Minimum Security Baseline (MSB) for Software Embedded in Space Systems

Based on ECSS-Q-ST-80-10C, ECSS-E-ST-40C, NIST.SP.800-53r5, CCSDS Magenta, CCSDS Green and CCSDS Blue standards
(*some text was generated by LLM GPT type AI, specifically chatGPT*)

Table of Contents

Version control

Version	Issued date	Description
0.0.1	January, 2025	First unpublished result of a comparison between standards, using OWASP ISVS (Pre-release 1.0RC) as ontology base.

Reference Standards

The following normative documents were harmonized in order to generate a minimum product common to all of them, called Minimum Security Baseline. All of these mentioned below were used in their latest available versions.

CCSDS Green Books	*350.0-G-3 - The Application Of Security To CCSDS Protocols*
	350.1-G-3 - Security Threats Against Space Missions
	350.4-G-2 - CCSDS Guide For Secure System Interconnection
	350.7-G-2 - Security Guide For Mission Planners
CCSDS Magenta Books	*351.0-M-1 - Security Architecture For Space Data Systems*
	354.0-M-1 - Symmetric Key Management
CCSDS Blue Books	*352.0-B-2 - CCSDS Cryptographic Algorithms*
	355.0-B-2 - Space Data Link Security Protocol
	357.0-B-1 - Authentication Credentials
ECSS-E-ST-80C	*Space engineering - Security in space systems lifecycles*
ECSS-E-ST-40C	*Space engineering - Software*
NIST Special Publication 800-53 Revision 5	*Security and Privacy Controls for Information Systems and Organizations*

Supply Chain Requirements

1. Supply Chain Management Requirements
To ensure the authenticity, integrity, and security of components, services, and subsystems across the supply chain, the following key principles and strategies are established:

- **Definition and Implementation of Processes:** Suppliers must define and enforce processes and technical measures to verify the authenticity of components at all stages of the project, including those provided by third parties such as contractors and subcontractors.
- **Flow-Down of Security Requirements:** Security engineering requirements, aligned with standards like ECSS-Q-ST-80 and ECSS-E-ST-40 for software modules, must be communicated to relevant suppliers of security-sensitive products.
- **Vendor Assessment:** Vendors are evaluated based on criticality and sensitivity criteria, ensuring they:
    - Source components from original manufacturers or authorized resellers with clear and traceable bills of materials.
    - Avoid suppliers with a history of significant breaches, intrusions, or data losses.
    - Maintain mature cybersecurity measures and certifications, such as ISO/IEC 27001.
    - Comply with national regulations, including export controls and data protection laws.

2. Acquisition Strategies, Tools, and Methods
Organizations must employ strategies and tools to mitigate supply chain risks and enhance transparency and security, including:

- **Risk-Informed Procurement:** Leverage supply chain risk assessments to guide acquisition strategies. Consider tools like blind buys, tamper-evident packaging, and trusted distribution channels to protect against unauthorized production, counterfeiting, and malicious software.
- **Incentives for Suppliers:** Promote transparency and security by incentivizing suppliers who implement robust controls and adhere to contractual obligations prohibiting tainted or counterfeit components.
- **Contractual Safeguards:** Define documentation protection and enforce security and privacy requirements throughout the development lifecycle via contracts.

  Control Enhancements:

A. **Adequate Supply Controls:** Ensure sufficient availability of critical components by using multiple suppliers, stockpiling spares, or identifying alternative components.
B. **Assessments Before Selection:** Conduct thorough evaluations of systems, components, and services before selection, modification, or acceptance. Techniques include design reviews, physical inspections, and penetration testing.

3. Component Authenticity Policies and Procedures
To protect against counterfeit components, organizations must:

- **Anti-Counterfeit Policies:** Develop procedures to detect and prevent counterfeit items from entering the system. Report incidents to the source of the counterfeit or relevant external organizations (e.g., Cybersecurity and Infrastructure Security Agency - CISA).
- **Training and Awareness:** Train personnel to recognize counterfeit hardware, software, and firmware.
- **Configuration Control:** Maintain strict configuration management for components awaiting service, repair, or reintegration.
- **Scanning for Counterfeits:** Regularly scan system components to identify counterfeit elements using appropriate methods for the component type (e.g., x-ray for hardware or web application scanning for software).

