this document to the downgrading or declassification of ADST memory devices in accordance with NATO directives. Removing data from a memory element or ultimately physically destroying the media is only the first step in sanitizing and subsequently declassifying it. All markings, records and logs for the data and ADST memory device must also be removed and eliminated. Once the memory has been purged or destroyed, the responsible Security Officer will assess the risk of declaring the memory element “declassified” and determine if the required procedures have been properly followed and the documentation properly completed. The procedures for a specific system must include a clear definition of the criteria to be used to verify that the memory is sanitized and must identify all forms and records that need to be completed. The assessment must be made and the documentation verified prior to declaring the memory declassified and releasable. If physical destruction is required in an emergency situation, established procedures should be used and destruction should be verified to the extent possible.

2.7. ORGANIZATIONAL CONTROL OF MEDIA

A factor influencing an organizational sanitization and security downgrading decision is who has control of and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned for repair, update, and modification or are provided to another user of the RMM. The following are examples of media control:

Under Organization Control:

- Media being used and stored within a system or between an ISR acquisition platform and ground system and stored in a controlled environment
- Maintenance, repair or update being performed on an organization’s site, under the organization’s supervision by their personnel or a maintenance provider

Not Under Organization Control:

- Media or a complete RMM that is being returned to the manufacturer or support site for repair, warranty, or other purposes and where the specific media may be accessible by others or not be returned to the organization that provided it

- Media or a complete RMM that is not stored in a controlled environment by the organization
- Media or a complete RMM that is transferred or loaned to another user or operational entity

CHAPTER 3 MEDIA SANITIZATION GUIDANCE

3.1. APPROACH

The sanitization guidance defined herein is to be applied based on the risk, threat, and operational situation. Levels of media sanitization are defined below and are to be supported in procured NATO ADST hardware and software. Guidance for their use with FLASH solid state memories, Solid State Disks and Magnetic Disk based memories is provided herein. Those NATO nations and the officers responsible for the development and deployment of systems must determine applicability of the guidelines to each nation's data storage systems based on their own policies and NATO guidelines.

3.2. SANITIZATION LEVELS

Three levels of sanitization are defined below. Implementation of these levels is different for each specific technology and RMM implementation. Technical requirements for sanitization procedures related to specific technologies are provided in subsequent paragraphs.
Note that a basic file deletion does not qualify as any form of sanitization. While this operation may remove the "deleted" file's metadata, the contents of the file are generally left untouched and are therefore vulnerable to recovery using trivial means.

Level #1 - Clear is an "Erase" of the entire directory and entire data storage element using a technologically appropriate and verified procedure. Notes in subsequent paragraphs provide details related to specific technologies. All operations must be run to completion to ensure a complete data erasure.

Level #2 – Purge - A level of sanitization that applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques. Data Purge can be accomplished by using technologically appropriate procedures to overwrite previously recorded data with a known "unclassified" pattern and verifying that the known pattern was written and the "purge" process has been properly completed. Some media types will require an erase or re-format cycle prior to writing new data. Specific requirements for different media types are defined in the following paragraphs. Alternatively, Cryptographic Erase followed by an acceptable verification may be used as defined in subsequent paragraphs, to purge data.

Level # 3-Destroy - The complete destruction of the storage media. Implementing the procedure for Levels 1 and 2 results in a re-useable memory media element while, level #3 will not. In the case of an imminent threat situation (and in particular, if accompanied by a power loss), destruction or physical damage to the media may be the most immediate and appropriate security action. Destruction of the media precludes normal verification although the destruction method should be verified and approved for the specific media type.

3.2.1. Overwrite Data Type

Recording of overwrite data may be accomplished by recording any verifiable data pattern. A Pseudo-Random Data sequence (PRD) such as 2e23-1 is acceptable. When block erase is used to overwrite FLASH memory the erase pattern can be used for verification.

3.2.2. Sanitization Alternatives and Approach

Multiple implementations and approaches may be used for each level of sanitization. Command structures such as SECURE ERASE, or Cryptographic Erase can be incorporated into and verified in the RMM command structure. Automatic Operational Procedures used in a ground system or work station to sanitize the RMM can be incorporated as a SANITIZE command that incorporates routines and/or procedures in software/hardware control to sanitize the media using approved procedures such as overwrite and then verify the addressable media within the RMM. Manual Sanitization Control Procedures which are operator initiated and use allowable commands for the RMM/media can also be used to perform appropriate Sanitization procedures on the media.

