[AGENCY]

[SYSTEM]

Security Plan

Sensitive System Specific

**[DATE]**

**AUTHORIZED BY:**

**[Agency ISO] Date**

**[Agency Head Name and Title] Date**

**[Additional Authorizer Name and Title] Date**

# SECURITY PLAN HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VERSION | AUTHOR | DATE | CHANGES | REVIEWER |
| 1.0 | Chandos Carrow | 01/05/2024 | New Document |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# CONTENTS

[SECURITY PLAN HISTORY 1](#_Toc156907160)

[CONTENTS 1](#_Toc156907161)

[EXECUTIVE SUMMARY 2](#_Toc156907162)

[SYSTEM INVENTORY & DEFINITION 2](#_Toc156907163)

[DATA SET CLASSIFICATION INVENTORY 2](#_Toc156907164)

[BUSINESS PROCESSES 2](#_Toc156907165)

[SYSTEM BOUNDARY DIAGRAM 2](#_Toc156907166)

[INFORMATION FLOW DIAGRAM 3](#_Toc156907167)

[CSRM RESOURCES 4](#_Toc156907168)

[ITRM-SEC530 CONTROLS 4](#_Toc156907169)

[AC – ACCESS CONTROL 4](#_Toc156907170)

[AU - AUDIT AND ACCOUNTABILITY 20](#_Toc156907171)

[CA - SECURITY ASSESSMENT AND AUTHORIZATION 27](#_Toc156907172)

[CM – CONFIGURATION MANAGEMENT 29](#_Toc156907173)

[IA – IDENTIFICATION AND AUTHENTICATION 34](#_Toc156907174)

[IR – INCIDENT RESPONSE 44](#_Toc156907175)

[MA – MAINTENANCE 46](#_Toc156907176)

[PE – PHYSICAL AND ENVIRONMENTAL PROTECTION 48](#_Toc156907177)

[PL – PLANNNING 50](#_Toc156907178)

[RA – RISK ASSESSMENT 51](#_Toc156907179)

[SA – SYSTEM AND SERVICES ACQUISITION 51](#_Toc156907180)

[SC – SYSTEM AND COMMUNICATION PROTECTION 71](#_Toc156907181)

[SI – SYSTEM AND INFORMATION INTEGRITY 96](#_Toc156907182)

[POAM/Remediation Plan Template 110](#_Toc156907183)

# EXECUTIVE SUMMARY

[Please provide an executive summary of the System Security Plan here]

# SYSTEM INVENTORY & DEFINITION

Please use the template located at the following URL to complete the application inventory template. Follow the instructions on the tab labeled “Instructions”. This application information will be populated into the Commonwealth Security and Risk Management (CSRM) governance, risk, and compliance (GRC) application. Upon completion, send the completed inventory spreadsheet to [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)

[Application-Template.xlsm (live.com)](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.vita.virginia.gov%2Fmedia%2Fvitavirginiagov%2Fcommonwealth-security%2Fdocs%2FApplication-Template.xlsm&wdOrigin=BROWSELINK)

[Attach the System Inventory as an appendix to the SSP or insert file object here]

# DATA SET CLASSIFICATION INVENTORY

The purpose of a data classification is to summarize the data types contained within the data set inventory of this system. IT systems should be classified as “sensitive” if a type of data handled by the IT system has two or more classifications with a sensitivity of moderate on the criteria of confidentiality, integrity, and availability. Documentation should be developed and maintained by the agency in cases where this determination is identified as “non-sensitive.” The data classification types are: PCI, PII, PHI, HIPAA, PMI, FTI, FERPA, Control Systems/SCADA, Intellectual Property, Law Enforcement Data, Legal or Legislative Data, Critical Infrastructure Information, and Social Security Administration (SSA). The data set inventory is the complete catalog of the system information and should be completed in the CSRM GRC tool. If you do not have access to the CSRM GRC tool, please submit a request to CommonwealthSecurity@VITA.Virginia.Gov or you may utilize the following template to complete the data set inventory and submit the results to CommonwealthSecurity@VITA.Virginia.Gov

Instructions can be found on the tab labeled “Instructions”.

[Data-Set-Template.xlsm (live.com)](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.vita.virginia.gov%2Fmedia%2Fvitavirginiagov%2Fcommonwealth-security%2Fdocs%2FData-Set-Template.xlsm&wdOrigin=BROWSELINK)

[Attach the Data Set Classification Inventory as to the SSP or insert file object here]

# BUSINESS PROCESSES

Please list the business processes that rely on the system and complete the Business Impact Analysis (BIA) template located at

<https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/docs/BIA_Spreadsheet_Template.xlsx>

[Attach the BIA template as an appendix to the SSP or insert file object here]

# SYSTEM BOUNDARY DIAGRAM

[Provide diagram of system network with device names and asset tags]

# INFORMATION FLOW DIAGRAM

[Insert information flow diagram]

# CSRM RESOURCES

For additional ITRM Policies, Standards & Guidelines please visit: <https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>

# ITRM-SEC530 CONTROLS

The following section contains the SEC530 security control catalog. Please indicate the implementation status for each control and describe in detail the implementation strategy, or how this control will be met for this particular IT system.

*Disclaimer: This control catalog does not account for additional control requirements from other regulatory bodies that the system may be subject to. Future iterations will try to include a more comprehensive list of controls. It is incumbent upon the system owner to know and comply with all state and federal laws and regulations.*