4. Supply Chain Management Plan (SCMP)

Organizations must develop and implement a SCMP, which includes:

- **Privacy and Security Requirements:** Define these based on the criticality of assets and services provided by suppliers.
- **Compliance and Evidence:** Require suppliers to provide statements of compliance with project-specific requirements, supported by credible evidence.
- **Hierarchical Management:** Define and implement supply chain requirements at every level of the customer-supplier network.

  Expected Deliverable for this section:
  A comprehensive **Supply Chain Management Plan (SCMP)**, reviewed and updated at project milestones, including Proposal/ Kick-off meeting (KOM), System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), Qualification Review (QR) and Acceptance Review (AR) phases.

Logging Requirements

1. EVENT LOGGING

- **Control:**

  a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
  b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
  c. Specify the following event types for logging within the system: [Assignment: organization-defined event types along with the frequency of (or situation requiring) logging for each identified event type];
  d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

- **Discussion**: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

  To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

2. CONTENT OF AUDIT RECORDS

- **Control:** Ensure that audit records contain information that establishes the following:

  a. What type of event occurred;
  b. When the event occurred;
  c. Where the event occurred;
  d. Source of the event;
  e. Outcome of the event; and
  f. Identity of any individuals, subjects, or objects/entities associated with the event.

- **Discussion**: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

- **Control Enhancements:**

A. **CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION**: Generate audit records containing the following additional information: [Assignment: organization-defined additional information].

Discussion: The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

B. **CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENT**S: Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].

Discussion: Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

3. AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

- **Control:**

a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;
b. Report findings to [Assignment: organization-defined personnel or roles]; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

- **Discussion**: Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

- **Control Enhancements:**

A. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION**: Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].

Discussion: Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

B. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES**: Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion: Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

C. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS**: Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Discussion: Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

D. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS**: Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

Discussion: Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

E. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING**: Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

   Discussion: The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual’s identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

F. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS**: Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.

   Discussion: Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

G. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS**: Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

   Discussion: Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

H. **AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES**: Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Discussion: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Identification and Authentication Requirements

1. **Credential Specification**

   - **X.509 Certificate Syntax**
     - X.509 V3 certificates shall be used, utilizing generalized time and the CCSDS Calendar Segmented Time Code (CCS).
     - Certificates must adhere to the personal information exchange syntax (PKCS12) and employ a digital signature algorithm.

   - **Protected Simple Authentication Specification**
     - Protected simple authentication must be implemented, leveraging passwords and utilizing the CCS time code formats.
     - A specified cipher algorithm shall be employed to ensure robust protection.

2. **Password-Based Authentication for Protected Credentials**

   - **Password Management and Verification**
     - Maintain and regularly update a list of commonly used, expected, or compromised passwords. This list must be checked whenever users create or update passwords.
     - Require passwords to comply with defined complexity and composition rules, ensuring robust protection against brute-force and dictionary attacks.
     - Encourage the use of long passwords or passphrases, allowing all printable characters, including spaces, to maximize strength and usability.

   - **Secure Password Transmission and Storage**
     - Transmit passwords exclusively over cryptographically protected channels to prevent interception during authentication processes.

    - Store passwords using an approved salted key derivation function, with a preference for keyed hashes, to ensure resistance against offline attacks.

- Recovery and Update Processes
    - Require immediate password updates upon account recovery to minimize the risk of compromise.
    - Employ automated tools to assist users in selecting strong, secure password authenticators.

3. **Integration of Protected Credentials and Authentication Management**

- **X.509 Certificates and Password-Based Protection**
    - Use X.509 certificates alongside password-based authentication for enhanced security. Certificates should be securely transmitted and stored using cryptographic channels and algorithms specified in CCSDS standards.
    - Ensure passwords used in simple authentication are validated against a list of compromised or weak passwords to align with organizational security policies.

- **Cryptographic Alignment**
    - Both X.509 certificates and password-based authentication rely on cryptographic mechanisms, including specified cipher algorithms and secure hash functions, to ensure data integrity and confidentiality.
    - Employ CCS time codes for synchronization and traceability within the authentication process.