3.3. SPECIFIC TECHNOLOGY SANITIZATION GUIDANCE

The procedures defined below for media sanitization are currently recommended. The risk that proper and appropriate level of sanitization has been effectively implemented will ultimately reside with the user/customer/ program/security manager. It is anticipated that the acquisition Program Manager will verify by test and demonstration (i.e. First Article Inspection/Test) that any ADST memory that is developed, will properly implement appropriate sanitization procedures that are defined in this document. The program Security Officer will determine or approve the specific Sanitization procedures for any program situation. It is their responsibility to correctly apply the guidelines in this AEDP to the program, to optimize the cost/effect/risk while providing appropriate protection for the data.

3.3.1. FLASH Solid State Memory Sanitization Procedures

The levels of sanitization identified below are to be applied for FLASH memory based RMMs. This implies that all of the user addressable memory in the RMM is FLASH Solid State memory and that the RMM is a custom design for a specific application.

Level #1 - Clear – Overwrite media by using organizationally approved and verified overwriting technologies/methods/tools. The clear procedure shall consist of at least one (1) complete Solid State Memory Erasure over the entire data storage element. The erasure can be a sequential data erasure or block erasure. Multiple passes or more complex overwrite sequences may alternatively be used.

Level #2 – Purge: Eliminate the data from the FLASH memory by overwriting and verifying the overwrite of the entire data storage element using the following steps:
1. Clear the Solid State Memory. Block ERASE is recommended.
2. Perform one overwrite of the entire memory (which includes both the file directory and all stored data), using a verifiable pattern. See notes below on failed blocks.
3. Verify the overwritten data pattern over the entire storage element using either full sampling or representative sampling of the overwritten pattern In accordance with the verification requirements of paragraph 3.4. A block erasure of the overwrite pattern is recommended subsequent to verification.
4. Alternatively, Cryptographic Erase may be used in lieu of Clear/Overwrite if supported by the RMM. Verify that the key has been eliminated. See Paragraph 3.4.2 for additional information. Optionally, perform a block erase over the entire memory space after the key has been eliminated and then verify the block erase pattern in accordance with paragraph 3.4.
5. Verify that the procedure has been properly completed, document the completion results and remove markings and labels from the memory unit.

Level #3 - Destruction– Destruction is the permanent physical damage and/or complete destruction of the data storage elements and applicable controller memories. Physical damage must be to the extent that makes it physically impossible to connect to or electronically/physically evaluate or interrogate the memory elements. Destruction consists of shredding, disintegrating, pulverizing or incinerating the device by a licensed incinerator.

1 Flash Memory Sanitization Procedure Notes:

a. Flash memory is erased by setting all bit cells to logic high (NAND) or logic low (NOR), which also prepares the memory for writing new data. The "CLEAR"/erase function must be verified to operate correctly and fully erase the memory in the design verification testing of the RMM.

b. Verification requires the use of a known pattern for overwrite. Verification requirements are defined in Para.3.4

c. Evaluation of Failed Bit Cell Impact. Special consideration should be given to the data cells that have been identified or mapped as "failed". If possible, all bit cells in the storage media should be overwritten. The verification step may identify blocks with failed memory cells or cells that have been previously mapped out of the active memory. The dominant cause of Flash block failures is individual storage bit cells that are unreadable. Since functioning storage cells within blocks with failed bit cells are expected to be properly overwritten by the purge sequence, the value of any residual data (in the failed blocks) for reconstruction of the original classified ISR data is likely to be negligible if the data has been encoded, randomized or error detection coded prior to recording.

d. Level #3 Destruction is intended to render the data contained on the media element unrecoverable. Approved methods of destruction such as smelting or incinerating the media elements are defined in reference documents. This level is to be used to dispose of media at end of life or in emergencies when no alternative is available.

3.3.2. Hard Disk and RAID System Sanitization Procedures

The following levels of sanitization are applicable to a magnetic disk or group of magnetic disks in a RAID configuration:

Level #1- Clear - Perform one full OVERWRITE operation to all user data areas by use of a SECURE ERASE, a SCSI FORMAT UNIT command (or equivalent).Alternately, use an organizationally approved and validated manually initiated overwrite technology/method/tool. This operation shall write at least one pass of a known pattern of data to all user accessible areas of the media. Multiple write passes or more complex values may optionally be used. Additional guidance is provided below in “Notes”.