# AC – ACCESS CONTROL

## AC-2 ACCOUNT MANAGEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. account management | automated temporary and emergency account management   Automatically disable temporary and emergency accounts after no more than 30 days.  Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.  Related Controls: None.   1. account management | disable accounts   Disable accounts within 24 hours when the accounts:   * 1. Have expired;   2. Are no longer associated with a user or individual;   3. Are in violation of organizational policy; or   4. Have been inactive for 90 days   Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality, which reduce the attack surface of the system.  Related Controls: None.   1. account management | automated audit actions   Automatically audit account creation, modification, enabling, disabling, and removal actions.  Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.  Related Controls: AU-2, AU-6.   1. account management | inactivity logout   Require that users log out when the session inactivity time has exceeded 30 minutes.  Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.  Related Controls: AC-11.   1. account management | account monitoring for atypical usage    1. Monitor system accounts for atypical or suspicious usage; and    2. Report atypical usage of system accounts to the Information Security Officer, Agency Head, or Chief Information Security Officer.   Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals.  Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.  Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-2-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Each agency shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:  Note: It is strongly recommended technical controls be implemented wherever possible to fulfill the following requirements, understanding that manual processes must sometimes be implemented to compensate for technical controls that might not be feasible.   1. For all internal and external IT systems:    1. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.    2. Disable unneeded accounts in a timely manner.    3. Retain unneeded accounts in a disabled state in accordance with the agency’s records retention policy.    4. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.    5. Require that the System Administrator and the Information Security Officer or designee investigate any unusual system access activities.    6. Require the System and Data Owner approve changes to access level authorizations.    7. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.    8. Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head’s explicit acceptance of defined residual risks.    9. Require that at least two individuals have administrative accounts to each IT system.    10. The information system automatically audits account creation, disabling, and termination actions and notifies, as required, appropriate individuals.    11. Temporarily disable logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.    12. Disable logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes. 2. For all internal IT systems:    1. Require a documented request from the user to establish an account on any internal IT system.    2. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.    3. Require confirmation of the account request and approval by the IT system user’s supervisor and approval by the Data Owner, Data Owner or designee, or ISO to establish accounts for all sensitive IT systems.    4. Require secure delivery of access credentials to the user based on information already on file.    5. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.    6. Promptly remove access when no longer required. 3. For all external IT systems, require secure delivery of access credentials to users of all external IT systems. 4. For all service and hardware accounts:    1. Document account management practices for all agency created service accounts, including, but not limited to granting, administering and terminating accounts. If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the Password Management section of this Standard.   Discussion: None.  Related Controls: None.  Control Enhancements:   1. If the IT system is classified as sensitive, prohibit the use of guest accounts. 2. If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:    1. Are documented according to standard practice and maintained on file;    2. Include access attributes for the account.    3. Are approved by the System Owner and communicated to the ISO; and    4. Expire after a predetermined period, based on sensitivity and risk. 3. For all external IT systems:    1. Require confirmation of the user’s request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.    2. Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail). |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-3 ACCESS ENFORCEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.  Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.  Related Controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC- 24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.  Control Enhancements:   1. access enforcement | role-based access control   Enforce a role-based access control policy over defined subjects and objects and control access based upon organization-defined roles and users authorized to assume such roles.  Discussion: Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization- defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.  Related Controls: None.   1. access enforcement | controlled release   Release information outside of the system only if:   1. The receiving organization authorized system or system component provides security controls that meet Commonwealth security standards; and 2. The organization-defined controls are used to validate the appropriateness of the information designated for release.   Discussion: Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigation measure, organizations procedurally determine whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals’ privacy.  Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.  Related Controls: CA-3, PT-7, PT-8, SA-9, SC-16.   1. access enforcement | restrict access to specific information types   Restrict access to data repositories containing organization-defined information types.  Discussion: Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role- based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.  Related Controls: CM-8, CM-12, CM-13, PM-5. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-4 INFORMATION FLOW ENFORCEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Enforces approved authorizations for controlling the flow of information within the system and between connected systems based on the appropriate organization-defined information flow control policies.  Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.  Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross- domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high- assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).  Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-6 LEAST PRIVILEGE

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. least privilege | log use of privileged functions   Log the execution of privileged functions.  Discussion: The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.  Related Controls: AU-2, AU-3, AU-12.   1. least privilege | prohibit non-privileged users from executing privileged functions   Prevent non-privileged users from executing privileged functions.  Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non- privileged users from executing privileged functions is enforced by AC-3.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-7 UNSUCCESSFUL LOGON ATTEMPTS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Enforce a limit of 5 consecutive invalid logon attempts by a user during a 15 minute period; and 2. Automatically locks the account or node for a minimum of a 30 minute period or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.   Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.  Related Controls: AC-2, AC-9, AU-2, AU-6, IA-5.  Control Enhancements:   1. unsuccessful logon attempts | purge or wipe mobile device   Purge or wipe information from mobile devices based on organization-defined purging or wiping requirements and techniques after 10 consecutive, unsuccessful device logon attempts.  Discussion: A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.  Related Controls: AC-19, MP-5, MP-6.   1. unsuccessful logon attempts | use of alternate authentication factor    1. Allow the use of organization-defined authentication factors that are different from the primary authentication factors after the number of organization- defined consecutive invalid logon attempts have been exceeded; and    2. Enforce a limit of 5 consecutive invalid logon attempts through use of the alternative factors by a user during a 15 minute period.   Discussion: The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.  Related Controls: IA-3. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-8 SYSTEM USE NOTIFICATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Display organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and states that: 2. Users are accessing a system; 3. System usage may be monitored, recorded, and subject to audit; 4. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 5. Use of the system indicates consent to monitoring and recording; 6. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and 7. For publicly accessible systems: 8. Display system use information, before granting further access to the publicly accessible system; 9. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 10. Include a description of the authorized uses of the system.   Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.  Related Controls: AC-14, PL-4, SI-4. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-8-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.  Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-10 CONCURRENT SESSION CONTROL

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Limit the number of concurrent sessions for each server and database administrative account to 5.  Discussion: Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.  Related Controls: SC-23. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-11 DEVICE LOCK