4. **Additional Security Considerations**

- Organizations must enforce password composition rules judiciously to balance security and usability, leveraging context-specific guidelines.
- Passwords must be safeguarded against known risks by employing frequent updates, secure recovery practices, and cryptographic enhancements.

Authorization Requirements

The principle of least privilege is a foundational concept in security architecture and privacy engineering. It ensures that each entity—be it a user, system, or component—is granted only the minimum resources and authorizations necessary to perform its designated functions, thereby limiting its scope of action.

1. **Core Principle of Least Privilege**

- Each system component or entity is allocated just enough privileges to accomplish its specified tasks, but no more. This approach minimizes the potential impact of failures, corruption, or misuse, reducing the overall security risk.

- By limiting privileges, the principle also simplifies security analysis, making it easier to assess and mitigate vulnerabilities in individual components.

2. Application in System Design

Least privilege is a pervasive principle that influences all aspects of secure system design:

- Interface Restrictions: Interfaces to invoke component capabilities are restricted to specific subsets of the user population. For example, an audit mechanism may have:
- A configuration interface for the audit manager.
- A collection and storage interface for the audit operator.
- A viewing interface for the audit reviewer, who has no need to modify the data.
- Fine Granularity: The design supports a fine granularity of privilege decomposition, ensuring that users and components only access what is strictly necessary.

3. Internal Structure of Least Privilege

The principle extends beyond user access to the internal structure of systems:

- Encapsulation: Modules are constructed so that only the elements encapsulated within the module are directly operated on by its functions. External elements affected by the module are accessed indirectly through controlled interactions (e.g., function calls).
- Scope Limitation: The scope of a module or component includes only the system elements necessary for its functionality, with access modes carefully restricted to ensure minimal exposure.

4. Benefits of Least Privilege

Applying the least privilege principle:

- Reduces the security impact of a compromised component by limiting its reach and influence within the system.
- Improves the manageability and clarity of security measures, aiding in system analysis and maintenance.
- Ensures that resources and permissions are allocated judiciously, enhancing overall system efficiency and security.

Data Protection Requirements

1. Protection of Confidentiality and Integrity of Information at Rest through Media Sanitization

- To ensure the protection of information at rest, organizations must adopt robust sanitization techniques to eliminate the risk of unauthorized disclosure or reconstruction of sensitive data. These measures apply to system components such as hard disk drives, storage area networks, and databases, as well as portable storage devices. The sanitization process must align with the security category or classification of the data.

2. Cryptographic Methods for Data Protection and Sanitization for protecting and sanitizing information at rest:

- Cryptographic mechanisms, such as encryption, are recommended for securing information during storage. If the information is no longer required, cryptographic erasure—destroying the decryption keys—ensures data cannot be recovered.
- Additional sanitization techniques, including clearing, purging, and destruction, should be employed depending on the sensitivity and classification of the data.

3. Non-Destructive Techniques for Portable Storage Devices

- Portable storage devices, including external hard drives, flash memory, and optical discs, require specific sanitization techniques before reuse or connection to organizational systems. Nondestructive techniques, such as cryptographic wiping or secure overwriting, ensure that information cannot be retrieved while preserving the usability of the devices.

4. Dual Authorization for Secure Sanitization

- Dual authorization is essential for ensuring the effectiveness and accountability of media sanitization processes. By requiring two qualified individuals to oversee and perform sanitization tasks, organizations reduce the risk of errors or unauthorized actions, enhancing the protection of information at rest.

5. Remote Purging or Wiping for Information at Rest

- Organizations must implement remote purging or wiping capabilities for system media to protect against unauthorized access in cases where devices are lost, stolen, or repurposed. Secure remote wiping ensures that information on compromised devices is rendered inaccessible. This process may include overwriting data multiple times or destroying decryption keys used for encrypted data.

6. Sanitization of System Media Prior to Reuse or Disposal

- System media containing information at rest must be sanitized before being reused, disposed of, or released outside organizational control. The sanitization process ensures that the data cannot be reconstructed, mitigating risks associated with unauthorized access. For critical and classified data, trusted sources, such as secure offline storage facilities, should be used for obtaining or replacing sanitized media.

