



Storage Security Best Current Practices (BCPs)

Version 2.1.0

Publication of this SNIA Technical Proposal has been approved by the SNIA. This document represents a stable proposal for use as agreed upon by the Security TWG. The SNIA does not endorse this proposal for any other purpose than the use described. This proposal may not represent the preferred mode, and the SNIA may update, replace, or release competing proposal at any time. If the intended audience for this release is a liaison standards body, the future support and revision of this proposal may be outside the control of the SNIA or originating Security TWG. Suggestion for revision should be directed to <http://www.snia.org/feedback/>.

SNIA Technical Proposal

September 4, 2008

The 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:

1. Any text, diagram, chart, table or definition reproduced must be reproduced in its entirety with no alteration, and,
2. Any document, printed or electronic, in which material from this document (or any portion hereof) is reproduced must acknowledge the SNIA copyright on that material, and must credit the 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. 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.

Copyright © 2008 Storage Networking Industry Association.

Revision History

Revision	Date	Sections	Originator:	Comments
2.1.0	9/4/2008	All	Eric Hibbard	Initial SNIA Proposal

Table of Contents

EXECUTIVE SUMMARY	1
1 INTRODUCTION.....	2
2 SNIA STORAGE SECURITY – CORE BCPS.....	3
2.1 GENERAL STORAGE SECURITY (GEN).....	3
2.1.1 GEN01 – Identify & Assess All Storage Interfaces.....	3
2.1.2 GEN02 – Create Risk Domains.....	3
2.1.3 GEN03 – Monitor & Control Physical Access.....	4
2.1.4 GEN04 – Avoid Failures Due to Common Mistakes.....	5
2.1.5 GEN05 – Address Data Security Compliance.....	5
2.1.6 GEN06 – Implement Appropriate Service Continuity.....	6
2.1.7 GEN07 – Align Storage and Policy.....	7
2.2 STORAGE SYSTEMS SECURITY (SSS).....	7
2.2.1 SSS01 – Understand the Exposures.....	7
2.2.2 SSS02 – Utilize Event Logging.....	8
2.2.3 SSS03 – Secure Backups and Replication.....	10
2.2.4 SSS04 – Use Trusted and Reliable Infrastructure.....	11
2.3 STORAGE MANAGEMENT SECURITY (SMS).....	11
2.3.1 SMS01 – Secure the Management Interfaces.....	11
2.3.2 SMS02 – Harden Management Applications.....	12
2.3.3 SMS03 – Tightly Control Access and Privileges.....	12
2.3.4 SMS04 – Restrict Remote Support.....	13
2.3.5 SMS05 – Include Configuration Management (CM).....	13
3 SNIA STORAGE SECURITY – TECHNOLOGY SPECIFIC BCPS	14
3.1 NETWORK ATTACHED STORAGE (NAS).....	14
3.1.1 NAS01 – Network File System (NFS).....	14
3.1.2 NAS02 – SMB/CIFS.....	15
3.2 BLOCK-BASED IP STORAGE (IPS).....	15
3.2.1 IPS01 – Secure iSCSI.....	15
3.2.2 IPS02 – Secure FCIP.....	16
3.3 FIBRE CHANNEL STORAGE (FCS).....	16
3.3.1 FCS01 – Secure FCP.....	16
3.3.2 FCS02 – Secure Fibre Channel Storage Networks.....	17
3.4 ENCRYPTION FOR STORAGE (ENC).....	17
3.4.1 ENC01 – Protect Externalized Data.....	18
3.4.2 ENC02 – Pedigree of Encryption.....	18
3.4.3 ENC03 – Risk Assessment in Use of Encryption.....	19
3.4.4 ENC04 – Encryption Issues.....	19
3.5 KEY MANAGEMENT FOR STORAGE (KMS).....	20
3.5.1 KMS01 – Key Management Principles.....	20
3.5.1 KMS02 – Key Management Functions.....	21
3.5.1 KMS03 – Key Management Issues.....	21

3.6 LONG-TERM INFORMATION SECURITY	22
3.6.1 ARC01 – On-line Fixed Content	22
3.6.2 ARC02 – Off-line Fixed Content	22
4 SUMMARY.....	24
APPENDIX A – REFERENCES.....	25
APPENDIX B – BEST CURRENT PRACTICES (BCP) BACKGROUND.....	27
ABOUT THE AUTHOR(S)	29
ABOUT THE SNIA.....	30
ABOUT THE SNIA SECURITY TECHNICAL WORK GROUP	30
ABOUT THE SNIA STORAGE SECURITY INDUSTRY FORUM	30
INDEX	31

Executive Summary

With the increasing importance and emphasis on security in mind, the SNIA Security Technical Work Group (TWG) has prepared a revision to the SNIA storage security best current practices (BCPs). This vendor neutral guidance has a broad scope, covering both storage systems and entire storage ecosystems.

These new SNIA storage security BCPs are grouped into **core** BCPs and **technology specific** BCPs. The core BCPs are intended to apply to all storage systems/ecosystems and they cover basic storage security elements. The technology specific BCPs are above and beyond the core BCPs and they may or may not apply. When they do apply, multiple categories of the technology specific BCPs may be applicable for a given environment.

The following lists the categories associated with both the core and technology specific BCPs:

- Core:
 - General Storage Security
 - Storage Systems Security
 - Storage Management Security
- Technology specific:
 - Network Attached Storage (NAS)
 - Block-based IP Storage
 - Fibre Channel Storage
 - Encryption for Storage
 - Key Management for Storage
 - Long-term Information Security

Judicious use of the SNIA storage security best current practices will allow an organization to take a holistic approach to securing its storage systems/ecosystems.

1 Introduction

From a storage perspective, *storage security* represents the convergence of the storage, networking, and security disciplines, technologies, and methodologies for the purpose of protecting and securing digital assets. From a security perspective, storage security is simply a part of information assurance, which includes information security, network and communications security, host-based security, and data security. Although security within storage has some unique attributes, these attributes are not significant enough to warrant a special designation like storage security; however, the need to draw attention to the security aspects of this segment of infrastructure is the primary reason the Storage Networking Industry Association (SNIA) Security Technical Work Group (TWG) uses the term storage security.

As with many aspects of security, a balance must be struck between mitigating risks and minimizing the impacts, which may take the form of cost, complexity, throughput, availability, scalability, etc. Each organization must make its own trade-off decisions based on its unique situation (e.g., deployed infrastructure, legal and regulatory requirements, and due care expectations) and the importance of its data.

The purpose of this SNIA document is to provide broad guidance to organizations seeking to secure their individual storage systems as well as their storage ecosystems. This guidance is provided in a vendor neutral manner as a collection of **best** current practices or BCPs¹. By focusing on best practices rather than a more minimalist set of requirements, organizations have flexibility in how they implement this guidance (e.g., specific technology areas, phased approach, etc.).

Most of the BCPs are written in layman terms, avoiding unnecessary storage- or security-specific jargon and acronyms. However, the target audience is expected to have a basic working knowledge of storage or security practices and concepts. As written, this content should be usable by practitioners, IT architects, IT managers, and corporate executives (CIOs and CSOs, in particular).

¹ Readers who are familiar with the initial version of the SNIA storage security BCPs may want to consult Appendix B for additional background information.

2 SNIA Storage Security – Core BCPs

This section provides a complete list of the SNIA storage security BCPs, which are considered applicable to all storage systems/ecosystems. These core BCPs are organized into the categories:

- General Storage Security (GENxx)
- Storage Systems Security (SSSxx)
- Storage Management Security (SMSxx)

2.1 General Storage Security (GEN)

The BCPs defined in this category lay the ground work necessary to secure storage systems/ecosystems. They cover topics spanning asset assessments, establishing risk domains, physical security, guarding against mistakes, factoring in compliance, service continuity, and policy.

2.1.1 GEN01 – Identify & Assess All Storage Interfaces

Any serious attempt to secure storage requires a clear understanding of the assets involved (technology and data) as well as a basic classification. These BCPs offer guidance to address both the technology and data aspects of an asset assessment.

- GEN01.A Identify physical & logical interfaces
 - Identify both in-band and out-of-band management interfaces
 - Identify all storage resources, including type, usage and users
- GEN01.B Inventory physical & logical interfaces
 - Identify and document which storage devices are visible to which servers
 - Identify and document the networks to which the storage devices are attached
 - Identify and document which servers might export data (e.g. via NAS interfaces)
- GEN01.C Classify Sensitive & Critical² Interfaces
 - Identify and document interfaces supporting business/mission critical application and data
 - Identify and document those interfaces supporting sensitive information (e.g., personally identifiable information or PII)

2.1.2 GEN02 – Create Risk Domains

In the world of security, a defense-in-depth strategy is often employed with an objective to align the security measures with the risks involved. These BCPs offer guidance on ways to minimize risks to storage ecosystems, especially the damage from a successful attack.

- GEN02.A Physical
 - Segregate production from other system classes (Quality Assurance, Development)
 - Do not co-mingle shared array ports if possible
 - Use independent fabric and independent storage if appropriate
 - Physically separate systems in each class
 - Isolate storage devices from other data center devices, if practical

² Most organizations are motivated to protect sensitive (and business/mission critical) data, which typically represents a small fraction of the total data. This narrow focus on the most important data can be leveraged as the starting point for data classification and a way to prioritize protection activities.

- GEN02.B Logical
 - Segregate storage traffic from normal server traffic
 - Use FC/zoning and IP/VLANs to control network access
 - Use hardware-enforced zoning for access control
 - Use LUN Masking at the point closest to source device
 - Segregate management traffic from all other traffic
 - Carefully review configuration of network gateways, especially FC-iSCSI³
- GEN02.C Virtual
 - Manage the movement of virtual servers⁴
 - Carefully monitor migration of virtual servers between risk domains
 - Assure that a virtual server image is afforded the same protections as if it were a physical server
 - Ensure appropriate service level objectives for virtual storage
 - Match the availability objective for the “storage cloud” to the application requirements
 - Match the confidentiality and privacy requirements for the “storage cloud” to the types of information stored

2.1.3 GEN03 – Monitor & Control Physical Access

An underlying assumption for most aspects of storage security is that the storage resources enjoy a certain amount of physical protection. These BCPs offer guidance on controlling physical access to the storage ecosystem.

