iNEMI Statement of Work (SOW)
Sustainable Electronics TIG
Non-Physical Data Destruction for Enterprise Storage Project

Version # 1.2
Date: April 28, 2020

Project Leader: Ke Du, Marvell
Co-Project Leader: TBD
iNEMI Project Manager: Mark Schaffer

Basic Project Information

Background/Context

Eventually all storage devices (e.g. HDDs) need to be decommissioned at end of life cycle. A significant method today is physical destruction, to mitigate risk of access to the information on the storage media. Unfortunately, this renders limited value recovery from the hardware, and is also an incremental operational expense. Prior iNEMI projects successfully explored and demonstrated techniques to drastically improve the value recovery of end of life HDDs with specific focus on the economic and technical feasibility. The results were quite promising. If we could mitigate the need for physical destruction, value recovery would increase even more, and EOL operating expense would decrease.

That’s the challenge we will address in this project:
- identify the data center expectations for data security and data sanitization at EOL
- identify and as appropriate demonstrate non-physical means of data sanitization
- as appropriate, identify, engage with and influence relevant standards work and advances for non-physical sanitization technologies

In the US alone, approximately 20 million storage devices are being decommissioned in data centers annually. U.S. laws and regulations require that sensitive data be completely sanitized before disposing. There are several sanitization “standards” that may be followed. The two most widely utilized standards in the US are from the Department of Defense (DoD), or DoD 5220.22-M, and from the National Institute for Standards and Technology (NIST), or NIST SP800-88R1. For the most part, the NIST800-88R1 has replaced DoD 5220.22-M as the benchmark standard used by enterprises and government agencies.

Value Recovery Phase 2  -  https://community.inemi.org/value_recovery_2
The NIST standard defines three forms of compliant sanitization: Clear, Purge, and Destroy. The regulation/law requires that if all these sanitization methods fail, the device (media) needs to be physically shredded (SSD/HDD) or degaussed 2 (HDD) at decommission. The table below summarizes the attributes of several common sanitization methods (Reference 1 – Center for Memory and Recording Research (CMRR): data sanitization tutorial).

<table>
<thead>
<tr>
<th>Type of Erasure</th>
<th>Average Time (100 GB)</th>
<th>Security</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal File Deletion</td>
<td>Minutes</td>
<td>Very Poor</td>
<td>Deletes only file pointers, not actual data</td>
</tr>
<tr>
<td>DoD 5220 Block Erase</td>
<td>Up to several days</td>
<td>Medium</td>
<td>Need 3 writes + verify, cannot erase reassigned blocks</td>
</tr>
<tr>
<td>Secure Erase</td>
<td>1-2 hours</td>
<td>High</td>
<td>In-drive overwrite of all user accessible records</td>
</tr>
<tr>
<td>NIST 800-88 Enhanced Secure Erase</td>
<td>Seconds</td>
<td>Very high</td>
<td>Change in-drive encryption key</td>
</tr>
</tbody>
</table>

The overwrite, block erase methods have inherent issues such as implementation difficulties and operation efficiency. The Cryptographic Erase (CE) is promising if implemented correctly. All these methods require working devices. However, the decommission process also needs to deal with drives that have failed.

When using CE with current Self Encryption Drive (SEDs), NIST800-88R1 requires that all encryptions keys, including the wrapping keys, be sanitized. These keys cannot be erased if a device fails. This means the device (media) needs to be physically shredded (SSD/HDD) or degaussed (HDD) if devices fail at decommission. The physical destruction of the SSD has additional concern since the die size can be very small. The shredding may not be effective or difficult to verify.

New methodologies, such as Cryptographic Erase (CE) technology in Self Encryption Drive (SED) are emerging to make the data sanitization process automatic and effective, regardless of device working conditions. CE, for example, has the following benefits when used in enterprise data applications:

- Meets NIST800-88R1 data sanitization standards
- Automatic data sanitization (decommission, repurpose, disposal, etc.)
- Simple implementation in SED design, and can be as extension of Trusted Computing Group 3 (TCG) standard
- Effective regardless of devices working conditions (functional or non-functional)
- Effective for HDD (and SSD)

**Scope of Work**

This project will apply to spinning media hard drives and solid-state drives that are used

---

2 Also called “demagnetizing.” This is a procedure to reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive.

3 [https://trustedcomputinggroup.org/about/](https://trustedcomputinggroup.org/about/)
in public and private data centers and data servers. Within those boundary conditions, the project will:

- Identify policy, standards, regulations, guidelines and customer requirements that are driving data destruction decisions at data centers
- Understand the risk assessments that are being made, both real and perceived risks, and available mitigation strategies
- Identify and verify "data erasure solutions" that conform to the NIST guidelines for Clear and ideally, NIST Purge
- Demonstrate feasibility and effectiveness of non-physical destruction, ideally with multiple stakeholders/partners/sites relative to the needs of the data center

It is estimated that the project would take no more than 12 months.