7. Verification and Documentation of Sanitization Processes

- Media sanitization and disposal actions must be thoroughly reviewed, documented, and verified. This includes tracking the sanitization methods, personnel involved, and the effectiveness of the process. Maintaining detailed records ensures compliance with organizational and regulatory standards for protecting information at rest.

8. Comprehensive Cryptographic Key Management for Integrity Protection

- Organizations must establish and manage cryptographic keys to support cryptographic mechanisms that protect the integrity of software, firmware, and information. Key management encompasses key generation, distribution, storage, access control, and destruction, ensuring alignment with organizational policies, standards, and regulatory requirements.
- Proper key management is critical for cryptographic mechanisms such as digital signatures and signed hashes that detect unauthorized changes to software, firmware, and data.

9. Cryptographic Mechanisms for Integrity Verification

- Cryptographic mechanisms, such as digital signatures and signed hashes, rely on robust key management. Digital signatures use asymmetric cryptography, where the private key generates the signature, and the public key verifies it, ensuring that unauthorized modifications are detectable.
- For integrity protection, cryptographic keys must be securely managed to prevent unauthorized access or misuse. This includes safeguarding private keys used to sign hashes and ensuring that public keys are readily available for verification.

10. Key Availability and Recovery

- To maintain operational continuity, organizations must ensure the availability of cryptographic keys. Key escrow mechanisms can mitigate the impact of key loss, such as forgotten passphrases or hardware failures, ensuring integrity protections remain active.

11. Use of Validated Cryptographic Modules

- Cryptographic key management should employ validated cryptographic modules, adhering to standards such as NIST FIPS or NSA-approved guidelines, for both symmetric and asymmetric key operations.
- For symmetric keys, standards such as NIST SP 800-57 provide detailed guidance on key establishment and management. Similarly, asymmetric key management must adhere to frameworks like DoD-approved PKI certificates and hardware security tokens.

12. Integration of Key Management with Cryptographic Protection

- Key management solutions must seamlessly integrate with cryptographic mechanisms used for software, firmware, and information integrity. This includes:
    - Generating and distributing keys in a secure manner.
    - Protecting the confidentiality of keys, particularly private keys, to prevent unauthorized signing of hashes or digital signatures.
    - Maintaining the lifecycle of keys to ensure expired or compromised keys do not compromise integrity protections.

13. Consideration of Advanced Cryptographic Techniques

- Organizations should leverage advanced cryptographic techniques, such as:
  - Signed hashes using algorithms defined in SP 800-56A, SP 800-56B, and SP 800-56C.
  - Hardware security modules or tokens to securely store private keys, preventing exposure during cryptographic operations.

Cryptography Requirements

1. Confidentiality and Integrity Protections

- The protection of information at rest requires mechanisms to safeguard its confidentiality and integrity. Information at rest refers to data stored on system components such as hard disk drives, storage area networks, and databases. Cryptographic methods, including encryption, are essential for preventing unauthorized disclosure and modification of this information. For enhanced security, mechanisms like Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM) are recommended. AES, as specified by NIST FIPS 197 and ISO/IEC 18033-3, provides robust encryption standards suitable for both software and hardware implementations.

2. Cryptographic Algorithms and Modes

To meet a minimum security baseline:

- All CCSDS missions must implement AES for encryption.
- Counter Mode is the preferred mode of operation, offering efficiency and reliability. Other modes may be used but require careful consideration to ensure security.
- When encryption must ensure data integrity and authentication, GCM is mandated. GCM combines high-speed encryption with origin authentication, making it ideal for protecting data at rest and in transit.

3. Cryptographic Key Management

Key size and management are critical for robust cryptographic protection:

- Future implementations require a 256-bit key, while existing systems may use 128-bit keys.
- Cryptographic keys must be stored securely, with options including hardware-protected stores such as Trusted Platform Modules (TPM). Protected storage ensures the keys remain confidential and accessible only to authorized processes.

4. Offline and Hardware-Based Storage

- In cases where online protection is insufficient, organizations should transition sensitive information to offline storage. Offline storage eliminates the risk of unauthorized network access. For added protection, cryptographic keys should utilize hardware-protected storage or safeguards defined by the organization.