- GEN03.A Facilities
 - Restrict access to the data center
 - Be cognizant of social engineering attacks such as impersonation, forgotten passwords and forgotten badges
 - Secure all lockable racks, cabinets, arrays and libraries
- GEN03.B Network Infrastructure & Cable plant
 - Physically isolate core from edge switches
 - Disable unused ports and E_Port Access on non inter-switch ports
 - Restrict access to fiber patch panels and switches
 - Monitor fiber and cable plant; investigate errors
- GEN03.C Storage resources
 - Use port authentication if available
 - Secure hot-swappable drives; investigate errors
 - Monitor access to removable media

³ Within the context of this document, FC-iSCSI is a shorthand notation for storage networking gateways that allow iSCSI initiators and targets to use and be used by Fibre Channel entities, and vice versa.

⁴ Virtual servers are much easier to migrate between physical hosts in an infrastructure and this movement may have unintended security consequences. For example, moving a virtual server from a lower-risk (more trusted) to a higher-risk (less trusted) domain may expose the sensitive information the server contains or allowed to process unless its configuration is hardened appropriately. Conversely when a virtual server is moved from a higher-risk (less trusted) domain to a lower-risk (more trusted) domain, its hardening configuration may interfere with normal operation unless it is matched to that appropriate for the lower-risk domain.

2.1.4 GEN04 – Avoid Failures Due to Common Mistakes

Not all compromises are due to malicious behaviors, but may be due to mistakes by trusted personnel. These BCPs offer guidance on ways to avoid common mistakes within the storage ecosystem.

- GEN04.A Software configurations
 - Only install software and firmware from authorized sources
 - Maintain a verifiable Definitive Software Library (DSL)⁵, both locally and at a remote site
 - Pre-stage equipment to remove default configurations and assure compliance with configuration baselines
 - Remove current configuration from switches being moved to new fabrics
- GEN04.B Maintenance
 - Explicitly schedule updates rather than allowing automatic updates, which occur at unpredictable times
 - Pull unused jumpers
 - Require physical presence or secure procedures to update firmware
 - Validate firmware that is installed and running
- GEN04.C Access Controls
 - Implement appropriate access controls before:
 - Connecting a switch to a live storage network
 - Changing the configuration of a live storage network
 - Adding a host to a storage network

2.1.5 GEN05 – Address Data Security Compliance

Complying with legal and regulatory requirements has become an important issue world-wide and this compliance is driving the security agenda and strategy of many organizations. These BCPs offer guidance on addressing compliance by focusing on the key aspects of a storage ecosystem that are of concern to an information systems (IS) auditor.

- GEN05.A Accountability
 - Ensure that users, especially privileged users, have unique userids (i.e., no shared accounts)
 - When possible, grant rights and privileges based on roles
 - Log all attempted (successful and unsuccessful) management events and transactions
- GEN05.B Traceability
 - Ensure logged event/transaction data contains sufficient application and/or system detail to clearly identify the source
 - Ensure that the user information can be traced to a specific individual
 - When appropriate, treat log records as evidence (chain of custody, non-repudiation, authenticity, etc.)
- GEN05.C Risk Management
 - Enumerate and classify the information assets (e.g., data/information technology and value)
 - Perform risk assessment (vulnerabilities and threats)
 - Perform risk analysis (probabilities/likelihood and impacts)
 - Implement risk treatment (avoid, transfer, reduce, or accept)

⁵ Within this context, a Definitive Software Library (DSL) stores the master copies of all software and it is from this source that software control and release is managed.

- Regularly test controls and review processes
- GEN05.D Detect, Monitor, and Evaluate
 - Ensure that the storage layer participates in the external audit logging measures
 - Monitor the audit logging events and issue the appropriate alerts
- GEN05.E Information Retention & Sanitization
 - Implement appropriate data retention measures
 - Implement appropriate data integrity and authenticity measures
 - Correctly sanitize data upon deletion, repurposing or decommissioning of hardware
 - Correctly sanitize virtual server images, and their copies, at end of life
- GEN05.F Privacy
 - Implement appropriate data access control measures to control access to data and metadata (e.g., search results); assume a least privilege posture whenever possible
 - Implement appropriate data confidentiality measures to prevent unauthorized disclosure
- GEN05.G Legal
 - Ensure that the use of data deduplication does not conflict with data authenticity requirements
 - Ensure data and media sanitization mechanisms do not violate preservation orders
 - Ensure proper chain of custody procedures are followed when evidentiary data (e.g., audit logs, metadata, mirror images, point-in time copies, etc.) is handled

2.1.6 GEN06 – Implement Appropriate Service Continuity

Business survivability is frequently determined by the organization's ability to recover from a disaster and re-establish business processes. These BCPs offer guidance on the storage ecosystem's participation in this critical process.

- GEN06.A Disaster Recovery (DR)
 - Ensure the storage ecosystem is factored into the DR planning and implementation
 - Prepare for limited disruption events (system failures, hacker attacks, operator errors)
 - Tightly integrate recovery activities into IT systems design and incorporate them into day-to-day production practices
 - Move toward more automation⁶ to reduce recovery times and eliminate human error
- GEN06.B Business Continuity (BC)
 - Consider large-scale (natural) disasters and, where appropriate, mitigate risks with multiple, out-of-area recovery locations
 - Ensure the storage ecosystem is factored into the BC planning and implementation
 - Identify and document the unique staffing and facility requirements associated with the storage ecosystem

⁶ Within this context, automation refers to the processes and technologies that facilitate a failover to DR/BC facility resources. The underlying assumptions are that the DR/BC facility is a hot site and that this failover is executed with no or very little human intervention.

- GEN06.C Planning & Testing
 - Perform on-going planning and regular testing of assumption, which are critical to successful DR/BC.
 - Develop test cases
 - Document and script
 - Test as regressions with every configuration change (a loop-hole we closed before should not be reopened by accident)
 - Use automated testing tools (largest shops) to run the most possible test cases to improve quality of security infrastructure

2.1.7 GEN07 – Align Storage and Policy

The presence or absence of policy plays a major role in assuring both security and compliance. These BCPs offer guidance on storage-related issues that should be addressed by policy, including matters of compliance.

- GEN07.A Incorporate Storage in Policies
 - Identify most sensitive (personally identifiable information, intellectual property, trade secrets, etc.) and business/mission critical data categories as well as protection requirements
 - Integrate storage-specific policies with other policies (i.e., avoid creating a separate policy document for the storage ecosystem)
 - Address data retention and protection (e.g., write-once-read-many or WORM, authenticity, access controls, etc.)
 - Address data destruction and media sanitization
- GEN07.B Conformance with Policies
 - Ensure that all elements of the storage ecosystem comply with policy (e.g., ISO/IEC 27001/27002)
 - Give most sensitive/most critical data a priority

2.2 Storage Systems Security (SSS)

The BCPs defined in this category address the security associated with underlying storage systems/ecosystems. They cover topics spanning vulnerability assessments and management, audit logging, data protection (backups and replication), and IT infrastructure dependencies.

2.2.1 SSS01 – Understand the Exposures

With few exceptions, the long-term security of a storage system/ecosystem is not based on a single set of measures implemented at the time of initial deployment. Instead, a measured approach, which includes maintaining a constant understanding of the security posture and taking steps to adjust this security posture, is necessary. These BCPs offer guidance on components of such a measured approach.

- SSS01.A Perform Vulnerability Assessments
 - Perform security scans against the elements of the storage ecosystem to understand the security posture of the technology⁷
 - Maintain awareness of advertised vulnerabilities in platforms supporting management applications

⁷ Note that traditional security scanning only looks for publicly known issues in widely used software, and will not find anything new or unique in your specific implementations. Automated negative testing (such as robustness testing or fuzzing) provides capability to facilitate discovering new issues when more detailed analysis is needed.

- Maintain awareness of advertised vulnerabilities in virtualization platforms and their management applications
- SSS01.B Maintain Security of Systems
 - Install security patches and fixes in a timely fashion
 - Consider upgrading applications/software when end-of-life products contain exploitable, but unpatchable vulnerabilities
- SSS01.C Monitor for Zero-day Events
 - Integrate intrusion detection/prevention technology

2.2.2 SSS02 – Utilize Event Logging

Within a storage system/ecosystem, there are a wide range of transactions or events that can result in the generation of event log entries (messages). From a security or compliance perspective, it is important to capture those event log entries necessary to demonstrate proof of operations (e.g., encryption and retention), enforcement of accountability and traceability, meeting evidentiary requirements, and adequate monitoring of systems. This subset of general event logging is commonly called audit logging.

Generally speaking, the event log entries can be categorized as one of the following:

- **management** – messages that represent explicit actions to change the configuration, move data, and invoke security measures (e.g., authentication, account management, etc.).
- **data access** – messages that document transactions associated with data; for example, when a particular host accesses a LUN or a NAS users attempts to access a specific file or directory.
- **control** – messages that document events that provide status, warn of pending failures, identify network connections, etc.

Not all event log entries are created equal, as some may only be useful for debugging purposes, provide system health status, warn of minor configuration problems, etc. From an audit logging perspective the management events (i.e., what a human did) are always of interest, the data access events are usually of limited interest (except in situations where critical files and directories need to be tightly monitored), and control events are typically of the least interest (they can provide useful information during root-cause analysis after an incident).