Level #2 – Purge - Use one of the following techniques to perform a full Purge operation for all user data areas and a verification of the entire storage element as follows:

OPTION 1:

1. Overwrite the entire user accessible memory element with a known pattern using the Secure Erase command/Format Unit function of the disk drive or apply the SCSI sanitize command. Alternately, use an organizationally approved and validated manually initiated overwrite technology/method/tool. This operation writes a known pattern of data to all user accessible areas of the media. Multiple write passes or more complex values may optionally be used.
2. Verify the written pattern at all memory locations using the verification methods described herein.
3. Verify that the procedure has been properly carried out and documented. Remove all markings and labels from the memory unit.

OPTION 2**:**

Apply Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. Verify that the procedure has been properly carried out and documented.

Optionally: After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, Secure Erase or the Clear procedure could alternatively be applied.

OPTION 3:

4. Purge disk drives by degaussing, using an approved automatic degausser, which will also make the drives inoperable.

Level #3 – Destruction is the permanent physical damage or destruction of the data storage elements (specifically the magnetic disks themselves in a disk-based system) and the applicable controller memories. Disintegrate, pulverize, shred or incinerate.

1. Hard Disk and RAID Sanitization Notes

a. Sanitization for RAID (or individual disk drives) includes verification that all previously recorded user accessible data is removed, but an unclassified Operating System (OS) may remain on the disks to facilitate reuse. If the OS remains on the disks after sanitization, it must be verified that the RMM design does not allow data to be written to this, or any other unallowable area of the disk.

b. Bad Bytes and Sectors. Issues related to mapping of uncorrectable Bytes and sectors apply to RAID or individual hard disk drive systems. The overwriting of all memory locations/elements within the disks (including bad blocks and spare areas of the disk) is the recommended method of purging data and is incorporated into the Enhanced Secure Erase function. The actual overwrite method may vary and the potential impact of bad blocks and sectors must be considered when applying sanitization procedures to determine if recovering valid or useful data from an existing bad block or sector is possible. The risk is likely to be low if the data has been encoded, randomized or error detection encoded prior to recording.

c. The verification Pattern can be any known pattern chosen by the manufacturer or program which can be written over the entire memory element and fully verified. A long Pseudo-Random Data Sequence is often used for this purpose.

d. Sanitization using the Enhanced Secure Erase Function (available in some disk drives) will overwrite all data locations including failed blocks, spare storage area and all other addressable blocks in the media and is preferred if available.

e. The storage device may support configuration capabilities that ` artificially restrict the ability to access portions of the media, such as SCSI mode select. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique.

f. When Cryptographic Erase is applied, verification that the key has been destroyed must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic erase operation was completed successfully.

g. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified.

h. This guidance applies to Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media, SSD or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in an RMM.

3.3.3. Solid State Disk Based RMM Sanitization

1. SSD Description - Solid State Disks (SSDs) are devices that incorporate solid state memory in place of or in addition to magnetic disks. They interface through magnetic disk interfaces so that they can replace standard magnetic disks in computer systems. SSDs incorporate a controller and firmware to match the disk drive interface to the solid state memory, provide wear leveling, encoding, error correction, spare memory control, erasure and other functions. There are a wide variety of implementations used in various SSDs for memory allocation, data routing, buffering and other functions performed by the controller/firmware in addition to the potential incorporation of multiple configurations of RAM, FLASH and magnetic memory devices.

2. SSD Recognition - The essential issue is that the program incorporating the device and the user must recognize that the RMM/device being used is SSD based, rather than a magnetic disk or that the RMM itself is comprised of SSDs rather than either a magnetic disk or custom FLASH memory blocks with a program specific controller. The designers and manufacturers always know what has been incorporated into the RMM, and they know the technical implications of their choices. However, the new user may not be aware of the internal components of an RMM and must be able to rely on the specified or incorporated sanitization procedure. It is a program responsibility to assure that the SSDs used in all RMMs properly implement the required sanitization procedures throughout the production run of RMMs

3. SSD Erasure and Sanitization Methods - Erase and Sanitize are (disk type) commands that are recognized by most SSDs and are meant to cause the destruction of the data and make it unrecoverable. AEDP-3 sanitization procedures used on a device that appears to be a “Disk” would require a “Secure Erase” that overwrites all user accessible memory locations and then verifies the overwritten pattern. It is

necessary to verify that any sanitization command that is used with the device is fully supported and properly and completely carries out the command. This is typically verified in first article test and maintained through Configuration Management of the supplied components and SSDs.