5. **Importance of Authenticated Encryption**

- Authenticated Encryption with Associated Data (AEAD), including GCM, addresses the dual need for encryption and origin authentication. Without data origin authentication, encryption security can degrade, emphasizing the necessity of modes like GCM for safeguarding the integrity and confidentiality of stored information.

6. DEVICE IDENTIFICATION AND AUTHENTICATION

- **Control**: Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

- **Discussion**: Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

- **Control Enhancements:**

A. **DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION**: Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.

   Discussion: A local connection is a connection with a device that communicates without the use of a network. A network connection is a connection with a device that communicates through a network. A remote connection is a connection with a device that communicates through an external network. Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk.

B. **DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION**

Discussion: The Dynamic Host Configuration Protocol (DHCP) is an example of a means by which clients can dynamically receive network address assignments.

B.1 Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and

B.2 Audit lease information when assigned to a device.

C. **DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION**: Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].

Discussion: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Device attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices.

7. ACCESS CONTROL

- The basic function of access control is to ensure that data or information-technology resources are available only for authorized users or processes. As a result of ensuring data availability, access-control mechanisms may provide limited confidentiality and integrity. It should be noted, however, that access control is not a fundamental technique for providing these other two security services; it is purely a barrier in the path of a potential intruder.
- Access control requires the use of a number of techniques, including the establishment of access-control information bases in which the access rights of users or processes are maintained securely. Authentication information such as identification, cryptographic credentials (e.g., X.509 certificate, Kerberos ticket), and passwords provide management and control of access to the system. Passwords should be administered effectively by establishing details such as appropriate password length and content, implementing procedures for regularly changing passwords, and ensuring that password secrecy is maintained. It should be noted that automation of password generation increases security significantly. Plaintext passwords should never be transmitted over an unprotected medium. If passwords must be sent over a network, an encryption function (e.g., SSH, TLS, IPSec, or another Virtual Private Network (VPN)) should be used. Audit trails are an important mechanism in security management. They are used to monitor system usage and

password changes, and should contain as much information regarding the system details and previous accesses as possible.

A. Non-Persistence in Cryptographic Key Lifecycle

- The principles of non-persistence directly align with the lifecycle management of cryptographic keys. Non-persistent cryptographic keys, such as Session Keys, are generated and used temporarily for specific sessions or tasks. At the conclusion of their usage, these keys are securely deleted, minimizing their exposure and reducing the risk of advanced persistent threats (APTs). This approach ensures that adversaries have a limited window of opportunity to exploit vulnerabilities.

B. Implementation of Non-Persistent Cryptographic Components

- Non-persistent cryptographic operations can be implemented by:
  - Session Keys: Session Keys are designed for transient use, providing encryption, authentication, or authenticated encryption during their active lifecycle. Once their purpose is fulfilled, they transition to the Destroyed state, ensuring they cannot be reused or exploited.
  - Key Refresh: Periodic refreshing of Session Keys aligns with the non-persistence principle, ensuring that new keys are generated for continued secure operations while minimizing residual exposure to compromised keys.

C. Trusted Sources for Key Generation and Management

- The generation and management of cryptographic keys must utilize trusted and secure sources. For instance:
  - Master Keys in the Pre-Activation state must be securely transmitted using authenticated encryption.
  - Session Keys may be generated on demand and must also be safeguarded during their lifecycle, particularly when transitioning between states.

D. State Transitions and Non-Persistence

- The cryptographic key lifecycle mirrors non-persistent design by organizing keys into distinct states, each with specific operational rules:
  - Pre-Activation State: Keys are securely prepared and held until activated.
  - Active State: Keys are operational for a defined period or session.
  - Deactivated State: Keys no longer in use are retired, maintaining system integrity by limiting their availability.
  - Destroyed State: Keys are securely erased, rendering them irrecoverable, which aligns with the non-persistence requirement of deleting information when no longer needed.

E. Handling Compromised and Non-Persistent Keys

- Keys declared as compromised during any state must be treated as non-persistent assets. They should be limited to processing previously protected information and immediately transitioned to the Destroyed state when feasible. This practice reduces the potential attack surface and aligns with the goal of mitigating risks associated with retaining sensitive cryptographic information.