In addition, audit logging often requires the event entries of interest to be handled differently and separately from most other event log entries generated by a device. This special handling can be accomplished by having the devices send the audit log entries to special log infrastructure or they can be culled out of the general log stream, using a log filtering mechanism (a more challenging approach because it requires all the event entries of interest to be known a priori). Another aspect of this special handling is that an organization often has to demonstrate that it is monitoring (e.g., generating alerts for anomalous events) and reporting; these actions usually require some form of centralized logging infrastructure beyond simple collectors.

The logging BCPs described in this section were derived from the SNIA *Audit Logging for Storage* whitepaper (available at: http://www.snia.org/forums/ssif/knowledge_center/white_papers) and they offer guidance on

audit logging for storage systems/ecosystems. Additional guidance can be found in NIST⁸ Special Publication 800-92 *Guide to Security Log Management*.

- SSS02.A Include Storage in Logging Policy
 - With regard to storage systems and devices, the following elements of policy should be addressed:
 - Storage systems and devices must participate in audit logging
 - All *significant* storage management events are collected
 - Log data is preserved
 - Log data is archived and retained
 - The device time is synchronized with a reliable, external source
 - The logging policy should include evidentiary expectations (authenticity, chain of custody, etc.)
- SSS02.B Employ External Event Logging
 - Implement centralized⁹ audit logging to collect events from all sources in a single repository
 - Establish and use a common, accurate time source across the environment to assure that event records from different sources can be correlated
 - For anything other than system health monitoring and debugging, device resident logs are not recommended because they are more easily subjected to tampering or destruction, there is limited storage space available for logs, and they preclude the use of centralized automated analysis, alerting, and archiving.
 - Storage devices must be capable of natively logging events to one, and preferably multiple, external log servers (preferably syslog¹⁰).
 - Audit logging for which compliance, accountability, and/or security serve as the primary drivers must have devices configured to log events on a transactional basis (no buffering) .
 - Implement an analysis protocol to correlate audit log records to identify significant security events that provide indication of security incidents
- SSS02.C Ensure Complete Event Logging
 - From an accountability perspective the management events are always of interest, the data access events are usually of limited interest (except in situations where critical files and directories need to be tightly monitored), and control events are typically of the least interest (they can provide useful information during root-cause analysis after an incident).
 - Once the types of events to be logged have been determined, then ALL occurrences of these events must be logged (both in-band and out-of-band)
 - The following kinds of events should be logged:
 - Failed logon attempts¹¹
 - Failed file and object access attempts
 - Account and group profile additions, changes, and deletions

⁸ The Computer Security Resource Center (CSRC) within the National Institute of Standards and Technology (NIST) makes a wide range of information security resources available at: <http://csrc.nist.gov/publications/nistpubs/>

⁹ Centralization in this context should not be interpreted as meaning that all audit logging within an organization has to use a common infrastructure. It is more important to have storage systems/ecosystems within a single *risk domain* use a common audit logging infrastructure.

¹⁰ The Internet Engineering Task Force (IETF) has an activity called the Security Issues in Network Event Logging (syslog) Work Group (<http://www.ietf.org/html.charters/syslog-charter.html>), which is standardizing event logging.

¹¹ Successful logons should also be logged.

- Changes to system security configurations (e.g., audit logging, network filtering, zoning changes)
- Changes to security server usage (e.g., syslog, network time protocol or NTP, domain name system or DNS, authentication)
- System shutdown and restarts
- Privileged operations (i.e., administrator initiated changes)
- Use of sensitive utilities (e.g., sudo, cron)
- Access to critical data files
- Movement of virtual servers between physical hosts
- Each log entry should include a timestamp (date and time), a severity level, the source of the log entry (distinguishing name, IP address, etc.), and a description of the event.
- Use care when filtering on fields like “severity” as the enterprise logging policy should serve as the guide for determining what kind of filtering is appropriate and what level of information requires long term storage.
- SSS02.D Implement Appropriate Retention and Protection
 - Make sure the event log data from the affected systems are handled and retained correctly
 - Implement appropriate measures to preserve log integrity and prevent their modification or destruction (either maliciously or accidentally)
 - Depending on the importance of the data and/or the type of log entries, protective measures may be required to ensure the confidentiality¹² and integrity of the log data.
 - Use special purpose log servers to handle unique and/or sensitive data requirements
 - Leverage log relays and log filtering to minimize the impact of specialized storage requirements (WORM)

2.2.3 SSS03 – Secure Backups and Replication

Because of the increased dependency on data availability and integrity, many organizations employ a range of data protection mechanisms for increased data resiliency. These BCPs offer guidance on two important aspects of this data protection: backups and replication.

- SSS03.A Backup Security
 - Ensure that the backup approach, especially for business/mission critical data, is aligned with its associated restore strategy.
 - Ensure that the backup approach provides adequate protections against unauthorized access (e.g., encryption)
 - Establish a chain of trusted individuals (and vendors) who handle the storage media
 - When required, implement backup success validation to show “proof” that records retention requirements are being met
- SSS03.B Replication Security
 - Ensure that the replication approach, especially for business/mission critical data, is aligned with its associated reliability, fault-tolerance, or performance requirements.

¹² Some log entries may expose things like passwords (e.g., when a user types a password instead of the userid), but more subtle problems may exist as well (e.g., search commands that expose specific names and health issues).

- Ensure that the replication approach provides adequate protections against unauthorized access (e.g., encryption in-flight)

2.2.4 SSS04 – Use Trusted and Reliable Infrastructure

When securing storage systems/ecosystems, it is important to consider dependencies on other elements of the IT infrastructure. These BCPs offer guidance on ways to guard against having this infrastructure becoming an attack vector.

- SSS04.A Use Trusted Services
 - When possible, use secure connections (e.g., IPsec) for network services
 - Network services (DNS, SMTP, NTP, etc.) are often segregated into internally- and externally-visible services; use internal systems
- SSS04.B Minimize Impacts of Failures
 - Configure systems to use primary and replica servers for centralized authentication
 - Take full advantage of redundant IT infrastructure (e.g., DNS, NTP, directory services, etc.)
- SSS04.C Limit Dynamic Discovery
 - When possible, restrict the storage ecosystem’s use of service discovery protocols (e.g., service location protocol or SLP, Internet storage name service or iSNS, etc.) for automatic detection of devices and services on a computer network¹³

2.3 Storage Management Security (SMS)

The BCPs defined in this category address the security associated with managing storage systems/ecosystems. They cover topics spanning management interfaces, management applications, access control, remote support, and configuration management.

2.3.1 SMS01 – Secure the Management Interfaces

Protecting the management interfaces from unauthorized access and reconnaissance is of paramount importance. Failure to implement the appropriate controls could result in data destruction, corruption, and denial of access. These BCPs offer guidance on ways to protect the management interfaces.

- SMS01.A Segregate Out-of-band Management
 - Segregate management interface traffic from other traffic; physical isolation is preferred, but logical isolation should be used at a minimum
 - Protect management subnets by firewalls which pass only permitted traffic
 - Leverage intrusion detection mechanisms to identify anomalous behaviors
 - Disable and disconnect RS-232 management ports when not in use
- SMS01.B Restrict In-band Management
 - Use secure channels and strong authentication for all remote access (VPN, SSL/TLS, SSH, HTTPS)
 - Use caller ID access control for telephone lines used for “phone home”

¹³ Discovery services are a convenient way for administrators to provide and use (and even manage) storage resources because configurations do not need to be set a priori. However, the IETF specified approach for securing iSNS and SLP against a range of attacks is to use IPsec, which can be difficult to configure. The use of IPsec eliminates most or all of the convenience, so it is rarely used in combination with the discovery services; consequently, an organization ends up trading off security for convenience, which may not be appropriate for sensitive and business/mission critical data.

- Avoid indirect attacks from IT infrastructure (DNS, SLP, NTP)
- In-band and out-of-band management should be subjected to common security measures
- SMS01.C Control Vendor Maintenance
 - Restrict access to dial-in modems used for vendor support
 - Restrict access to out-of-band management network to authorized hosts and protocols

2.3.2 SMS02 – Harden Management Applications

A variety of storage management applications are available to manage storage systems/ecosystems, and it is important to ensure that these applications do not become attack vectors. These BCPs offer guidance on ways to help prevent the management applications from becoming sources of attack.

- SMS02.A Administrative Consoles and Management Applications
 - Guard against malware (e.g., viruses, worms, rootkits, etc.)
 - Log all attempted (successful and unsuccessful) management events and transactions
- SMS02.B SMI-S¹⁴ Access
 - Use more secure authentication when managing sensitive and high-value data
 - Clients and providers must communicate securely (e.g., over HTTPS) when sensitive and high-value data are involved
 - Realms can be used to establish protection domains on SMI-S providers
 - Make sure the SMI-S provider is free of common Web vulnerabilities¹⁵
 - Leverage basic network filtering to help mitigate denial of service attacks
- SMS02.C SNMP Access
 - Disable SNMP access if not needed
 - Replace default community names
 - Use SNMPv3 to provide authentication and secure communication
- SMS02.D Command Line Interface (CLI) Access
 - Limit installation of command line utilities to systems that require them
 - Use access control lists to limit systems that can use management capabilities
 - Do not use scripts with hard-coded userids and passwords
- SMS02.E Web-based Access
 - Communicate securely (e.g., over HTTPS) when sensitive and high-value data are involved
 - Make sure the HTTP/S server is free of common Web vulnerabilities¹⁵
 - Leverage basic network filtering to help mitigate denial of service attacks, especially when HTTPS is used

2.3.3 SMS03 – Tightly Control Access and Privileges

The individuals managing the storage systems/ecosystems are generally privileged users. It is important to limit privileges to the minimum needed to complete the required duties. These BCPs offer guidance on ways to control these privileged users and assure that adequate checks-and-balances are in place.

¹⁴ The SNIA Storage Management Initiative – Specification (SMI-S) Version 1.1.1 is defined in *ANSI/INCITS 388–2008 Storage Management*.