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Prevent further access to the system by initiating a device lock after 15 minutes of inactivity or upon receiving a request from a user; and 2. Retain the device lock until the user reestablishes access using established identification and authentication procedures.   Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.  Related Controls: AC-2, AC-7, IA-11, PL-4.  Control Enhancements:   1. device lock | pattern-hiding displays   Conceal, via the device lock, information previously visible on the display with a publicly viewable image.  Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-12 SESSION TERMINATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Automatically terminate a user session after 24 hours of inactivity.  Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user’s logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.  Related controls: MA-4, SC-10, SC-23.  Control Enhancements:   1. session termination | user-initiated logouts   Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to information resources.  Discussion: Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.  Related Controls: None.   1. session termination | termination message   Display an explicit logout message to users indicating the termination of authenticated communications sessions.  Discussion: Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-17 REMOTE ACCESS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. remote access | monitoring and control   Employ automated mechanisms to monitor and control remote access methods.  Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.  Related Controls: AU-2, AU-6, AU-12, AU-14.   1. remote access | protection of confidentiality and integrity using encryption   Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.  Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.  Related Controls: SC-8, SC-12, SC-13.   1. remote access | managed access control points   Route all remote accesses through authorized and managed network access control points.  Discussion: Organizations consider the Trusted Internet Connections (TIC) initiative [DHS TIC] requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.  Related Controls: SC-7.   1. remote access | authenticate remote commands   Implement organization-defined mechanisms to authenticate organization-defined remote commands.  Discussion: Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.  Related Controls: SC-12, SC-13, SC-23. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-17-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling. 2. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of approved encryption. 3. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the Agency’s remote access capabilities. 4. Document requirements for the physical and logical hardening of remote access devices. 5. Require maintenance of auditable records of all remote access. 6. Where supported by features of the system, session timeouts shall be implemented after a period of no longer than 15 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented. 7. The organization ensures that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.   Discussion: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-18 WIRELESS ACCESS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. wireless access | authentication and encryption   Protect wireless access to the system using authentication of users, devices, and encryption.  Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.  Related Controls: SC-8, SC-12, SC-13.  (3) wireless access | disable wireless networking  Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.  Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AC-21 INFORMATION SHARING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. information sharing | automated decision support   Employ organization-defined automated mechanismsto enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.  Discussion: Automated mechanisms are used to enforce information sharing decisions.  Related Controls: None.   1. information sharing | information search and retrieval   Implement information search and retrieval services that enforce organization-defined information sharing restrictions.  Discussion: Information search and retrieval services identify information system resources relevant to an information need.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# AU - AUDIT AND ACCOUNTABILITY

## AU-3 CONTENT OF AUDIT RECORDS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Ensure that audit records contain information that establishes the following:   * 1. What type of event occurred;   2. When the event occurred;   3. Where the event occurred;   4. Source of the event;   5. Outcome of the event; and   6. 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.  Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.  Control Enhancements:   1. content of audit records | additional audit information   Generate audit records containing the following additional information:please see the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management**.**  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.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AU-4 AUDIT LOG STORAGE CAPACITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Allocate audit log storage capacity to accommodate the retention requirements identified in the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management.  Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.  Related controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.  Control Enhancements:   1. audit log storage capacity | transfer to alternate storage   Transfer audit logs at least once every 30-days to a different system, system component, or media other than the system or system component conducting the logging.  Discussion: Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU- 9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AU-5 RESPONSE TO AUDIT LOGGING PROCESSING FAILURES

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Alert designated organizational officials in near real-time in the event of an audit logging process failure; and 2. Take the following additional actions: investigate the cause of the disruption, take appropriate corrective actions, and shall escalate and report disruptions.   Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization- defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.  Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.  Control Enhancements:   1. response to audit processing failures | real-time alerts   Provide an alert within 15 minutes to appropriate personnel, to include information security personnel, system owner, and business owner when the following audit failure events occur: failure of any audit log types identified in the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management.  Discussion: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).  Related Controls:None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (4) 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.  Related Controls: AU-2, AU-12. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AU-8 TIME STAMPS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Use internal system clocks to generate time stamps for audit records; and 2. Record time stamps for audit records that meets the organizational defined granularity of time measurement based on the sensitivity of the system and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.   Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g. clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.  Related Controls: AU-3, AU-12, AU-14, SC-45. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AU-9 PROTECTION OF AUDIT INFORMATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and 2. Alert the Information Security Officer upon detection of unauthorized access, modification, or deletion of audit information.   Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.  Related Controls: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.  Control Enhancements:   1. protection of audit information | store on separate physical systems or components   Store audit records at least once every 24 hours in a repository that is part of a physically different system or system component than the system or component being audited.  Discussion: Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.  Related Controls: AU-4, AU-5. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## AU-12 AUDIT RECORDS GENERATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on the operating system, services, applications, and network components; 2. Allow System Owner, Data Owner, or Information Security Officer to select event types that are to be logged by specific components of the system; and 3. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.   Discussion: Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.  Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.  Control Enhancements:   1. audit record generation | system-wide and time-correlated audit trail   Compile audit records from all systems and components into a system-wide (logical or physical) audit trail that is time-correlated to within 5 seconds COV authorized time server.  Discussion: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.  Related Controls: AU-8, SC-45.   1. audit record generation | standardized formats   Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.  Discussion: Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.  Related Controls: None.   1. audit record generation | changes by authorized individuals   Provide and implement the capability for the Information Security Officer or designee to change the logging to be performed on all systems and components based on organization-defined selectable event criteria within organization-defined time thresholds.  Discussion: Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).  Related Controls: AC-3. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# CA - SECURITY ASSESSMENT AND AUTHORIZATION

## CA-7 CONTINUOUS MONITORING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. continuous monitoring | risk monitoring   Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:   * 1. Effectiveness monitoring;   2. Compliance monitoring; and   3. Change monitoring.   Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.  Related Controls: None.  (6) continuous monitoring | automation support for monitoring  Ensure the accuracy, currency, and availability of monitoring results for the system using organization-defined automated mechanisms.  Discussion: Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## CA-9 INTERNAL SYSTEM CONNECTIONS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Authorize internal connections of organization-defined system components or classes of components to the system; 2. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; 3. Terminate internal system connections after organization-defined conditions; and 4. Review organization-defined frequency the continued need for each internal connection.   Discussion: Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.  Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.  Control Enhancements:   1. internal system connections | compliance checks   Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.  Discussion: Compliance checks include verification of the relevant baseline configuration.  Related Controls: CM-6. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# CM – CONFIGURATION MANAGEMENT