**Purpose of Project**

- This project will improve value recovery though reuse and operational expenses to both data centers and their supply chains.
- This project will focus on defining the customer requirements for data removal from devices; both described and implied, and proposing potential solutions for those requirements that can be implemented across multiple companies.
- This project will focus on SSD and HDD, though various techniques may also be applicable to other storage media that contain customer data.
IS / IS NOT Analysis

<table>
<thead>
<tr>
<th>This Project IS:</th>
<th>This Project IS NOT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spinning Media HD; Solid State Drives</td>
<td>For use primarily as Consumer, Mobile ICT or Persistent Memory Devices; or other parts of the system that could include persistent data that could be identifiable to a customer on a non-HDD or SSD (such as adapters that might have a cache or system data)</td>
</tr>
<tr>
<td>Non-governmental data (classified or unclassified)</td>
<td>Classified governmental data</td>
</tr>
<tr>
<td>Identification of policy, related standards, regulations, guidelines, customer requirement that are driving data center decisions</td>
<td>Biased towards specific suppliers, geographies, or market segments</td>
</tr>
<tr>
<td>Understanding and addressing the risk assessments that are being made which includes both the Real Risks and Perceived Risks of the data centers</td>
<td>Not physically stealing data devices (though may prevent access if device is stolen)</td>
</tr>
<tr>
<td>Customer responsibility for data erasure</td>
<td>Standards Development</td>
</tr>
<tr>
<td>Creation of case studies with/by data centers and/or other key stakeholders about reuse of drives that have been erased for sale or internal reuse.</td>
<td>Holistic Data Security; Chain of Custody and/or “Bad” internal players</td>
</tr>
<tr>
<td>Identification and verification of data security erasure solutions</td>
<td>Physical Data Destruction (i.e. degaussing, shredding, incinerating, punching etc.)</td>
</tr>
<tr>
<td>Conformance to NIST guidelines (Purge and Clear levels), ISO 27040:2015</td>
<td>Repeat of prior or existing work</td>
</tr>
<tr>
<td>Public and Private Data Centers (And Data Servers)</td>
<td></td>
</tr>
</tbody>
</table>

Business Impact

- This project will review the impact of non-physical data destruction of enterprise storage media on various stakeholders from these perspectives:
  - Financial Impacts
    - Consider the loss of resale value if drives must be destroyed vs. opportunity to gain revenue from reuse of drives or to avoid the cost of having to purchase new drives
    - Review the costs of physical drive destruction, including the labor to remove and handle drives and the charges for shredding or other physical destruction of the

NOTE: All changes to SOW must be approved by the Technical Committee for version control
Page 4 of 10
drives
  o Identify the costs for electronic sanitization of drives (license, software, hardware, labor)
  o Compare value/performance of used drives to cost/performance of new drives
  o Understand the cost of a typical data breach resulting from an unsuccessfully sanitized drive and the probability of this type of a breach
• Compliance to regulations and conformance to customer requirements
  o Consider what is required by regulation for data destruction on enterprise storage media and identify the cost of compliance
  o Consider customer requirements for privacy protection and ability to satisfy these requirements
  o Determine the efficacy of non-physical data destruction on media to demonstrate compliance to regulations and requirements
  o Recognize perceived risk by stakeholders related to physical vs. non-physical data destruction on media and what might influence these perceptions
• Environmental Sustainability
  o Determine shareholder/stakeholder value of promoting reuse of drives over destruction/recycling of drives
  o Understand, and where possible, quantify the environmental impact of both creating additional reuse streams (whole drives) and avoidance of a waste stream (shredded material)
  o Consider the role, if any, of drive reuse in circular economy models promoted by business
• Priorities
  o Consider competing priorities for data security in organizations and how critical the method of data sanitization is compared to other information destruction priorities