4. SSD Sanitization Procedures:

a. **Level #1 CLEAR:** Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.

b. **Level #2 PURGE:** Two options are available:

Apply the ATA or SCSI SANITIZE command, if supported. Alternately, one or both of the following options may be available:

1 The block erase command followed by verification.

OPTIONALLY: After the block erase is successfully completed, write binary 1s across the addressable area of the storage media and then perform another block erase.

2 If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command followed by verification.

OPTIONALLY: After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied.

c. **Level #3 DESTROY:** Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

5. SSD Sanitization NOTES:

a.. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information.

b Flash devices that support the TRIM command (or equivalent) provide a mechanism to disassociate an addressable block (“LBA”) from a physical storage element, which are then marked for erasure as part of the device’s “garbage collection” procedures. The practical effect of this operation is to make deleted files that have been subject to TRIM operations impossible to access using normal methods. However, the data is still vulnerable to laboratory recovery, and great care must be taken to ensure that the host and device implement the use of the TRIM command correctly.

c. Appropriate use of TRIM commands can implement a partial sanitization operation on specific locations, but not all areas, of a storage device. Great care is required to ensure that the TRIM command and associated “garbage collection” procedure implementation and timing performs as expected. There are many variations in the actual implementation of TRIM by different manufacturers.

6. SSD Verification: The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as SCSI mode select. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique.

When Cryptographic Erase is applied, verification that the key is destroyed must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A sampling verification as described in the paragraph 3.4.2 should also be performed after any additional techniques are applied following Cryptographic Erase.

Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes identified in NIST 800-88. Degaussing must not be performed as a sanitization technique on flash-based storage devices.

3.4. VERIFICATION OF SANITIZATION RESULTS.

The goal of sanitization verification is to ensure that the Target Data was effectively sanitized. When supported by the device interface (such as an ATA or SCSI hard drive or solid state drive), the highest level of assurance of effective sanitization (outside of a laboratory) is typically achieved by a full reading of all accessible areas to verify that the expected sanitized value is in all addressable locations. A full verification should be performed if time and external factors permit. Representative sampling defined below may be used for verification when it is necessary to limit sanitization/verification times. This manner of verification typically only applies where the device is in an operational state following sanitization so that data can be read and written through the native interface.

3.4.1. Representative Sampling for Verification

If an organization chooses representative sampling then there are three main goals applied to electronic media sanitization verification:

1. Select pseudorandom locations on the media each time the analysis tool is applied. This reduces the likelihood that a sanitization tool that only sanitizes a

subset of the media will result in verification success in a situation where sensitive data still remains.

2. Select locations across the addressable space. For instance, conceptually break the media up into equally sized subsections. Select a large enough number of subsections so that the media is well-covered. The number of practical subsections depends on the device and addressing scheme. The suggested minimum number of subsections for hard drives leveraging LBA addressing is one thousand. Select at least two non-overlapping pseudorandom locations from within each subsection. For example, if one thousand conceptual subsections are chosen, at least two pseudorandom locations in the first thousandth of the media addressing space would be read and verified; at least two pseudorandom locations in the second thousandth of the media addressing space would be read and verified, and so on. In addition to the locations already identified, include the first and last addressable location on the storage device.
3. Each consecutive sample location (except the ones for the first and last addressable location) should cover at least 5% of the subsection and not overlap the other sample in the subsection. Given two non-overlapping samples, the resulting verification should cover at least 10% of the media once all subsections have had two samples taken.

3.4.2. Cryptographic Erase Verification

Cryptographic Erase has different verification considerations than procedures such as rewriting or block erasing. When the crypto key is erased, that location must be verified to contain no data. Without the key, contents of the physical media, following Cryptographic Erase are not known and therefore cannot be externally evaluated unless the location of the key is known by the controller. When Cryptographic Erase is leveraged, there are multiple options for verification, and each uses a review of a subset of the media. Each involves a selection of pseudorandom locations to be sampled from across the media and is defined in NIST 800-88. Due to the difficulty of implementing a high confidence verification of CE after a PURGE operation that uses crypto key erasure, the CE function, followed by a block erase of the media and a standard full verification is recommended. This allows a straightforward verification, prepares the media for re-use and provides high confidence sanitization.