¹⁵ The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software; it's website at <http://www.owasp.org> is a good source of information for common web application problems.

- SMS03.A Configure Administrative Accounts
 - Remove manufacturers' default passwords
 - Use separate user IDs and require strong passwords for each user on each device
 - When possible, use a centralized authentication (e.g., RADIUS, Single-Sign-on, etc.) solution for improved monitoring and control
- SMS03.B Use Good Access Control Practices
 - Grant the least set of privileges required to perform the activity
 - Employ separation of duties, differentiating security administrator and storage administrator privileges
 - Manage access permissions by role rather than by user

2.3.4 SMS04 – Restrict Remote Support

To minimize system downtime and accelerate problem diagnostics and resolution, it is often necessary to have vendor personnel and the organization's systems administrators remotely monitor and access storage systems. This access must be provided in a way that complies with the organization's policy requirements and assure that this access cannot become a source of attack. These BCPs offer guidance on ways to control remote access and support.

- SMS04.A Limit access to dial in modems
 - Use caller-id features to limit access to explicitly permitted numbers
 - Use dial-back to mitigate risk of caller-id spoofing
- SMS04.B Control Remote Network Access
 - Permit inbound connections only from authorized hosts
 - Limit access to required protocols and services
 - Require secure protocols such as SSHv2 (secure shell), HTTPS, IPsec, etc, to mitigate risk of sniffing management traffic

2.3.5 SMS05 – Include Configuration Management (CM)

Increasingly, auditors are scrutinizing the change and configuration management practices of an organization because vulnerabilities are often introduced as a result of intentional and unintentional changes. These BCPs offer guidance on ways to minimize problems, stemming from system and configuration changes.

- SMS05.A Baseline Configurations
 - Establish a secure baseline configuration standard for all production devices
 - Regularly audit production configurations to assure compliance with the baseline
- SMS05.B Institute Operational CM
 - Implement change detection mechanisms for critical systems and record the results (audit trail)¹⁶
 - Practice change management to ensure a structured approach to transition from a current state to a desired future state.

¹⁶ Consider logging dynamic configuration changes introduced through mechanisms like the dynamic host configuration protocol (DHCP), dynamic discovery, etc.

3 SNIA Storage Security – Technology Specific BCPs

This section provides a complete list of the SNIA storage security BCPs, which are considered technology specific (i.e., not generally applicable). It is important to note that these BCPs are in addition to the core BCPs, which were defined in the previous section. Additionally, it is possible that one or more of these technology specific categories may be applicable in a given situation.

The remainder of this section defines the technology specific BCPs, which are organized into the categories:

- Network Attached Storage (NASxx)
- Block-based IP Storage (IPSxx)
- Block-based Fibre Channel Storage (FCSxx)
- Encryption for Storage (ENCxx)
- Key Manage for Storage (KMSxx)
- Long-term Information Security (ARCxx)

3.1 Network Attached Storage (NAS)

Network attached storage (NAS) is a file-level data storage providing data access to heterogeneous network clients. The BCPs defined in this category address the security associated with file-level storage systems/ecosystems. They cover the Network File System (NFS), which is often used by UNIX[®] and Linux (and their derivatives) clients, as well as SMB/CIFS, which is frequently used by Windows clients.

3.1.1 NAS01 – Network File System (NFS)

NFS is a client/server application, communicating with a remote procedure call (RPC)-based protocol. It enables filesystems physically residing on one computer system or NAS device to be used by other computers in the network, appearing to users on the remote host as just another local disk. These BCPs provide guidance on using NFS securely.

- NAS01.A Control NFS Network Access and Protocols
 - Enable NFS only if needed. This will eliminate it as a possible attack vector available to an intruder.
 - Use NFSv4 whenever possible and limit NFSv3 usage
 - Filter client and management access by IP address for additional security
 - Only allow NFS connections from well-known ports
 - Only enable multi-protocol (e.g., NFS & CIFS) access where required
 - Encrypt client data access when necessary (e.g., IPsec)
- NAS01.B Apply Access Controls to NFS Exported Filesystems
 - Employ user-level authentication whenever possible (e.g., NFSv4 with Kerberos V5)
 - Configure the NFS server to export file systems explicitly for the authorized users.
 - Configure the NFS server to export file systems with minimum required privileges.
 - Avoid granting “root” or “administrator” access to files on network filesystems
 - Make sure NFSv4 ACLs (access control lists) are assigned correctly
- NAS01.C Restrict NFS Client Behaviors
 - Filter client access to NFS shares whenever possible
 - Do not allow NFS clients to run *suid* and *sgid* programs on exported file systems.

- NAS01.D Secure Data on NFS Filer
 - Exported file systems should be in their own partitions to prevent system degradation by an attacker writing to an exported file system until it is full.
 - Encrypt data at-rest when necessary
 - Do not allow NFS exports of administrative file systems (e.g., /etc)
 - Guard against malware (e.g., viruses, worms, rootkits, etc.)
 - Continually monitor content placed in NFS shares and relevant access controls

3.1.2 NAS02 – SMB/CIFS

SMB/CIFS is a network protocol whose most common use is sharing files, especially in Microsoft operating system environments. These BCPs provide guidance on using SMB/CIFS securely.

- NAS02.A Control SMB/CIFS Network Access and Protocols
 - If SMB/CIFS is not needed, turn it off. This will reduce the number of possible attack vectors available to an intruder.
 - Encrypt client data access when necessary
 - Implement CIFS with strong authentication (NTLMv2, Kerberos)
- NAS02.B Apply Access Controls to SMB/CIFS Exported Filesystems
 - Disable unauthenticated access to CIFS shares and NAS devices (i.e. Restrict Anonymous)
 - Disable “Guest” and “Everyone” access to all CIFS shares
 - Implement authentication and access control via a centralized mechanism (RADIUS, LDAP)
- NAS02.C Restrict SMB/CIFS Client Behaviors
 - Enable SMB signing for Windows client and the NAS device
- NAS02.D Secure Data on SMB/CIFS Filer
 - Enable CIFS auditing whenever possible
 - Continually review content placed in CIFS shares and relevant access controls
 - Encrypt data at-rest when necessary
 - Guard against malware (e.g., viruses, worms, rootkits, etc.)

3.2 Block-based IP Storage (IPS)

Block-based IP storage is implemented, using protocols such as iSCSI, iFCP¹⁷ and FCIP to transmit SCSI commands over IP networks, potentially exposing both the control and data packets to attack¹⁸. The BCPs in this category address the security associated with the use of these protocols in conjunction with storage systems/ecosystems. They cover Internet SCSI (iSCSI) and Fibre Channel over TCP/IP (FCIP).

3.2.1 IPS01 – Secure iSCSI

Internet SCSI or iSCSI, which is described in IETF RFC 3720, is a connection-oriented command/ response protocol that runs over TCP, and is used to access disk, tape and other devices. These BCPs offer guidance on ways to secure iSCSI.

¹⁷ No iFCP-specific BCPs are included in this document.

¹⁸ IETF RFC 3723 *Securing Block Storage Protocols over IP* is also a useful source of information for securing IP storage.

- IPS01.A Control iSCSI Network Access and Protocols
 - Filter based on source IP addresses and protocols
 - Avoid connecting iSCSI interfaces to general purpose LANs; segregate for security and performance
 - Carefully use VLANs when the use of physically isolated LANs are not an option
- IPS01.B Implement iSCSI Security Measures
 - Use CHAP authentication for both initiators and targets in all iSCSI implementations
 - Use IPsec to secure the communication channel when sensitive data could be exposed
 - Avoid indirect attacks from IT infrastructure (iSNS¹⁹, SLP²⁰, DNS)

3.2.2 IPS02 – Secure FCIP

Fibre Channel over TCP/IP (FCIP), defined in IETF RFC 3821, is a pure Fibre Channel encapsulation protocol. It allows the interconnection of islands of Fibre Channel storage area networks through IP-based networks to form a unified storage area network. These BCPs offer guidance on ways to secure FCIP.

- IPS02.A Control FCIP Network Access and Protocols
 - Carefully set up the peer-to-peer relationship between FCIP Entities, recognizing that the security policies will be applied uniformly
 - Consider using a private IP network used exclusively by the FCIP Entities
- IPS02.B Implement FCIP Security Measures
 - Use IPsec to secure the communications between FCIP Entities.
 - Perform cryptographic authentication and data integrity at a minimum
 - Protect sensitive data by appropriate confidentiality measures

3.3 Fibre Channel Storage (FCS)

Fibre Channel is a gigabit-speed network technology used for block-based storage and the Fibre Channel Protocol (FCP) is the interface protocol used to transmit SCSI on this network technology. The BCPs in this category address securing the use of FCP as well as Fibre Channel storage networks.

3.3.1 FCS01 – Secure FCP

Fibre Channel entities (host bus adapters or HBAs, switches, and storage) can contribute to the overall secure posture of a storage network by employing mechanisms like filtering and authentication. These BCPs offer guidance on ways the Fibre Channel entities can be leverage to further harden storage networks.

- FCS01.A Control FCP Node Access
 - Restrict access to storage with World Wide Name (WWN) filtering (LUN masking)
 - Restrict host access on the switches (e.g., ACLs, binding lists, FC-SP policy)
 - Use NPIV (N Port ID Virtualization) to assign individual N_Port_IDs to virtual hosts

¹⁹ RFC 4171, *Internet Storage Name Service (iSNS)*, provides useful security guidance for the iSNS.

²⁰ RFC 3723, *Securing Block Storage Protocols over IP*, provides useful security guidance for the Service Location Protocol Version 2 (SLPv2).