**Participating organizations in development of the SOW**
- Marvell
- WhiteCanyon
- IBM
- HP Enterprise
- Cascade Asset Management
- Seagate
- Toshiba
- NIST

**Outcome of Project**
- Understanding of the reasons behind current practices of physical destruction of storage media and the risk assessments being done
- Identification of policies, standards, and data center user requirements that are driving current practices
- Identification and verification of data erasure solutions available
- Potential demonstration projects based upon discovery that occurs during the project including pilot testing of multiple erasure solutions with data center partners
• Provide feedback to NIST and other relevant organizations based on the findings of the project

Sharing Project Results: To be determined by the project team on what information will be shared outside of the team.

Previous Related Work and References

• CMRR Data Sanitization Tutorial https://cmrr.ucsd.edu/_files/data-sanitization-tutorial.pdf
• UCSD paper: http://cseweb.ucsd.edu/users/swanson/papers/Fast2011SecErase.pdf
• NIST800-88R1 - Guidelines for Media Sanitization
• Value Recovery Phase 1 - https://community.inemi.org/value_recovery
• Value Recovery Phase 2 - https://community.inemi.org/value_recovery_2
• Circular Economy at work in Google data centers (Case Study) -- https://www.ellenmacarthurfoundation.org/case-studies/circular-economy-at-work-in-google-data-centers
• Debunking the three-pass wipe requirements / Why the DoD 5220.22-M 3-pass wipe standard has effectively been replaced by NIST 800-88, https://cascade-assets.com/resources/whitepapers.html
• The Internal Revenue Service addressed data sanitization in its 2016 IRS, Publication 1075 “Tax Information Security Guidelines For Federal, State and Local Agencies”. In it, the IRS specifies that “if media will be reused and repurposed . . . then purging should be selected as the sanitization method. If the media will not be reused at all, then destroying is the method for sanitization.” The IRS provides additional guidelines on the topic of data sanitization which provide additional detail on why electronic reuse and sanitization of data is allowable.
• The U.S. Department of Justice tackles data destruction through the Criminal Justice Information Services (CJIS) Security Policy, last updated on August 16, 2018. Section 5.8.3 reads, “The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.).”
• The Federal Trade Commission manages consumer privacy protection through FACTA. Part 682 of the regulation covers data sanitization. It requires organizations that store consumer information to protect against the unauthorized access to this information by “Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.”
• HIPAA governs the protection of Personal Health Information (PHI) collected in the healthcare industry. The HIPAA Privacy Rule requires that covered entities “apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI in any form.” For PHI on electronic media, “clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)“ are acceptable forms of data destruction.
Prospective Participants

- Data Security experts
- Data Center owners
- Risk Management/Insurance experts
- "Data Erasure" solution providers
- Data Sanitization Standards/Guidelines organizations
- HDD and SSD Manufacturers
- Commercial forensics lab
- Governmental Agencies

Project Plan

Schedule with Milestones

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Phase 1 – Detailed Information

Task 1 – Identify policy, standards, regulations, guidelines, customer requirement, etc. that are driving data destruction decisions at data centers and what security protocols that data sanitization providers need to meet

- Resources
  - Identifying all major government standards and guidelines
  - Identifying all major relevant corporate, industry body or government certifications
  - Identifying all major legal requirements
  - Identifying a sampling of major corporate (and/or government) internal requirements across industries e.g. defense, financial, medical

- Materials and Processes
  - None are anticipated

- Testing Procedures
  - None are anticipated

Task 2 – Understand the risk assessments that are being made, including both real and perceived risks and what mitigation strategies are available

Project participants will identify potential subject participants and solicit information from them about their risk assessment processes that have influenced their data destruction
policies and practices,

- **Resources**
  - The group will identify potential organizations to include in the evaluation.
  - A survey will be developed and distributed to subject participants. The group can use an online survey tool available through iNEMI or a member organization at no additional cost.
  - To promote participation in the survey, additional resources may be needed to encourage participation (phone calls, emails etc.).