## CM-5 ACCESS RESTRICTIONS FOR CHANGE

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   1. access restrictions for change | automated access enforcement and audit records    * + - 1. Enforce access restrictions using organization-defined automated mechanisms; and          2. Automatically generate audit records of the enforcement actions.   Discussion: Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after- the-fact actions should organizations discover any unauthorized changes.  Related Controls: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## CM-6 CONFIGURATION SETTINGS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization defined hardening standards; 2. Implement the configuration settings; 3. Identify, document, and approve any deviations from established configuration settings for system components based on operational requirements; and 4. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.   Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.  Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.  Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.  Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## CM-7 LEAST FUNCTIONALITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Configure the system to provide only mission essential capabilities; and 2. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services that are not required for the business function of the system.   Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA- 8, SC-2, and SC-3).  Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC- 2, SC-3, SC-7, SC-37, SI-4.  Control Enhancements:   1. least functionality | periodic review    1. Review the system on a monthly basis or more frequently if required to address an environmental change to identify unnecessary and/or non-secure functions, ports, protocols, software, and services; and    2. Disable or remove functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or non-secure.   Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.  Related Controls: AC-18.  (7) least functionality | code execution in protected environments  Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of Information Security Officer when such code is:   * 1. Obtained from sources with limited or no warranty; and/or   2. Without the provision of source code.   Discussion: Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.  Related Controls: CM-10, SC-44.  (8) least functionality | binary or machine executable code   * 1. Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and   2. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.   Discussion: Binary or machine executable code applies to all sources of binary or machine- executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.  Related Controls: SA-5, SA-22.  (9) least functionality | prohibiting the use of unauthorized hardware   * 1. Identify through the Commonwealth of Virginia Technology Roadmaps the hardware components authorized for system use;   2. Prohibit the use or connection of unauthorized hardware components;   3. Review and update the list of authorized hardware components at least on a monthly basis.   Discussion: Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## CM-11 USER-INSTALLED SOFTWARE

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (2) user-installed software | software installation with privileged status  Allow user installation of software only with explicit privileged status.  Discussion: Privileged status can be obtained, for example, by serving in the role of system administrator.  Related Controls: AC-5, AC-6. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## CM-14 SIGNED COMPONENTS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.  Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.  Related Controls: CM-7, SC-12, SC-13, SI-7. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# IA – IDENTIFICATION AND AUTHENTICATION

## IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.  Discussion: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [HSPD 12]. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.  Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.  The use of encrypted virtual private networks for network connections between organization- controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.  Related Controls: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA- 5, PE-2, PL-4, SA-4, SA-8.  Control Enhancements:   1. identification and authentication (organizational users) | multi-factor authentication to privileged accounts   Implement multi-factor authentication for access to privileged accounts.  Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.  Related Controls: AC-5, AC-6.  (5) identification and authentication (organizational users) | individual authentication with group authentication  When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.  Discussion: Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.  Related Controls: None.  (6) identification and authentication (organizational users) | access to accounts – separate device  Implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:   * 1. One of the factors is provided by a device separate from the system gaining access; and   2. The device meets organization-defined strength of mechanism requirements.   Discussion: The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.  Related Controls: AC-6.  (8) identification and authentication (organizational users) | access to accounts – replay resistant  Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.  Discussion: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.  Related Controls: None.  (10) identification and authentication (organizational users) | single sign-on  Provide a single sign-on capability for organization-defined system accounts and services.  Discussion: Single sign-on enables users to log in once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add multi-factor authentication for applications and systems (existing and new) that may not be able to natively support multi-factor authentication.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-4 IDENTIFIER MANAGEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (9) identifier management | attribute maintenance and protection  Maintain the attributes for each uniquely identified individual, device, or service in organization-defined protected central storage.  Discussion: For each of the entities covered in IA-2, IA-3, IA-8, and IA-9, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-5 AUTHENTICATION MANAGEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Manage system authenticators by:   1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; 2. Establishing initial authenticator content for any authenticators issued by the organization; 3. Ensuring that authenticators have sufficient strength of mechanism for their intended use; 4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; 5. Changing default authenticators prior to first use; 6. Changing or refreshing authenticators at least every 90 days and a minimum of 1 day or at least on an annual basis when multi-factor authentication occurs; 7. Protecting authenticator content from unauthorized disclosure and modification; 8. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and 9. Changing authenticators for group or role accounts when membership to those accounts changes.   Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.  Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.  Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.  Control Enhancements:   1. authenticator management | password-based authentication   For password-based authentication:   * + 1. Maintain a list of commonly-used, expected, or compromised passwords and update the list at least on a quarterly basis and when organizational passwords are suspected to have been compromised directly or indirectly;     2. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);     3. Transmit passwords only over cryptographically-protected channels;     4. Store passwords using an approved salted key derivation function, preferably using a keyed hash;     5. Require immediate selection of a new password upon account recovery;     6. Allow user selection of long passwords and passphrases, including spaces and all printable characters;     7. [Withdrawn: Not applicable to COV.]; and     8. Enforce the following composition and complexity rules:        1. When a password is the only authenticator:           1. At least 14 characters in length;           2. Utilize each of the following four:   Special characters;  Alphabetical characters;  Numerical characters;  Combination of upper case and lower case letters; and   * + - * 1. Prohibits password reuse for 24 generations.       1. When used as a component of multi-factor authentication:          1. At least 8 characters in length;   Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.  Related Controls: IA-6.  (12) authenticator management | biometric authentication performance  For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements as described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.  Discussion: Unlike password-based authentication, which provides exact matches of user- input passwords to stored passwords, biometric authentication does not provide exact matches. Depending on the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and the stored biometric that serves as the basis for comparison. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system.  Related Controls: AC-7.  (13) authenticator management | expiration of cached authenticators  Prohibit the use of cached authenticators after organization-defined time period.  Discussion: Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.  Related Controls: None.  (18) authenticator management | password managers   * 1. Employ organization-defined password managers to generate and manage passwords; and   2. Protect the passwords using organization-defined controls.   Discussion: For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords (see IA-5(1)(d)) and storing the collection offline in a token.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-5-COV-2

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: An organization sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may:   1. Determine the appropriate validity period of the password, commensurate with sensitivity and risk; 2. Determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk; and 3. Allow the citizen to continue to use the initial password so long as the Agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.   The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.  Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-6 AUTHENTICATION FEEDBACK

