Refresh of ISO/IEC 27040:2015 Standard for Storage Security

- A SNIA Industry Advisory

Industry advisory to SNIA members and other interested parties on a forthcoming refresh of the international standard for storage security

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

Eric Hibbard, Chair, SNIA Security Technical Working Group

Table of Contents

Introduction

The purpose of this Advisory is to inform SNIA member companies and other interested parties of significant forthcoming changes to the ISO/IEC 27040 Storage Security standard, an overview of the changes, and where to get further information.

Scope of Proposed Standard

This International Standard provides detailed technical requirements and guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use or end of life.

Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage products and services, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security or storage security, storage operation, or who are responsible for an organization’s overall security program and security policy development. It is also relevant to anyone involved in the planning, design, and implementation of the architectural aspects of storage network security.

This International Standard provides an overview of storage security concepts and related definitions. It includes requirements and guidance on the threat, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other International Standards and technical reports that address existing practices and techniques that can be applied to storage security.

Details of the Standard

The ISO/IEC 27040 International Standard provides requirements and guidelines for storage security in meeting the requirements of an Information Security Management System (ISMS) according to ISO/IEC 27001. This International Standard recommends the information security

risk management approach as defined in ISO/IEC 27005. It also builds upon the security controls described in ISO/IEC 27002 that are organized into people, organizational, physical, and technological controls.

The objectives for this International Standard are the following:

- Highlight the risks arising out of potential threats and attack surfaces
- Assist organizations in better securing their data
- Provide a basis for auditing, designing, and reviewing storage security controls

It is emphasized that ISO/IEC 27040 provides further detailed implementation guidance on the storage security controls that are described at a basic standardized level in ISO/IEC 27002.

Storage security can also necessitate the introduction of specialized controls to address technologies such as:

- System security hardening
- Storage sanitization
- Virtualization security
- Self-encrypting storage devices and data encryption software
- Key management services
- Data authenticity and integrity services
- Data in motion protections (encryption and data reduction)
- Directory services and other user management systems
- Data retention and preservation
- Data protection and recovery

What is Changing?

The standard is being refreshed in line with normal refresh cycles, however the opportunity has been taken to introduce significant changes to the content in the following areas:

- The scope has been expanded to include requirements (shall statements).
- A new controls labeling scheme has been added to make it easier to identify important controls and clusters of controls.
- Updates have been made to the storage technologies covered to accommodate the rapid adoption of flash and solid-state storage technologies over the last five years.

- The structure of the clauses is more closely aligned with ISO/IEC 27002:2022.
- Annex A, which provides guidance on sanitizing specific types of media, was removed and text recommending IEEE Standard P2883 be used for this purpose.

Need for the Project

The primary reason for restructuring the 27040 was to align it with the new ISO/IEC 27002:2022 Security Techniques structure.

Timeline

- DIS* Ballot Initiation: May 2022
- FDIS** Ballot Initiation: October 2022 (if needed)
- Publication: by November 2022 (if no FDIS) or February 2023

**The key stage in the development of an ISO Standard is the DIS (Draft International Standard) stage. A DIS is the end result of the work produced by a Working Group and approved by a Technical Committee. A document in the DIS stage is more than 95% technically accurate. A DIS goes out for a five-month approval vote by all 89 voting nations of ISO. Any suggested changes offered as a result of this voting process must be addressed by the Technical Committee and may be incorporated or rejected.*

***The newly modified DIS is sent to the voting nations as an FDIS (Final Draft International Standard) for a final approval vote (yes or no). Approval of the FDIS automatically instructs ISO to issue the document as a formal ISO Standard within 60 days of FDIS approval.*

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. Changes have been made to reflect a more stringent compliance requirement which may require your business to review and/or recertify.

Additional Reference Material

The documents listed below are international standards and are available to purchase from ISO using the links below:

- ISO/IEC 27001 Information technology — Security techniques (2013 version) Currently undergoing a refresh.
- ISO/IEC 27002 Information technology — Information security, cybersecurity and privacy protection (2022 version).

Usage

SNIA hereby grants permission for individuals to use this document for personal use only, and for corporations and other business entities to use this document for internal use only (including internal copying, distribution, and display) provided that:

- Any text, diagram, chart, table, or definition reproduced shall be reproduced in its entirety with no alteration

- Any document printed or electronic, in which material from this document (or any portion hereof) is reproduced shall acknowledge the SNIA copyright on that material and shall credit SNIA for granting permission for its reuse

Other than as explicitly provided above, you may not make any commercial use of this document, sell any or this entire document, or distribute this document to third parties. All rights not explicitly granted are expressly reserved to SNIA.

- Any document printed or electronic, in which material from this document (or any portion hereof) is reproduced shall acknowledge the SNIA copyright on that material and shall credit SNIA for granting permission for its reuse

Permission to use this document for purposes other than those enumerated above may be requested by e-mailing tcmd@snia.org. Please include the identity of the requesting individual and/or company and a brief description of the purpose, nature, and scope of the requested use.

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 advisory 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 in regard to this advisory, 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 advisory. 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 askdppc@snia.org

About 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.

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