- FCS01.B Implement FCP Security Measures
 - Use SCSI-based protection information²¹ to help minimize the risk of data loss by protecting data through the complete data path.
 - Use DH-CHAP authentication²² (per ANSI 426–2007 FC-SP)
 - Use ESP_Header²³ to protect Fibre Channel connections that leave the protected area

3.3.2 FCS02 – Secure Fibre Channel Storage Networks

A storage area network (SAN) is an architecture to attach remote computer storage devices (such as disk arrays, tape libraries and optical jukeboxes) to servers in such a way that, to the operating system, the devices appear as locally attached. These SANs are often based on a Fibre Channel fabric topology that utilizes the Fibre Channel Protocol (FCP). These BCPs offer guidance on ways to secure Fibre Channel SANs.

- FCS02.A Implement Switch-based Controls
 - Restrict switch interconnections (e.g., ACLs, binding lists, FC-SP policy)
 - Carefully consider the adequacy of basic zoning as a security measure
 - Disable unused ports
 - Carefully use default zones and zone sets (assume a least privilege posture)
- FCS02.B Interconnect Storage Networks Securely
 - Configure switches, extenders, routers, and gateways (e.g., FCIP and FC-iSCSI³) with the least amount of access

3.4 Encryption for Storage (ENC)

The primary purpose of encryption is to protect the confidentiality of stored or transmitted data. The process of encryption is a matter of applying an encryption algorithm (or cipher) to plaintext data yielding encrypted data (or ciphertext). Conversely, a decryption transforms ciphertext back into its original plaintext. The definition and specification of many important ciphers can be found in: ISO/IEC 18033:2005, NIST FIPS 197, NIST Special Publication 800-67, IEEE 1619-2007, and IEEE 1619.2 (draft).

For some types of ciphers (e.g., n-bit block ciphers) there are multiple ways (called *modes of operation*) in which the cipher can be used to encrypt plaintext. The definition and specification of the modes of operation can be found in: ISO/IEC 10116:2006, NIST Special Publication 800-38A, NIST Special Publication 800-38C, and NIST Special Publication 800-38D.

Ciphers work in association with a key and possibly other keying material (e.g., initialization vectors). In a symmetric cipher, the same key is used with both the encryption and decryption algorithms. In an asymmetric cipher, different but related keys are used for encryption and decryption. The management and protection of keys (known as key management) is critically important in maintaining data confidentiality, so Section 3.5 should also be consulted for relevant BCPs.

²¹ The SCSI Protection Information Model is defined in *ANSI INCITS 405–2005 SCSI Block Commands - 2 (SBC-2)*.

²² In this context, DH-CHAP is a reference to the AUTH-A element of *ANSI INCITS 426–2007 Fibre Channel Security Protocols (FC-SP)*

²³ ESP_Header Authentication and Confidentiality optional headers are defined in *ANSI INCITS 424–2007 Fibre Channel – Framing and Signaling-2 (FC-FS-2)*.

The encryption BCPs described in this section and the key management BCPs described in the next section were significantly influenced by the SNIA *Encryption of Data At-rest – Step-by-step Checklist* whitepaper (available at: http://www.snia.org/forums/ssif/knowledge_center/white_papers). These BCPs offer guidance on ensuring data confidentiality for storage systems/ecosystems. The remainder of this section identifies the applicable BCPs when using encryption within storage systems/ecosystems.

3.4.1 ENC01 – Protect Externalized Data

Many of the data breaches that fill the newspapers and create significant embarrassments for organizations involve loss of *externalized data*²⁴ such as backup media. These BCPs provide recommendations for protecting this information from unauthorized disclosure while it is in transit.

- ENC01.A Secure Sensitive Data on Removable Media
 - Off-site backup tapes of sensitive or regulated data should be encrypted²⁵ as a general practice, and must be encrypted when leaving the direct control of the organization; encryption keys must be stored separately from data
 - Use only secure and bonded shippers if not encrypted (remember that Duty of Care contractual provisions often contain a Limitation of Liability limited to the bond value. The risk transfer value is often less than the data value.)
- ENC01.B Secure Sensitive Data Transferred Between Data Centers
 - Sensitive/regulated data transferred to and from remote data centers must be encrypted in-flight
- ENC01.C Secure Sensitive Data in 3rd-party Data Centers
 - Sensitive/regulated data stored in third-party datacenters must be encrypted prior to arrival (both in-flight and at-rest)

3.4.2 ENC02 – Pedigree of Encryption

The protection provided by encryption very much depends on the quality of the algorithm selected and how it is used in practice. These BCPs provide guidance in selecting algorithms and establishing appropriate parameters for its use in protecting information.

- ENC02.A Encryption Algorithms
 - Cryptographic algorithms should be both publicly known and widely accepted (e.g. RSA, SHA, Triple DES, Blowfish, Twofish, etc.) or banking industry standard algorithms
 - Selection of a cryptographic algorithm should include choosing key sizes (e.g., 40-bit, 128-bit) and key space
- ENC02.B Symmetric Encryption Modes
 - When a symmetric key block cipher algorithm is selected, it is also important to select a mode of operation that provides the required information service such as confidentiality or authentication

²⁴ Within this context, externalized data is data that has left the direct control of the organization. This loss of control can be temporary (e.g., transmission between two data centers) or long-term (e.g., archived in a third-party data center).

²⁵ Consider using tape drives, which are compliant with the IEEE 1619.1-2007 standard, or other encryption mechanisms that offer a comparable level of protection.

- ENC02.C Strength of Encryption
 - Consider meeting or exceeding the US NIST (SP 800-57 Part 1) recommended minimum symmetric security levels, defined as bits of strength (not key size)
 - 80 bits of security until 2010 (128-bit AES and 1024-bit RSA)
 - 112 bits of security through 2030 (3DES, 128-AES and 2048-bit RSA)
 - 128 bits of security beyond 2030 (128-AES and 3072-bit RSA)

3.4.3 ENC03 – Risk Assessment in Use of Encryption

Certain data do not contain any recognizable or distinguishable data/information and may not be a candidate for encryption unless there is a unique business need. There should be a risk assessment performed on all data to understand what data (or group of data) are sensitive and whether they should be encrypted. This evaluation should be performed from a risk perspective for unauthorized viewing and the justifiable business need given the cost versus benefit or risk reduction. It is important to note that there are other vehicles to safeguard the confidentiality of information when the data are considered a critical asset. These BCPs provide guidance for using encryption as an appropriate risk mitigation mechanism.

- ENC03.A Identify and Classify Sensitive Data
 - Document what data are considered sensitive and require encryption as well as requirements for when and how the encryption is to be applied
 - Document the sensitive data's characteristics, including an estimate of the financial value of each data item to be protected
- ENC03.B Analyze Risks and Protection Options
 - Analyze data flows cradle-to-grave (DR/BC & archives are often overlooked)
 - Understand potential operational issues and their impacts to availability, performance, scalability, and proof of encryption
 - Understand the costs of protection
 - Define a rollback plan at the same time as defining the encryption scheme
- ENC03.C Mitigate Risks with Encryption
 - Ensure that the chosen algorithm protects at the desired level (according to the risk analysis) and is cost effective and convenient
 - Ensure that the chosen algorithm has a sufficient work factor to deter cryptanalytic attack
 - Ensure that all applicable local and international laws and regulations (where applicable) have been considered and respected.

3.4.4 ENC04 – Encryption Issues

The use of encryption technology introduces certain challenges that cannot be ignored. These challenges may include identifying the appropriate point of encryption, aligning the encryption with data reduction mechanisms, and creating appropriate audit trails. These BCPs provide guidance to help address these challenges.

- ENC04.A Point of Encryption
 - Select the location of at-rest encryption such that it minimizes the impacts to: users, data availability, information and communications technology (ICT) infrastructure, performance and throughput, scalability, BC/DR, and environmental
 - Implement the in-flight and at-rest encryption mechanisms such that they provide end-to-end protections
 - Migrate data between storage volumes if necessary to optimize end-to-end protection

- If undecided between two potential points of encryption, pick the one closest to the application generating the data
- ENC04.B Align with Data Reduction Services
 - Ensure that compression is performed before encryption to realize the maximum data reduction benefits
 - Ensure that deduplication is performed prior to encryption (and compression) to realize the maximum data reduction benefits
- ENC04.C Proof of Encryption
 - Ensure the encryption mechanisms create appropriate audit log entries (activation, verification, integrity checks, re-keying, etc.)
 - Agree in advance what audit log material will be necessary for the legal department to accept that encryption was properly performed
 - Perform regular and audited checks that encryption was properly performed, consider outside accreditation

3.5 Key Management for Storage (KMS)

The purpose of key management is to provide procedures for handling the cryptographic keying material used with symmetric or asymmetric cryptographic mechanisms (See Section 3.4 for BCPs that may be applicable to cryptographic mechanisms). The definition and specification of different aspects of key management can be found in: ISO/IEC 11770:1996 (Part 1 & 2), NIST Special Publication 800-57 (Part 1 & 2), IEEE 1619.3 (draft).

The remainder of this section identifies the BCPs applicable to key management for storage systems/ecosystems.

3.5.1 KMS01 – Key Management Principles

Successful use of cryptography is dependent on adhering to basic principles associated with keying material as well as implementing key management. These BCPs provide guidance on basic aspects of keys and key management.

- KMS01.A Observe Important Properties of Keys
 - Use a cryptographic key for only one purpose, specifically, do not use key-encrypting keys (also known as key wrapping keys) to encrypt data or use data-encrypting keys to encrypt other keys
 - Randomly choose keys from the entire keyspace
 - Check for and avoid use of known weak keys
 - Limit the amount of time a key is in plaintext form and prevent humans from viewing plaintext keys
- KMS01.B Implement and Use Key Management Safely
 - Fully automate key management whenever possible
 - Limit the use of data encryption keys to a finite amount of time (known as a key lifetime or cryptoperiod) or to a maximum amount of data processed
 - Sparsely use keys with a long life
 - Separate the key-encrypting keys from the data encryption keys
 - Document the authorization and protection objectives and constraints that apply to the generation, distribution, accounting, storage, use, and destruction of cryptographic keying material.
 - Enforce strict access controls to limit user capabilities and separation of duties constraints for key generation, change and distribution

3.5.1 KMS02 – Key Management Functions

The widespread use of cryptographic mechanisms places increased importance on the management and protection of cryptographic parameters (e.g., the key). The secure management of these keys is critical to the integration of cryptographic functions into a system, since even the most elaborate cryptographic system will be ineffective if its keying materials are poorly managed. These BCPs provide guidance on the administration and use of the services of generation, distribution, storage, archiving, derivation and destruction of keying material in accordance with a security policy.