F. On-Demand and Temporary Connections

- Non-persistence is further supported by the use of cryptographic mechanisms to establish on-demand connections. Session Keys play a critical role here, enabling secure, ephemeral connections that terminate automatically after their intended use. This approach emphasis on minimizing persistent connectivity to limit adversarial movement and reconnaissance within systems.

Bootloader Requirements

1. INFORMATION CATEGORIZATION

In order to select appropriate security controls, organizations must clearly understand the criticality and sensitivity of the information that will be handled by the system according to the criteria of confidentiality, availability, and integrity. Systems may handle several different data types, each with different attributes. An example of information criticality and sensitivity categories applicable to various systems may be found in reference. Military or dual-use systems are usually subject to national security classification regulations that override organizational discretion in categorizing information. Civil systems may be bound by other laws and policies (e.g., export and copyright restrictions) controlling the handling of specific information types. Organizations should identify their system’s operational availability and integrity requirements for the information that may be unaddressed by legal and national-security requirements pertaining to information confidentiality.

2. PROTECTION OF INFORMATION AT REST

Control: Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Discussion: Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases.

However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

3. Encryption Algorithms

3.1 Algorithm and Mode: For a baseline standard, all CCSDS missions must use the AES algorithm. The AES algorithm is defined by NIST's FIPS 197 and ISO/IEC 18033-3.

3.2 Cryptographic Key Size

- Future CCSDS implementations (missions planned after the publication of this specification) are required to use a 256-bit key.
- Existing implementations may continue using a 128-bit key.

3.3 Algorithm Mode of Operation: CCSDS implementations are required to use Counter Mode for encryption. Alternative modes may be employed but must be carefully evaluated before implementation.

3.4 Authenticated Encryption: If encryption needs to ensure both data integrity and origin authentication, GCM is mandatory. The Media Access Control (MAC) size is set at 128 bits. GCM provides high-speed authenticated encryption, can be efficiently parallelized, and does not require padding, making it particularly suited for space applications.

4. Key Lifecycle

4.1 Key Lifecycle State Model: Cryptographic keys follow a lifecycle with the following states:

- Pre-Activation: Keys are newly generated and prepared for operational use.
- Active: Keys are operational and used for cryptographic processes.
- Suspended (Optional): Keys are temporarily inactive but can be reactivated.
- Deactivated: Keys have reached the end of their operational life.
- Destroyed: Keys are securely disposed of and irrecoverable.

A cryptographic key begins its lifecycle in the Pre-Activation state and ends in the Destroyed state. The Suspended state is optional and can be included at mission discretion.

4.2 Pre-Activation State

- Newly generated keys start in this state and remain there unless immediately transitioned to Active state due to security requirements.
- Master Keys in this state must be communicated securely, while Session Keys may use unprotected channels if secured by higher-tier keys.

4.2.1 Transitions:

- Keys move to the Active state upon activation.
- Keys can transition directly to Destroyed state if deemed necessary.

4.3 Active State

- Keys in this state are fully operational and subject to lifetime constraints.
- Only Active state keys are used for cryptographic processes.

4.3.1 Transitions:

- Upon reaching the end of their operational life, keys transition to Deactivated state.
- Keys may also transition to Suspended state temporarily or to Destroyed state upon secure disposal.

4.4 Suspended State

- An optional state for temporarily non-operational keys.
- Suspended keys do not interrupt their operational lifetime and can transition back to Active or move to Deactivated or Destroyed states as needed.

4.5 Deactivated State

- Keys in this state are no longer operational but can still be used for decrypting previously protected data.
- There is no time limit on the Deactivated state.

4.5.1 Transitions:

- Deactivated keys transition to Destroyed state upon secure disposal.

4.6 Destroyed State

- This is the final state, where all operational data associated with the key is permanently unrecoverable.

4.7 Compromised Keys

- Any key in any state can be declared compromised if its confidentiality is breached.
- Compromised keys may still process protected data but should not be used for new cryptographic operations.
- The use of compromised keys should be based on a thorough risk assessment and treated similarly to deactivated keys.