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.  Discussion: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.  Related Controls: AC-3. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.  Discussion: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.  Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.  Discussion: Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.  Related Controls: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA- 3, SA-4, SC-8.  Control Enhancements:  (4) identification and authentication (non-organizational users) | use of defined profiles  Conform to the following profiles for identity management as described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.  Discussion: Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the standards and technology implementations are assessed and scoped against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-8-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | 1. Accept only external authenticators that are NIST-compliant; and 2. Document and maintain a list of accepted external authenticators.   Discussion: Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with [SP 800-63B]. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Uniquely identify and authenticate on system services and applications before establishing communications with devices, users, or other services or applications.  Discussion: Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.  Related Controls: IA-3, IA-4, IA-5, SC-8. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IA-11 RE-AUTHENTICATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Require users to re-authenticate when organization-defined circumstances or situations requiring re-authentication.  Discussion: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.  Related Controls: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# IR – INCIDENT RESPONSE

## IR-1-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: The organization:   1. Shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following: 2. Designate an individual responsible for the agency’s threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance. 3. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). 4. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible. 5. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews. 6. Shall or shall require that its service provider, document and implement information security monitoring and logging practices that include the following components, at a minimum: 7. Designate individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs. 8. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place. 9. Prohibit the installation or use of unauthorized monitoring devices. 10. Prohibit the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head. 11. Shall document information security incident handling practices and where appropriate the agency shall incorporate its service provider’s procedures for incident handling practices that include the following at a minimum: 12. Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks. 13. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services. 14. Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks and zero-day exploits. 15. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## IR-4 INCIDENT HANDLING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (5) incident handling | automatic disabling of system  Implement a configurable capability to automatically disable the system if organization-defined security violations are detected.  Discussion: Organizations consider whether the capability to automatically disable the system conflicts with continuity of operations requirements specified as part of CP-2 or IR- 4(3). Security violations include cyber-attacks that have compromised the integrity of the system or exfiltrated organizational information and serious errors in software programs that could adversely impact organizational missions or functions or jeopardize the safety of individuals.  Related Controls: None.  (14) incident handling | security operations center  Establish and maintain a security operations center.  Discussion: A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization’s systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources.  These sources include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# MA – MAINTENANCE

## MA-3 MAINTENANCE TOOLS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (4) maintenance tools | restricted tool use  Restrict the use of maintenance tools to authorized personnel only.  Discussion: Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.  Related Controls: AC-3, AC-5, AC-6.  (5) maintenance tools | execution with privilege  Monitor the use of maintenance tools that execute with increased privilege.  Discussion: Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.  Related Controls: AC-3, AC-6.  (6) maintenance tools | software updates and patches  Inspect maintenance tools to ensure the latest software updates and patches are installed.  Discussion: Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.  Related Controls: AC-3, AC-6. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## MA-4 NONLOCAL MAINTENANCE

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (6) nonlocal maintenance | cryptographic protection  Implements the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: organization-defined cryptographic mechanisms.  Discussion: Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized access during remote maintenance sessions can result in a variety of hostile actions, including malicious code insertion, unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.  Related Controls: SC-8, SC-12, SC-13.  (7) nonlocal maintenance | disconnect verification  Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.  Discussion: Verifying the termination of a connection once maintenance is completed ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.  Related Controls: AC-12. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# PE – PHYSICAL AND ENVIRONMENTAL PROTECTION

## PE-1-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal. 2. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats. 3. All data centers must meet the requirements of a Tier III data center as defined by the Uptime Institute.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## PE-3-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).  Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## PE-18-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: The organization shall develop and publish a policy that requires all information system components such that:   1. All information system components and services remain within the United States. 2. All data and system information associated with the information system components and services remain within the Unites States. 3. All physical components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must be housed within approved storage locations and clearly marked. 4. All virtual components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must reside in hypervisors that are hardened to meet or exceed commonwealth security requirements for the guest VMs or data being processed or stored within the hypervisors control. 5. Each hypervisor can only host one tier of the application architecture and no hypervisor may host the application interface and the data storage component for any information system, even if the components in question do not interact within the same information system. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# PL – PLANNNING

## PL-2-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of: 2. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls; 3. How these controls provide adequate mitigation of risks to which the IT system is subject. 4. Submit the IT System Security Plan to the Agency Head or designated ISO for approval. 5. Plan, document, and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# RA – RISK ASSESSMENT

## RA-10 THREAT HUNTING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Establish and maintain a cyber threat hunting capability to:    1. Search for indicators of compromise in organizational systems; and    2. Detect, track, and disrupt threats that evade existing controls; and 2. Employ the threat hunting capability at least on an annual basis.   Discussion: Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.  Related Controls: CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# SA – SYSTEM AND SERVICES ACQUISITION

## SA-3-COV-1

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Project Initiation:    1. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.    2. Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system.    3. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.    4. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks. 2. Project Definition:    1. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.    2. Incorporate IT security requirements in IT system design specifications.    3. Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.    4. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.    5. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective. 3. Implementation:    1. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.    2. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.    3. Require that the system comply with all relevant Risk Management requirements in this Standard.    4. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see IT Systems Security Plans) of this document. 4. Disposition:    1. Require retention of the data handled by an IT system in accordance with the agency’s records retention policy prior to disposing of the IT system.    2. Require that electronic media is sanitized prior to disposal, as documented (see Data Storage Media Protection), so that all data is removed from the IT system.    3. Verify the disposal of hardware and software in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SA-3-COV-2