- KMS02.A Establish Keys Securely
 - Generate symmetric keys by using either an approved random number generation method, a key update procedure that creates a key from the previous key, or an approved key derivation function that derives a key from a master key
 - Avoid concatenating split- or multi-key components as the combination function used to generate keys
 - Limit the distribution of data encryption keys to backups or to other authorized entities that may require access to the information protected by the keys
 - Keys must be protected using either encryption or an appropriate physical security mechanism/procedure throughout the distribution process
- KMS02.B Ensure Proper Operational Use
 - Ensure that the installation of a key within the device or process that is going to use it does not result in leakage of the key or information about the key
 - Provide confidentiality for keying material in storage, using either encryption with an approved algorithm or physical protection (i.e., cryptographic module or secure storage with controlled access)
 - Use reasonable measures to prevent modifications, to use methods to detect (with a very high probability) any modifications that occur, and to restore the keying material to its original content when modifications have been detected.
 - Store symmetric data encryption keys in backup storage during the cryptoperiod of the keys in order to allow key recovery, and store in archive storage after the end of the key's cryptoperiod, if required.
 - Replace a key with another key (i.e., Key Change) when the key may have been compromised, the key's cryptoperiod is nearing expiration, or to limit the amount of data protected with any given key.
- KMS02.C Key Disposition
 - Remove keying material and other related information from backups when no longer needed for operational use
 - Destroy keying material as soon as it is no longer required (e.g., for archival or reconstruction activity) in order to minimize the risk of a compromise

3.5.1 KMS03 – Key Management Issues

The use of cryptographic technology introduces certain challenges that cannot be ignored. These challenges may include strict regulations governing the import/export of the technology as well as causing catastrophic losses under certain failure conditions. These BCPs provide guidance to help address these challenges.

- KMS03.A Comply with Import/Export Controls
 - Understand and obey government **import** regulations associated with encryption and key management
 - Understand and obey government **export** regulations associated with encryption and key management

- KMS03.B Plan for Problems
 - Have a compromise recovery plan in the event of a key compromise.
 - Consider escrowing keying material used to protect business/mission critical information²⁶

3.6 Long-term Information Security

The BCPs defined in this category address the security associated with fixed content systems. They cover topics spanning on-line and off-line fixed content.

3.6.1 ARC01 – On-line Fixed Content

An on-line fixed content system usually contains at least some data subject to retention policies and a retention-managed storage system/ecosystem is commonly used for such data. These BCPs offer guidance on ways to protect on-line fixed content.

- ARC01.A Secure the On-line Fixed Content
 - Ensure that the read-only enforcement mechanism protecting the original source data within the fixed content is adequate to meet compliance requirements
 - Ensure data privacy with encryption and access control mechanisms
 - Enhance data accessibility through the use of integrated index and search capabilities that can be used to quickly find the data (e.g., needed to meet e-Discovery requirements)
 - Ensure the fixed content is included as part of the disaster recovery and business continuity planning and use automatic data replication capabilities to meet data recovery and availability requirements
 - Manage the fixed content by restricting access and operations to roles (e.g., security, storage, and search)
- ARC01.B Provide Governance and Compliance Functionality
 - Establish and enforce data retention requirements, including Legal Hold requirements (e.g., e-Discovery)
 - Ensure that data disposition securely eliminates all instances in both on-line and off-line media at the end of its retention period as well as recording the transaction in a legal-quality audit trail
 - Preserve the evidentiary nature of the data through the careful use of authenticity (more than simple integrity checks) and chain of custody mechanisms

3.6.2 ARC02 – Off-line Fixed Content

Data is the principal asset protected by an off-line fixed content service. According to IETF RFC 4810, the principal threat that must be addressed by such a service is an undetected loss of data integrity, but ensuring long-term privacy of sensitive information may be of equal importance. These BCPs offer guidance on protecting off-line fixed content.

²⁶ The loss on an encryption key with no key recovery capability (backups, escrow, etc.) renders all of the corresponding ciphertext (i.e., data encrypted under the lost key) unusable. This situation and risk will persist for as long as the data is stored as ciphertext.

- ARC02.A Establish Off-line Fixed Content Policy
 - Identify the types of data to be accepted as well as the preservation period (e.g., not longer than 30 years)
 - Assure that the service operates in accordance with the policy by defining its characteristics such as:
 - Fixed content data object maintenance policy
 - Authorization policy
 - Specify the preservation activities performed for fixed content data objects subject to the policy.
 - Define a cryptographic maintenance policy for cryptographic mechanisms
- ARC02.B Maintain Off-line Fixed Content Security
 - Assure that access control mechanisms are appropriate to the lifespan of the fixed content objects
 - Perform periodic data conversions and revalidations to assure the integrity and authenticity of data to address data format changes or technological obsolescence during the lifespan of fixed content data
 - Address long-term non-repudiation of digitally signed data when required
 - Ensure that the cryptographic assurances of confidentiality²⁷ and authenticity are maintained

²⁷ There is an implicit assumption that encryption keys are protected and available to decrypt ciphertext stored in the off-line fixed content. As noted in the Key Management BCPs, the loss of a key renders its corresponding ciphertext unusable.

4 Summary

Storage technology has an intimate relationship with data (the “crown jewels”) of many organizations. Frequently it is the repository for this data as well as the last opportunity for defense. Thus, it seems logical that storage systems/ecosystems should participate in some or all of the typical security services (i.e., confidentiality, integrity, availability, access control, and non-repudiation).

A defense-in-depth security strategy is becoming increasingly realizable as more data security measures become available. Although potentially complex to implement, storage security can be an effective element of a defense-in-depth strategy, and in many cases, it is truly the last line of defense. The SNIA storage security best current practices, described in this document, provide detailed guidance to help with the implementation of such a strategy.

Appendix A – References

This appendix provides a complete list of the documents and standards that were consulted and/or used in the production of these best current practices.

- ANSI INCITS 388–2008 *Storage Management*.
- ANSI INCITS 405–2005 *SCSI Block Commands – 2 (SBC-2)*.
- ANSI INCITS 426–2007 *Fibre Channel Security Protocols (FC-SP)*
- ANSI INCITS 424–2007 *Fibre Channel – Framing and Signaling-2 (FC-FS-2)*
- IEEE 1619-2007 – *IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*
- IEEE 1619.1-2007 – *IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices*
- IEEE 1619.2 – *Draft Standard for Wide-Block Encryption for Shared Storage Media*
- IEEE 1619.3 – *Draft Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data*
- IETF RFC 3720 *Internet Small Computer Systems Interface (iSCSI)*
- IETF RFC 3723 *Securing Block Storage Protocols over IP*
- IETF RFC 3821 *Fibre Channel Over TCP/IP (FCIP)*
- IETF RFC 4171 *Internet Storage Name Service (iSNS)*
- IETF RFC 4810 *Long-Term Archive Service Requirements*
- ISO/IEC 10116:2006 *Information technology -- Security techniques -- Modes of operation for an n-bit block cipher*
- ISO/IEC 11770-1:1996 *Information technology -- Security techniques -- Key management -- Part 1: Framework*
- ISO/IEC 11770-2:1996 *Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques*
- ISO/IEC 18033-1:2005 *Information technology -- Security techniques -- Encryption algorithms -- Part 1: General*
- ISO/IEC 18033-3:2005 *Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*
- ISO/IEC 27001:2005 *Information technology -- Security techniques -- Information security management systems -- Requirements*
- ISO/IEC 27002:2005 *Information technology -- Security techniques -- Information security management -- Code of practice for information security management*
- NIST FIPS 197 -- *Advanced Encryption Standard (AES)*
- NIST Special Publication 800-38A *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*
- NIST Special Publication 800-38C *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*
- NIST Special Publication 800-38D *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*
- NIST Special Publication 800-57 Part 1 *Recommendation on Key Management – Part 1: General (Revised)*
- NIST Special Publication 800-57 Part 2 *Recommendation on Key Management – Part 2: Best Practices for Key Management Organization*
- NIST Special Publication 800-67 *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
- NIST Special Publication 800-88 *Guide for Media Sanitization*
- *NIST Special Publication 800-92 Guide to Security Log Management*
- Payment Card Industry (PCI) *Data Security Standard (DSS) Version 1.1*

- Storage Networking Industry Association (SNIA), *Introduction to Storage Security*, http://www.snia.org/forums/ssif/knowledge_center/white_papers.
- Storage Networking Industry Association (SNIA), *Audit Logging for Storage*, http://www.snia.org/forums/ssif/knowledge_center/white_papers.
- Storage Networking Industry Association (SNIA), *Encryption of Data At-rest – Step-by-step Checklist*, http://www.snia.org/forums/ssif/knowledge_center/white_papers.
- Trusted Computing Group (TCG), *TCG Storage Architecture Core Specification* Version 1.0 Revision 0.9

Appendix B – Best Current Practices (BCP) Background

For close to 10 years, SNIA has had an active storage security program, which has focused on both the vendor aspects of making storage product more secure and the consumer aspects associated with using storage products in secure ways. As part of this effort, a simple model (see Figure B1) was developed to show the key storage security components. This model was important because it shifted the focus from the abstract concepts of confidentiality, integrity, and availability to a more tangible set of technology-oriented components.