- **Materials and Processes**
  - A set of survey questions will need to be developed by the group. The survey should be tested and validated prior to distribution to project participants.
  - A policy for how survey responses will be protected should be developed (is it an anonymous survey or not?).
  - A survey distribution plan should be developed that identifies who receives the survey, how much time is necessary to complete the survey, and how the survey results will be analyzed.
  - There should be a process to follow-up on individual responses, if possible.
  - A review team should synthesize the survey responses and provide analysis on trends and themes to inform the group about current risk assessment processes.

- **Testing Procedures**
  - The survey should be tested and validated prior to distribution to project participants.

**Task 3 – Identify and verify “data erasure solutions” that, at a minimum, conform to the NIST guidelines for Clear and ideally, NIST Purge**

- **Resources**
  - Identification of, Access to and Use of multiple “data erasure solutions” to include, but not limited to existing Cryptographic Erase (CE), new CE technologies, software wiping solutions
  - Testing that shows these solutions conform to NIST guidelines for Clear, at a minimum
  - Identification/Understanding of the conditions in which various solutions can be applied to devices

- **Materials and Processes**
  - Understand the different levels of NIST requirements as outlined below and what verification testing must be done to determine if they are being met:

Data Sanitization (sanitization) is a process to render access to target data on the media infeasible for a given level of recovery effort. NIST Special Publication 800-88R1 is widely used guideline for the data sanitization. It defined three level of data erasure: Destroy, Purge and Clear where destroy is the highest level of data sanitization. Destroy is an option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media. The organizations should select a method based on cost, environmental impact, and the risks to an unauthorized disclosure of information.
The follow table summarizes the data erasure methods and solutions that conform to NIST guideline.

<table>
<thead>
<tr>
<th>Erasure</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Clear   | Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques | Overwrite  
Or resetting the device to factory state if rewriting is not supported |
| Purge   | Applies physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques. | Overwrite, block erase, and Cryptographic Erase, using dedicated, standardized device sanitize commands that bypass the typical read/write commands  
Destroy including incineration, shredding, disintegrating, degaussing, and pulverizing. |
| Destroy | Target data retrieval is infeasible using state of the art laboratory techniques. The media cannot be reused as originally intended. | Disintegrate, Pulverize, Melt, and Incinerate, Shred. |

- Testing Procedures
  - Testing and/or data will need to be collected to verify any claims that a “data erasure solution” conforms to the NIST guidelines.
  - The testing methodology necessary to conduct the verification will need to be determined by the project team.

**Task 4 – Conduct one or more “pilot” tests that demonstrate feasibility and effectiveness of non-physical destruction, ideally with multiple stakeholders/partners/sites relative to the needs of the data center that could ideally be used to move more storage devices into reuse**

- Resources
  - The project objective is to determine feasibility of non-physical data destruction options meeting data center provider expectations (e.g. NIST800-88R1 standard for Enterprise Storage).
  - The identified solutions need close collaboration from device makers, HDD/SSD vendors, enterprise/data center users and data sanitization providers.
  - The solution needs to be implemented and “pilot” tested in real application environment by all parties.
  - Ideally, the solution also should have cost advantage over existing solutions.
• Materials and Processes  
  o It is estimated the 10 or more devices are needed to conduct the “pilot” test.

• Testing Procedures  
  o Broad, Software testing  
  o Ideally, a chip-off hardware test (SSD) conducted by a qualified 3rd party test facility

Task 5 – Provide recommendations for improvements to data security requirements (such as NIST guidelines or HIPAA or GDPR requirements etc.) and to improve erasure technologies.

• Resources  
  o Team input from Tasks 1-4 including time for writing and developing the document  
    o Summarize findings of policy/standards/regulations/guidelines and customer requirements including requirements, perhaps providing levels of requirements (from Task 1 and 2)  
    o Provide evaluations of solutions, including new proposed solutions, comparing those solutions to different levels of requirements (From Task 3 and 4)  
    o Identify gaps that exist, and if they do exist, recommend new solutions that need to be developed  
    o Provide guidelines for improvements to data security requirements or new data security guidelines that may be needed  
  o iNEMI copyediting  
  o Webinar / scheduling

• Materials and Processes  
  o Development and/or authorized use of graphics, photographs etc.  
  o Permission to use from any parties that we worked with (such as Google)

• Testing Procedures  
  o None anticipated

General and Administrative  
Guidelines for this project and all other iNEMI Projects are documented at http://thor.inemi.org/webdownload/join/gen_guidelines.pdf.