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Each Information Security Officer is accountable for ensuring the following steps are documented and followed:   1. Application Planning:    1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.    2. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.    3. Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.    4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:       1. Encrypted communication channels shall be established for the transmission of sensitive information;       2. Sensitive information shall not be transmitted in plain text between the client and the application; and       3. Sensitive information shall not be stored in hidden fields that are part of the application interface. 2. Application Development:   The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development:   * 1. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.   2. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.   3. Data storage shall be separated physically from the application interface (i.e., design two or three tier architectures where the same hypervisor does not host both the application interface and the data storage instance).   4. Agencies shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).   5. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.   6. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted   7. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.   8. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.   9. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.  1. Production and Maintenance:    1. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.    2. Internet-facing applications classified as sensitive shall have periodic, not to exceed 90 days, vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:   * + 1. security and privacy engineering principles | clear abstractions   Implement the security design principle of clear abstractions.  Discussion: The principle of clear abstractions states that a system has simple, well-defined interfaces and functions that provide a consistent and intuitive view of the data and how the data is managed. The clarity, simplicity, necessity, and sufficiency of the system interfaces—combined with a precise definition of their functional behavior—promotes ease of analysis, inspection, and testing as well as the correct and secure use of the system. The clarity of an abstraction is subjective. Examples that reflect the application of this principle include avoidance of redundant, unused interfaces; information hiding; and avoidance of semantic overloading of interfaces or their parameters. Information hiding (i.e., representation- independent programming), is a design discipline used to ensure that the internal representation of information in one system component is not visible to another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.  Related Controls: None.   * + 1. security and privacy engineering principles | least common mechanism   Implement the security design principle of least common mechanism in organization-defined systems or system components.  Discussion: The principle of least common mechanism states that the amount of mechanism common to more than one user and depended on by all users is minimized [POPEK74].  Mechanism minimization implies that different components of a system refrain from using the same mechanism to access a system resource. Every shared mechanism (especially a mechanism involving shared variables) represents a potential information path between users and is designed with care to ensure that it does not unintentionally compromise security [SALTZER75]. Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing the system state among different programs. A single program that corrupts a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels [LAMPSON73].  Related Controls: None.   * + 1. security and privacy engineering principles | modularity and layering   Implement the security design principles of modularity and layering in organization-defined systems or system components.  Discussion: The principles of modularity and layering are fundamental across system engineering disciplines. Modularity and layering derived from functional decomposition are effective in managing system complexity by making it possible to comprehend the structure of the system. Modular decomposition, or refinement in system design, is challenging and resists general statements of principle. Modularity serves to isolate functions and related data structures into well-defined logical units. Layering allows the relationships of these units to be better understood so that dependencies are clear and undesired complexity can be avoided. The security design principle of modularity extends functional modularity to include considerations based on trust, trustworthiness, privilege, and security policy.  Security-informed modular decomposition includes the allocation of policies to systems in a network, separation of system applications into processes with distinct address spaces, allocation of system policies to layers, and separation of processes into subjects with distinct privileges based on hardware-supported privilege domains.  Related Controls: SC-2, SC-3.   * + 1. security and privacy engineering principles | partially ordered dependencies   Implement the security design principle of partially ordered dependencies in organization-defined systems or system components.  Discussion: The principle of partially ordered dependencies states that the synchronization, calling, and other dependencies in the system are partially ordered. A fundamental concept in system design is layering, whereby the system is organized into well-defined, functionally related modules or components. The layers are linearly ordered with respect to inter-layer dependencies, such that higher layers are dependent on lower layers. While providing functionality to higher layers, some layers can be self-contained and not dependent on lower layers. While a partial ordering of all functions in a given system may not be possible, if circular dependencies are constrained to occur within layers, the inherent problems of circularity can be more easily managed. Partially ordered dependencies and system layering contribute significantly to the simplicity and coherency of the system design. Partially ordered dependencies also facilitate system testing and analysis.  Related Controls: None.   * + 1. security and privacy engineering principles | efficiently mediated access   Implement the security design principle of efficiently mediated access in organization-defined systems or system components.  Discussion: The principle of efficiently mediated access states that policy enforcement mechanisms utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints. The mediation of access to system resources (i.e., CPU, memory, devices, communication ports, services, infrastructure, data, and information) is often the predominant security function of secure systems. It also enables the realization of protections for the capability provided to stakeholders by the system. Mediation of resource access can result in performance bottlenecks if the system is not designed correctly. For example, by using hardware mechanisms, efficiently mediated access can be achieved. Once access to a low-level resource such as memory has been obtained, hardware protection mechanisms can ensure that out-of-bounds access does not occur.  Related Controls: AC-25.   * + 1. security and privacy engineering principles | minimized sharing   Implement the security design principle of minimized sharing in organization-defined systems or system components.  Discussion: The principle of minimized sharing states that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify system design and implementation. In order to protect user-domain resources from arbitrary active entities, no resource is shared unless that sharing has been explicitly requested and granted. The need for resource sharing can be motivated by the design principle of least common mechanism in the case of internal entities or driven by stakeholder requirements. However, internal sharing is carefully designed to avoid performance and covert storage and timing channel problems. Sharing via common mechanism can increase the susceptibility of data and information to unauthorized access, disclosure, use, or modification and can adversely affect the inherent capability provided by the system. To minimize sharing induced by common mechanisms, such mechanisms can be designed to be reentrant or virtualized to preserve separation.  Moreover, the use of global data to share information is carefully scrutinized. The lack of encapsulation may obfuscate relationships among the sharing entities.  Related Controls: SC-31.   * + 1. security and privacy engineering principles | reduced complexity   Implement the security design principle of reduced complexity in organization-defined systems or system components.  Discussion: The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more analyzable, and less prone to error. The reduced complexity principle applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential. Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain; that is, simpler systems contain fewer vulnerabilities. An benefit of reduced complexity is that it is easier to understand whether the intended security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and the existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex.  Transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6) may require implementing the older and newer technologies simultaneously during the transition period. This may result in a temporary increase in system complexity during the transition.  Related Controls: None.   * + 1. security and privacy engineering principles | secure evolvability   Implement the security design principle of secure evolvability in organization-defined systems or system components.  Discussion: The principle of secure evolvability states that a system is developed to facilitate the maintenance of its security properties when there are changes to the system’s structure, interfaces, interconnections (i.e., system architecture), functionality, or configuration (i.e., security policy enforcement). Changes include a new, enhanced, or upgraded system capability; maintenance and sustainment activities; and reconfiguration. Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic direction, anticipated changes in the threat environment, and anticipated maintenance and sustainment needs. It is unrealistic to expect that complex systems remain secure in contexts not envisioned during development, whether such contexts are related to the operational environment or to usage. A system may be secure in some new contexts, but there is no guarantee that its emergent behavior will always be secure. It is easier to build trustworthiness into a system from the outset, and it follows that the sustainment of system trustworthiness requires planning for change as opposed to adapting in an ad hoc or non-methodical manner. The benefits of this principle include reduced vendor life cycle costs, reduced cost of ownership, improved system security, more effective management of security risk, and less risk uncertainty.  Related Controls: CM-3.   * + 1. security and privacy engineering principles | trusted components   Implement the security design principle of trusted components in organization-defined systems or system components.  Discussion: The principle of trusted components states that a component is trustworthy to at least a level commensurate with the security dependencies it supports (i.e., how much it is trusted to perform its security functions by other components). This principle enables the composition of components such that trustworthiness is not inadvertently diminished and the trust is not consequently misplaced. Ultimately, this principle demands some metric by which the trust in a component and the trustworthiness of a component can be measured on the same abstract scale. The principle of trusted components is particularly relevant when considering systems and components in which there are complex chains of trust dependencies. A trust dependency is also referred to as a trust relationship and there may be chains of trust relationships.  The principle of trusted components also applies to a compound component that consists of subcomponents (e.g., a subsystem), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is that of its least trustworthy subcomponent. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than the conservative assumption. However, any such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives as well as relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defense-in-depth layering within the component or a replication of components. Defense-in- depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.  Related Controls: None.   * + 1. security and privacy engineering principles | hierarchical trust   Implement the security design principle of hierarchical trust in organization- defined systems or system components.  Discussion: The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for trustworthiness reasoning or an assurance case (assurance argument) when composing a secure system from heterogeneously trustworthy components. To analyze a system composed of heterogeneously trustworthy components for its trustworthiness, it is essential to eliminate circular dependencies with regard to the trustworthiness. If a more trustworthy component located in a lower layer of the system were to depend on a less trustworthy component in a higher layer, this would, in effect, put the components in the same “less trustworthy” equivalence class per the principle of trusted components. Trust relationships, or chains of trust, can have various manifestations. For example, the root certificate of a certificate hierarchy is the most trusted node in the hierarchy, whereas the leaves in the hierarchy may be the least trustworthy nodes. Another example occurs in a layered high-assurance system where the security kernel (including the hardware base), which is located at the lowest layer of the system, is the most trustworthy component. The principle of hierarchical trust, however, does not prohibit the use of overly trustworthy components. There may be cases in a system of low trustworthiness where it is reasonable to employ a highly trustworthy component rather than one that is less trustworthy (e.g., due to availability or other cost-benefit driver). For such a case, any dependency of the highly trustworthy component upon a less trustworthy component does not degrade the trustworthiness of the resulting low-trust system.  Related Controls: None.   * + 1. security and privacy engineering principles | inverse modification threshold   Implement the security design principle of inverse modification threshold in organization-defined systems or system components.  Discussion: The principle of inverse modification threshold builds on the principle of trusted components and the principle of hierarchical trust and states that the degree of protection provided to a component is commensurate with its trustworthiness. As the trust placed in a component increases, the protection against unauthorized modification of the component also increases to the same degree. Protection from unauthorized modification can come in the form of the component’s own self-protection and innate trustworthiness, or it can come from the protections afforded to the component from other elements or attributes of the security architecture (to include protections in the environment of operation).  Related Controls: None.   * + 1. security and privacy engineering principles | hierarchical protection   Implement the security design principle of hierarchical protection in organization-defined systems or system components.  Discussion: The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted component, it protects itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it protects itself from all untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel. The trustworthiness of users is a consideration for applying the principle of hierarchical protection. A trusted system need not protect itself from an equally trustworthy user, reflecting use of untrusted systems in “system high” environments where users are highly trustworthy and where other protections are put in place to bound and protect the “system high” execution environment.  Related Controls: None.   * + 1. security and privacy engineering principles | minimized security elements   Implement the security design principle of minimized security elements in organization-defined systems or system components.  Discussion: The principle of minimized security elements states that the system does not have extraneous trusted components. The principle of minimized security elements has two aspects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally costlier to construct and implement, owing to the increased rigor of development processes. Trusted components require greater security analysis to qualify their trustworthiness. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. The analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to ascertain than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.  Related Controls: None.   * + 1. security and privacy engineering principles | least privilege   Implement the security design principle of least privilege in organization- defined systems or system components.  Discussion: The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified.  Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has need to view the audit data that has been collected but no need to perform operations on that data.  In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated on by the functions within the module. Elements external to a module that may be affected by the module’s operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality and that the access modes for the elements (e.g., read, write) are minimal.  Related Controls: AC-6, CM-7.   * + 1. security and privacy engineering principles | predicate permission   Implement the security design principle of predicate permission in organization-defined systems or system components.  Discussion: The principle of predicate permission states that system designers consider requiring multiple authorized entities to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is allowed to proceed. [SALTZER75] originally named predicate permission the separation of privilege. It is also equivalent to separation of duty. The division of privilege among multiple parties decreases the likelihood of abuse and provides the safeguard that no single accident, deception, or breach of trust is sufficient to enable an unrecoverable action that can lead to significantly damaging effects. The design options for such a mechanism may require simultaneous action (e.g., the firing of a nuclear weapon requires two different authorized individuals to give the correct command within a small time window) or a sequence of operations where each successive action is enabled by some prior action, but no single individual is able to enable more than one action.  Related Controls: AC-5.   * + 1. security and privacy engineering principles | self-reliant trustworthiness   Implement the security design principle of self-reliant trustworthiness in organization-defined systems or system components.  Discussion: The principle of self-reliant trustworthiness states that systems minimize their reliance on other systems for their own trustworthiness. A system is trustworthy by default, and any connection to an external entity is used to supplement its function. If a system were required to maintain a connection with another external entity in order to maintain its trustworthiness, then that system would be vulnerable to malicious and non-malicious threats that could result in the loss or degradation of that connection. The benefit of the principle of self-reliant trustworthiness is that the isolation of a system will make it less vulnerable to attack. A corollary to this principle relates to the ability of the system (or system component) to operate in isolation and then resynchronize with other components when it is rejoined with them.  Related Controls: None.   * + 1. security and privacy engineering principles | secure distributed composition   Implement the security design principle of secure distributed composition in organization-defined systems or system components.  