This model also provided a useful mechanism for organizing recommendations and guidance for securing storage infrastructure. However, there are administrative and physical controls that need to be factored into a holistic storage security program, which don't fit cleanly into the simplistic model. Consequently, this model is not used extensively in this document.

The SNIA security activities (Security Technical Work Group and Storage Security Industry Forum) recognized very early on that storage-centric security guidance was needed. However, the sheer absence of awareness on the subject matter seriously complicated the situation. Further, neither the security nor the storage communities were in a position to drive the needed awareness and requirements, but the auditing community was beginning to take notice of the issues at a time when they were driving much of the security agenda for the affected organizations.

SNIA addressed these challenges by developing a series of storage security tutorials as well as conducting multiple security summits for the storage industry. Ultimately, a core set of content was developed and captured in the SNIA *Introduction to Storage Security* whitepaper, which is still available at: http://www.snia.org/forums/ssif/knowledge_center/white_papers. A key element of this whitepaper was a set of ten storage security recommendations (see Table B1) and associated descriptions.

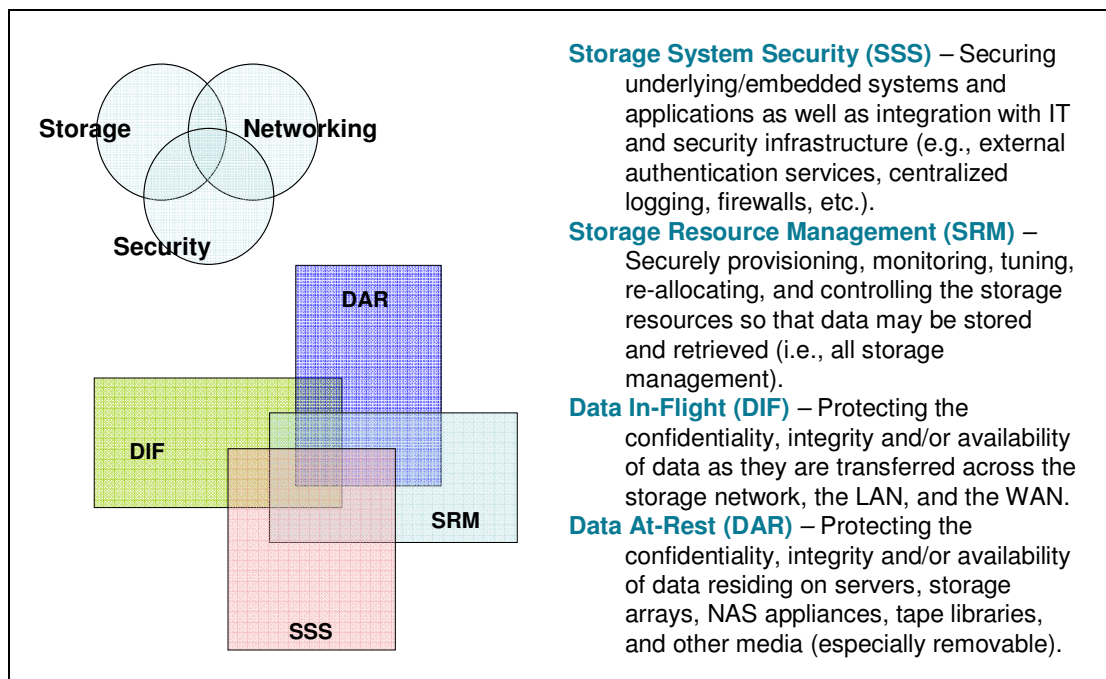


Figure B1. SNIA View of Storage Security

#	Recommendation Summary
1	Secure the Storage Management
2	Identify and Assess All Storage Interfaces
3	Create Risk Domains
4	Monitor and Control Physical Access
5	Avoid Failures Due to Common Mistakes
6	Address Data Security Compliance
7	Protect Externalized Data
8	Understand the Exposures
9	Implement Appropriate Service Continuity
10	Utilize Event Logging

Table B1. Storage Security BCP Version 1.0

This document builds upon and expands the original set of SNIA storage security best current practices (BCPs). In addition, the new BCPs are organized into categories that apply generally to all storage (known as **core**) and categories that are **technology specific**. Each of these categories is further subdivided into elements and sub-elements; a new numbering scheme, which tracks the new structure, has also been introduced to aid in referencing the BCPs.

To assist readers who are familiar with the original BCPs, a mapping diagram has been prepared (see Figure B2). It is worth noting that many of the original BCPs have become elements of the “General Storage Security” category.

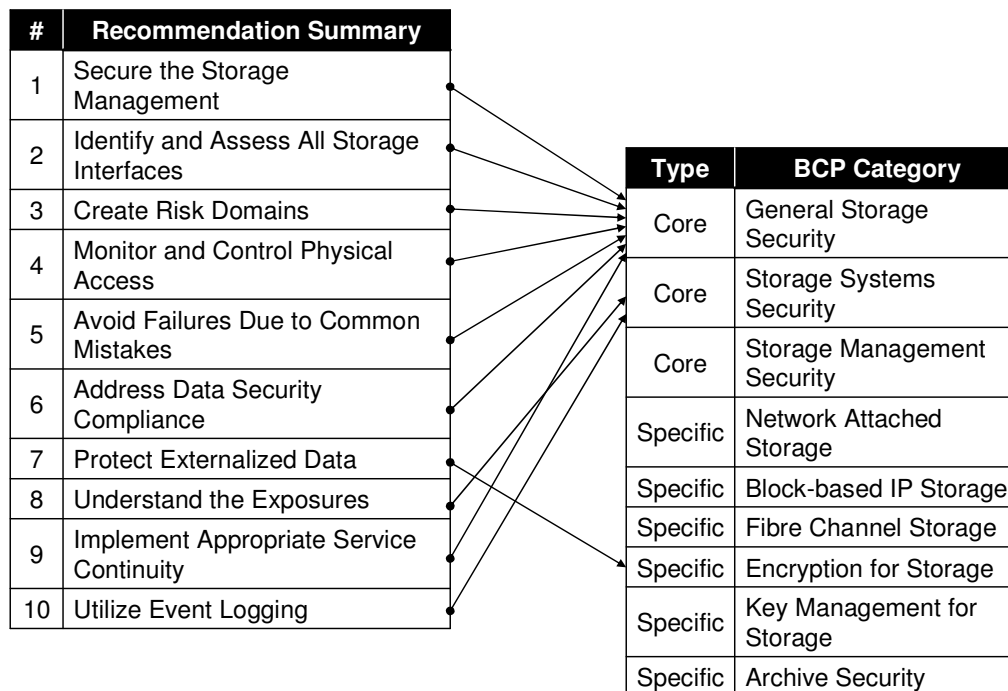


Figure B2. Storage Security BCP Mapping

About the Author(s)

Eric A. Hibbard

Mr. Hibbard is the Senior Director, Data Networking Technology in the Office of the CTO for Hitachi Data Systems where he is responsible for developing and leading the execution of the company's storage security strategy and serves as the principle storage security architect. He has significant experience architecting complex ICT and security infrastructures for large enterprises. Prior to joining HDS, he held key technology positions within government (DoD, NASA, DoE), academia (University of California at Lawrence Berkeley National Laboratory), and industry (Raytheon and QSS Group). In addition, Mr. Hibbard holds a unique combination of security (CISSP, ISSAP, ISSMP, and ISSEP from ISC²), IS auditing (CISA from ISACA), and storage (SCP and SCSE from SNIA) certifications. He is currently the Chair of the SNIA Security Technical Working Group, the Vice Chair of the IEEE P1619 (Security in Storage Work Group), and the International Representative for INCITS/CS1 (Cyber Security) as well as a member of INCITS/T11 (Fibre Channel Interfaces), IETF, W3C, the IEEE-USA Critical Infrastructure Protection Committee (CIPC), and the Trusted Computing Group (TCG).

Richard Austin

Richard is a 30+ year veteran of the IT industry in positions ranging from software developer to security architect. Before beginning a career as an independent consultant, he was focused on technology and processes for successfully protecting the 14PB storage area network infrastructure within the global IT organization of a Fortune 25 company. He earned a MS degree with a concentration in information security from Kennesaw State University, a National Center of Academic Excellence in Information Assurance Education, and serves as a part-time faculty in their CSIS department where he teaches in the Information Security and Assurance program. He holds the CISSP certification and is an active member of SNIA's Storage Security Industry Forum and Security Technical Working Group. He is a Senior Member of the IEEE and also belongs to the IEEE Computer Society, ACM, CSI, HTCIA, ISACA and ISSA (where he also serves on their international ethics committee). He is a frequent writer and presenter on storage networking security and digital forensics.

Many thanks to the following for their contributions to this whitepaper.

**Andrew Nielsen, CISSP, CISA
Roger Cummings
Jim Norton
Phil Huml
Anthony Whitehouse**

**Larry Hofer, CISSP
Walt Hubis
Vinod Bhat
LeRoy Budnik, CISA
Scott Kipp**

About the SNIA

The Storage Networking Industry Association (SNIA) is a not-for-profit global organization, made up of some 400 member companies and 7,000 individuals spanning virtually the entire storage industry. SNIA's mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organizations in the management of information. To this end, the SNIA is uniquely committed to delivering standards, education, and services that will propel open storage networking solutions into the broader market. For additional information, visit the SNIA web site at www.snia.org.

About the SNIA Security Technical Work Group

The Security Technical Work Group (TWG) consists of storage security subject matter experts, from the SNIA membership, who collaborate to develop technical solutions to secure storage networks and protect data. The Security TWG provides architectures and frameworks for the establishment of information security capabilities within the storage networking industry. Additionally, it provides guidance on the application of information assurance to storage systems/ecosystems as well as on matters of compliance as it relates to data protection and security. The focus of the Security TWG is directed toward both long-term and holistic security solutions.