INTENTIONALLY BLANK

CHAPTER 4 SANITIZATION RESPONSIBILITIES AND RISKS

4.1. RESPONSIBILITY AND RISK

The determination of the risk that proper and appropriate sanitization has been effectively implemented resides with the Program Security Manager and should be based on the associated Country Policy. Various levels of NATO classification require different control methods and possibly different sanitization levels or procedures. Programs must therefore incorporate the capability to perform the sanitization procedures into procurements of hardware and software, in addition to incorporating appropriate measures into their CONOPS. Additional notes related to potential capabilities that can be incorporated into RMM designs are provided in the appendix.

4.2. PROGRAM CONSIDERATIONS

The Program's responsibility and issues to be considered are identified below:

4.2.1 Sanitization Procedure Use

The primary and emergency sanitization procedure for each data storage element is to be addressed by each program. The program must evaluate the risks and vulnerability but must also address the specific technology or combination of technologies incorporated into the data storage system. This is essential due to the times and techniques required to sanitize different media types. Using one "Clear" cycle and re-initialization of the memory should be considered routine for use in a controlled, operational environment and as a standard minimum practice for stored or spare media elements. When the stored data is of high time value, this approach may be adequate for normal handling and re-issue rather than applying a full "Purge" cycle with verification, to the media.

4.2.2 Sanitization of Data Storage Elements in a Platform

The inclusion of an optional capability to clear and re-initialize a media element in the collection platform (via the primary aircraft interface and/or the NADS Interface) should be seriously considered as a valuable data security capability. This also allows for media re-use without the need for or availability of a native ground station, or the risk of substandard performance or capacity. In addition, this capability may allow the ADST memory device to remain installed in the data storage system of the aircraft and the aircraft would contain no classified data in the RMM.

4.2.3 Sanitization after a Media Failure

Programs must address the sanitization or control of media elements, containing classified data, which have suffered catastrophic failure and do not operate. In the case of low cost elements such as tape or magnetic disks, established methods of degaussing and destruction apply. There are significant issues and trade-offs related to the sanitization of and/or recovery of data from high and very high cost elements such as RAID and SSR memories. Failures of controllers, operating systems, actuators, motors, etc. may render the memory element un-addressable or inoperable. In these cases, special procedures are required for Sanitizing and handling these memories in accordance with NATO directives for handling classified data. The specific handling procedures must be developed by the program.

ANNEX A ADDED GUIDANCE FOR SANITIZATION OF DISK AND SOLID STATE MEMORY

A.1. TECHNICAL ISSUES

A.1.1 Overwrite Issues

Overwrite issues: The ability to overwrite all storage elements of a memory device is valuable in addressing spare data locations, failed cells, and other areas mapped out of the normal data storage areas. It may also be beneficial if the operating system for the storage device is read-only memory, in order to retain the OS when the active memory is overwritten.

A.1.2. Assurance Levels

The sanitization assurance level increases from low to high after the overwrite data is verified in a Purge. If the full overwrite has been accomplished properly, the data is not recoverable, but the user is not assured that Purge has been accomplished until it is verified.

A.1.3. Sanitization Level Changes From Previous AEDP-3 Versions

Previous versions of AEDP-3 incorporated 5 levels of “Sanitization”. Levels 1 and 2 provided no protection from attack using common software tools and have been removed from this version of AEDP-3. This version incorporates 3 levels of Sanitization. The levels defined in this document provide significant protection with level 2 and 3 making the data unrecoverable by any known means.

A.2. EXAMPLES

A. 2.1 Time Value of Data

When the data value decreases rapidly over time, the level of sanitization assurance required would also decrease over time.

A.2.2 Clear Procedure

A Clear is typically used for re-use or storage of RMMs after ISR data with high time value has been downloaded. If a recording capable RMM (i.e. without record inhibit function) is connected to a classified ground system, a Purge is usually required to sanitize the RMM since the RMM will become classified to the level of the ground system.

AEDP-3 (C)(2)