SNIA DPPC | DATA PROTECTION & PRIVACY COMMITTEE

# IEEE P2883™ Draft Standard for Sanitizing Storage: A SNIA Industry Advisory

*Industry advisory to SNIA members and other interested parties on a forthcoming IEEE standard for media sanitization*

Thomas Rivera, CISSP & P.K. Gupta
Co-Chairs, SNIA Data Protection & Privacy Committee

# Table of Contents

Introduction ..... 1
Details of Standard ..... 1
Further Detail ..... 2
Storage Sanitization - General ..... 2
Timeline ..... 3
SNIA Guidelines and Recommendation ..... 3
Additional Reference Material ..... 3
Usage ..... 3
Disclaimer ..... 4

# Introduction

The IEEE Security in Storage Work Group (SISWG) within the IEEE Computer Society's Cybersecurity and Privacy Standards Committee is in the final approval stages of a new standard that addresses the sanitization of storage. Given the increasing legislation and attention to data privacy, with the potential for data breaches also increasing, the disposition of data on all legacy and contemporary media formats needs to be addressed with clear guidance.

The purpose of this Advisory is to inform SNIA member companies and other interested parties of the detail of the standard, and where to get further information.

# Details of Standard

The document is in the form of a draft standard and is available to purchase from IEEE using the link below:

IEEE P2883™ Draft Standard for Sanitizing Storage
Sponsor: IEEE Computer Society Cybersecurity & Privacy Standards Committee (C/CPSC)

# Scope of Proposed Standard:

This standard specifies methods of sanitizing logical storage and physical storage as well as providing technology-specific requirements and guidance for the elimination of stored data. Note that the first edition of the standard is focused on media-based sanitization.

# Need for the Project:

A wide variety of data types are recorded on a range of data storage technologies. When these systems and/or their media are repurposed or retired from use, the stored data often must be eliminated (sanitized) to avoid data breaches. Depending on the storage technology, specific methods must be employed to ensure that the data are either eliminated or the logical storage and physical storage associated with the data devices/media are disposed of in a verifiable manner.

Existing published standards such as NIST SP 800-88 Revision 1 (Media Sanitization) and ISO/IEC 27040:2015 (Information technology – Security techniques – Storage security) provide guidance on sanitization, covering storage technologies from the last decade. When published, IEEE 2883 will address contemporary technologies as well as providing requirements that can be used for conformance purposes.

## Stakeholders for the Standard:

The stakeholders for this standard include all consumers of data storage technologies, especially those that store sensitive or high-value data or with stringent legal compliance obligations, and the vendors that manufacture, maintain, and support these technologies. Additionally, regulators and other standards development organizations may be able to leverage the contents of this standard.

## Further Details

### Storage Sanitization - General

Information and Communication Technology (ICT) systems capture, process, and store data using a wide variety of storage media. This data is not only located on the intended storage media, but also on storage devices used to create, process, or transmit this information. These storage media can require special disposition to mitigate the risk of unauthorized disclosure of data and to ensure the confidentiality of that data. Efficient and effective management of data that is created, processed, and stored by an ICT system throughout its life, from its inception through disposition, is a primary concern of an ICT system owner and the custodian of the data.

When storage media are transferred, become obsolete, or are no longer usable or required by an ICT system, it is important to ensure that residual magnetic, optical, electrical, or other representation of data are not readable or recoverable. For sensitive or regulated data, controlled and documented elimination of data recorded on storage is a necessity. Storage sanitization, henceforth sanitization, refers to the general process of eliminating access to data from storage media, such that there is reasonable assurance that the data cannot be retrieved or reconstructed. The focus on access is important because it may not be possible to eliminate the data on the media, so other steps (e.g., destruction of the storage media) can become necessary.

The concept of controlled elimination of data recorded on storage media is easy to understand, but putting the concept into practice can be challenging. An additional complication is the inconsistent use of terminology to describe this elimination of data. Whether the term is deletion, which is typically nothing more than changing a few file system pointers (i.e., no data is removed), secure data deletion (relies on overwrite techniques), or data shredding (implies destruction of encrypted data by deletion of the encryption key), and even some forms of physical destruction, **none are true, guaranteed, forms of data or media sanitization.**

An organization wishing to **sanitize** media must first determine whether it is able to apply the procedures defined in this standard. Some factors affect the feasibility of the organization sanitizing some media. If the organization is unable to sanitize the storage media and is unable to locate another organization that is able to do so, then the storage media shall be destroyed.

## Timeline

The IEEE Standards Association ballot was completed on 15th December 2021 and the public review period closed on 15th January 2022. Following the processing of comments, the draft will be forwarded for final publication approval. Publication is anticipated by June 2022.

## SNIA Guidelines and Recommendation

It is recommended that you examine the details of the standard as it is likely to be adopted as part of the broader storage security standards published by ISO. Please take due notice of this as it may affect how you and your organization operate.

## Additional Reference Material

- https://standards.ieee.org/project/2883.html
  (IEEE draft standard P2883)
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
  (Guidelines for media sanitization published previously by NIST)
- https://www.iso.org/standard/44404.html
  (Current ISO standard for storage security)

## Usage

Neither the name of The Storage Networking Industry Association (SNIA) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

## Disclaimer

The information contained in this publication is subject to change without notice. SNIA makes no warranty of any kind with regard to this specification, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this specification.

Suggestions for revisions should be directed to https://www.snia.org/feedback/.

## About the Data Protection & Privacy Committee (DPPC)

The DPPC is committed to the awareness and adoption of data protection technology, and to provide education, best practices and technology guidance on all matters related to the protection and privacy of data. This charter extends the focus of the DPPC into areas of data privacy, regulatory compliance, and a more generic view of protecting data.

This mission, in collaboration with other relevant groups, such as the SNIA Security Technical Work Group, is to deliver a point of reference for customers looking to improve their management of primary data assets and reduce exposure to external threats.

If you are interested in supporting this committee, please email Paul Talbut (paul.talbut@snia.org)

## About the SNIA

The Storage Networking Industry Association is a not-for-profit global organization, made up of member companies spanning the storage market. As a recognized and trusted authority for storage leadership, standards, and technology expertise worldwide, SNIA's mission is to lead the storage industry in developing and promoting vendor-neutral architectures, standards, and educational services that facilitate the efficient management, movement, and security of information.

SNIA DPPC | DATA PROTECTION & PRIVACY COMMITTEE

Storage Networking Industry Association
5201 Great America Parkway, Suite 320 • Santa Clara, CA 95054 • Phone: 719-694-1380 • Fax: 719-694-1389 • www.snia.org