About the SNIA Storage Security Industry Forum

The SNIA Storage Security Industry Forum (SSIF) is a consortium of storage professionals, security professionals, security practitioners, and academics dedicated to increasing the overall knowledge and availability of robust security solutions in today's storage ecosystems. The SSIF applies their deep body of knowledge and practical experiences in security and storage to produce best practices on building secure storage networks, provide education on storage security topics, and participate in standards development. SSIF educational, technical, and engineering activities influence the design, use, and management of storage technology to better protect and secure information. For more information, and to join, visit www.snia.org/forums/ssif.

Index

A

- access controls, 5, 15
 - to data and metadata, 6
 - zoning, 4
- accountability, 5
- ANSI INCITS
 - 388–2008, 12, 25
 - 405–2005, 17, 25
 - 424–2007, 17, 25
 - 426–2007, 17, 25
- archive. *See* fixed content
- asset assessments, 3
- audit logging, 9
 - accountability, 5
 - chain of custody, 6
 - common infrastructure, 9
 - confidentiality, 10
 - external, 6, 9
 - handling, 10
 - integrity, 10
 - monitoring, 6
 - no buffering, 9
 - retention, 10
 - traceability, 5
- audit trail, 13
 - legal-quality, 22
- auditor
 - information systems, 5
- authentication, 18
 - centralized, 11, 13
 - port, 4
 - strong, 15
- authenticity, 5, 6, 23

B

- backup security, 10
- backups, 7, 10
- BC. *See* business continuity
- BCPs. *See* best current practices
- best current practices, 2
 - core, 3
 - technology specific, 14
- bits of strength, 19
- business continuity, 6
 - fixed content, 22

C

- centralized authentication, 13
- chain of custody, 5, 6, 9, 22

- chain of trusted individuals, 10
- change detection, 13
- change management, 13
- CHAP, 16
- classify, 5
- Command Line Interface, 12
- compliance, 3, 5, 22
- compression
 - with deduplication, 20
 - with encryption, 20
- confidentiality, 6, 16, 18, 23
 - keying material, 21
- configuration management
 - operational, 13
 - practices, 13
- cryptographic
 - algorithms, 18
 - assurances, 23
 - maintenance, 23
 - mechanisms, 23
- cryptoperiod, 20

D

- data
 - authenticity, 6
 - availability, 10, 22
 - classification, 3
 - confidentiality, 6
 - critical, 7, 10
 - deduplication, 6
 - destruction, 7
 - disposition, 22
 - evidentiary, 6
 - externalized, 18
 - integrity, 6, 10, 16
 - most sensitive
 - identify, 7
 - priority, 7
 - privacy, 22
 - recovery, 22
 - replication, 10, 22
 - resiliency, 10
 - retention, 6, 7, 22
 - sanitization, 6
 - value, 18
- deduplication
 - with compression, 20
 - with encryption, 20
- default zones, 17
- Definitive Software Library, 5

- denial of service, 12
- DH-CHAP, 17
- directory services, 11
- disaster recovery, 6
 - fixed content, 22
- DNS, 10, 11, 12, 16
- DR. *See* disaster recovery
- dynamic discovery, 11

E

- e-Discovery, 22
- encryption
 - algorithms, 18
 - data at-rest, 15, 18
 - data in-flight, 18
 - modes of operation, 18
 - operational issues, 19
 - pedigree, 18
 - point of, 19
 - proof of, 19, 20
 - rollback plan, 19
 - strength of, 19
 - with compression, 20
 - with deduplication, 20
- ESP_Header, 17
- event logging
 - centralized audit logging, 9
 - control, 8
 - data access, 8
 - health monitoring, 9
 - management, 8
 - time source, 9
- evidence, 5
- evidentiary requirements, 8
- export controls, 21
- externalized data, 18

F

- fault-tolerance, 10
- FCIP, 16
- FCP, 16, 17
- FC-SP
 - authentication, 17
 - policy, 16, 17
- Fibre Channel Protocol, 16, 17
- fixed content
 - disaster recovery, 22
 - governance, 22
 - off-line, 22
 - access control, 23

- cryptographic
 - assurances, 23
 - data conversions, 23
 - data revalidations, 23
 - maintenance policy, 23
 - non-repudiation, 23
 - policy, 23
 - preservation period, 23
- on-line, 22
 - authenticity, 22
 - business continuity, 22
 - chain of custody, 22
 - data availability, 22
 - data disposition, 22
 - data privacy, 22
 - data recovery, 22
 - data replication, 22
 - data retention, 22
 - e-Discovery, 22
 - on-lineevidentiary, 22
- fuzzing, 7
- G**
- governance, 22
- H**
- HTTPS, 11, 12, 13
- I**
- IEEE
 - 1619.1-2007, 25
 - 1619.3 (draft), 20, 25
 - 1619-2007, 17, 25
- IETF
 - RFC 3720, 15, 25
 - RFC 3723, 15, 25
 - RFC 3821, 16, 25
 - RFC 4171, 25
 - RFC 4810, 22, 25
- import controls, 21
- integrity, 6
- interfaces
 - management
 - in-band, 3
 - out-of-band, 3
- intrusion
 - detection, 8
 - prevention, 8
- IPsec, 11, 13, 16
- iSNS, 11, 16
- ISO/IEC
 - 10116:2006, 17, 25
 - 11770-1:1996, 20, 25
 - 11770-2:1996, 20, 25
 - 18033-1:2005, 17, 25
 - 18033-3:2005, 17, 25

- 27001:2005, 7, 25
- 27002:2005, 7, 25
- K**
- Kerberos, 14, 15
- key
 - backup, 21
 - change, 21
 - cryptoperiod, 20, 21
 - derivation, 21
 - disposition, 21
 - escrowing, 22
 - lifetime, 20
 - recovery, 21
 - secure distribution, 21
 - size, 18, 19
 - space, 18, 20
 - update, 21
 - wrapping, 21
- keys
 - data encryption, 20
 - data-encrypting, 20
 - key-encrypting, 20
 - plaintext, 20
 - weak, 20
- L**
- LDAP, 15
- least privilege, 6, 17
- LUN masking, 4, 16
- M**
- maintenance
 - cryptographic, 23
 - policy, 23
 - system, 5
 - vendor, 12
- malware, 15
- management
 - in-band, 12
 - out-of-band, 11
- media sanitization, 7
- metadata
 - chain of custody, 6
- mistakes, 5
- modems, 12, 13
- multi-key, 21
- N**
- NAS. *See* network attached storage
- network attached storage, 14
 - NFS, 14
 - SMB/CIFS, 15
- network filtering, 12
- NFS

- ACLs, 14
- encryption, 15
- IPsec, 14
- Kerberos, 14
- multi-protocol, 14
- network access, 14
- well-known ports, 14
- NIST**
 - FIPS 197, 17, 25
 - SP 800-38A, 17, 25
 - SP 800-38C, 17, 25
 - SP 800-38D, 17, 25
 - SP 800-57 Part 1, 19, 20, 25
 - SP 800-57 Part 2, 20, 25
 - SP 800-67, 17, 25
 - SP 800-88, 25
 - SP 800-92, 9, 25
- non-repudiation, 5
 - long-term, 23
- NPIV, 16
- NTLMv2, 15
- NTP, 10, 11, 12
- O**
- out-of-area recovery, 6
- P**
- PCI
 - DSS v1.1, 25
- personally identifiable information, 3, 7
- physical access
 - cable plant, 4
 - facilities, 4
 - network infrastructure, 4
 - storage resources, 4
- physical protection, 4
- physical security, 3
- PII. *See* personally identifiable information
- planning
 - DR/BC, 7
- point of encryption, 19
- policy, 3, 7
 - authorization, 23
 - cryptographic
 - maintenance, 23
 - fixed content, 23
 - logging, 9
 - maintenance, 23
 - storage compliance, 7
 - storage-specific, 7
- port authentication, 4
- preservation
 - activities, 23

- orders, 6
- period, 23
- privacy
 - fixed content, 22
- proof
 - of encryption, 19
 - of records retention, 10

R

- RADIUS, 13, 15
- random number generation, 21
- recovery
 - activities, 6
 - disaster, 6
 - key, 21
 - out-of-area, 6
 - plan, 22
 - times, 6
- reliability, 10
- remote network access, 13
- removable media, 18
- replication, 7, 10
 - approach, 11
 - fixed content
 - automatic, 22
 - security, 10
- repurposing, 6
- retention, 6
- risk
 - analysis, 5
 - assessment, 5
 - domains, 3
 - audit logging, 9
 - logical, 4
 - physical, 3
 - virtual, 4

- management, 5
- transfer, 18
- treatment, 5
- roles
 - access permissions, 13
 - fixed content, 22
 - rights and privileges, 5
- rootkits, 15
- RS-232, 11

S

- SAN, 17
- sanitization, 6
 - media, 6
- secure baseline, 13
- security patches, 8
- security scans, 7
- sensitive data, 18
- separation of duties, 13
- service continuity, 3
 - business continuity, 6
 - disaster recovery, 6
- service discovery protocols, 11
- SLP, 11, 12, 16
- SMB/CIFS
 - encryption, 15
- SMI-S, 12
- SMTP, 11
- SNMP, 12
- social engineering, 4
- split-key, 21
- SSH, 11
- SSHv2, 13
- SSL, 11
- storage cloud, 4
- storage security, 2

- strength of encryption, 19
- symmetric encryption modes, 18
- syslog, 9, 10

T

- time source, 9
- TLS, 11
- traceability, 5
- trusted services, 11

V

- virtual
 - server, 4
 - storage, 4
- virtual server images
 - sanitize, 6
- virtualization platforms
 - advertised vulnerabilities, 8
- viruses, 15
- VLANs, 4, 16
- VPN, 11
- vulnerability assessments, 7

W

- weak keys, 20
- WORM, 7, 10
- worms, 15

Z

- zero-day events, 8
- zoning, 4
 - basic, 17