Discussion: The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy result in a system that enforces that policy at least as well as the individual components do. Many of the design principles for secure systems deal with how components can or should interact. The need to create or enable a capability from the composition of distributed components can magnify the relevancy of these principles. In particular, the translation of security policy from a stand-alone to a distributed system or a system-of-systems can have unexpected or emergent results. Communication protocols and distributed data consistency mechanisms help to ensure consistent policy enforcement across a distributed system. To ensure a system-wide level of assurance of correct policy enforcement, the security architecture of a distributed composite system is thoroughly analyzed.  Related Controls: None.   * + 1. security and privacy engineering principles | trusted communication channels   Implement the security design principle of trusted communications channels in organization-defined systems or system components.  Discussion: The principle of trusted communication channels states that when composing a system where there is a potential threat to communications between components (i.e., the interconnections between components), each communication channel is trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions). Trusted communication channels are achieved by a combination of restricting access to the communication channel (to ensure an acceptable match in the trustworthiness of the endpoints involved in the communication) and employing end-to-end protections for the data transmitted over the communication channel (to protect against interception and modification and to further increase the assurance of proper end-to-end communication).  Related Controls: SC-8, SC-12, SC-13.   * + 1. security and privacy engineering principles | continuous protection   Implement the security design principle of continuous protection in organization-defined systems or system components.  Discussion: The principle of continuous protection states that components and data used to enforce the security policy have uninterrupted protection that is consistent with the security policy and the security architecture assumptions. No assurances that the system can provide the confidentiality, integrity, availability, and privacy protections for its design capability can be made if there are gaps in the protection. Any assurances about the ability to secure a delivered capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unprotected while under control of the system (i.e., during the creation, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruption, and shutdown). Continuous protection requires adherence to the precepts of the reference monitor concept (i.e., every request is validated by the reference monitor; the reference monitor is able to protect itself from tampering; and sufficient assurance of the correctness and completeness of the mechanism can be ascertained from analysis and testing) and the principle of secure failure and recovery (i.e., preservation of a secure state during error, fault, failure, and successful attack; preservation of a secure state during recovery to normal, degraded, or alternative operational modes).  Continuous protection also applies to systems designed to operate in varying configurations, including those that deliver full operational capability and degraded-mode configurations that deliver partial operational capability. The continuous protection principle requires that changes to the system security policies be traceable to the operational need that drives the configuration and be verifiable (i.e., it is possible to verify that the proposed changes will not put the system into an insecure state). Insufficient traceability and verification may lead to inconsistent states or protection discontinuities due to the complex or undecidable nature of the problem. The use of pre-verified configuration definitions that reflect the new security policy enables analysis to determine that a transition from old to new policies is essentially atomic and that any residual effects from the old policy are guaranteed to not conflict with the new policy. The ability to demonstrate continuous protection is rooted in the clear articulation of life cycle protection needs as stakeholder security requirements.  Related Controls: AC-25.   * + 1. security and privacy engineering principles | secure metadata management   Implement the security design principle of secure metadata management in organization-defined systems or system components.  Discussion: The principle of secure metadata management states that metadata are “first class” objects with respect to security policy when the policy requires either complete protection of information or that the security subsystem be self-protecting. The principle of secure metadata management is driven by the recognition that a system, subsystem, or component cannot achieve self-protection unless it protects the data it relies on for correct execution. Data is generally not interpreted by the system that stores it. It may have semantic value (i.e., it comprises information) to users and programs that process the data. In contrast, metadata is information about data, such as a file name or the date when the file was created. Metadata is bound to the target data that it describes in a way that the system can interpret, but it need not be stored inside of or proximate to its target data.  There may be metadata whose target is itself metadata (e.g., the classification level or impact level of a file name), including self-referential metadata.  The apparent secondary nature of metadata can lead to neglect of its legitimate need for protection, resulting in a violation of the security policy that includes the exfiltration of information. A particular concern associated with insufficient protections for metadata is associated with multilevel secure (MLS) systems. MLS systems mediate access by a subject to an object based on relative sensitivity levels. It follows that all subjects and objects in the scope of control of the MLS system are either directly labeled or indirectly attributed with sensitivity levels. The corollary of labeled metadata for MLS systems states that objects containing metadata are labeled. As with protection needs assessments for data, attention is given to ensure that the confidentiality and integrity protections are individually assessed, specified, and allocated to metadata, as would be done for mission, business, and system data.  Related Controls: None.   * + 1. security and privacy engineering principles | self-analysis   Implement the security design principle of self-analysis in organization- defined systems or system components.  Discussion: The principle of self-analysis states that a system component is able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability is commensurate with the level of trustworthiness invested in the system. At the system level, self-analysis can be achieved through hierarchical assessments of trustworthiness established in a bottom-up fashion. In this approach, the lower-level components check for data integrity and correct functionality (to a limited extent) of higher- level components. For example, trusted boot sequences involve a trusted lower-level component that attests to the trustworthiness of the next higher-level components so that a transitive chain of trust can be established. At the root, a component attests to itself, which usually involves an axiomatic or environmentally enforced assumption about its integrity.  Results of the self-analyses can be used to guard against externally induced errors, internal malfunction, or transient errors. By following this principle, some simple malfunctions or errors can be detected without allowing the effects of the error or malfunction to propagate outside of the component. Further, the self-test can be used to attest to the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.  Related Controls: CA-7.   * + 1. security and privacy engineering principles | accountability and traceability   Implement the security design principle of accountability and traceability in organization-defined systems or system components.  Discussion: The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-object interactions) to the entity on whose behalf the action is being taken. The principle of accountability and traceability requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., an audit subsystem). To record the details about actions, the system is able to uniquely identify the entity on whose behalf the action is being carried out and also record the relevant sequence of actions that are carried out. The accountability policy also requires that audit trail itself be protected from unauthorized access and modification. The principle of least privilege assists in tracing the actions to particular entities, as it increases the granularity of accountability. Associating specific actions with system entities, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provide non-repudiation because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serves is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or component that allowed the violation of the security policy and the actions of individuals associated with the violation of the security policy.  Related Controls: AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.   * + 1. security and privacy engineering principles | secure defaults   Implement the security design principle of secure defaults in organization- defined systems or system components.  Discussion: The principle of secure defaults states that the default configuration of a system (including its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults applies to the initial (i.e., default) configuration of a system as well as to the security engineering and design of access control and other security functions that follow a “deny unless explicitly authorized” strategy. The initial configuration aspect of this principle requires that any “as shipped” configuration of a system, subsystem, or system component does not aid in the violation of the security policy and can prevent the system from operating in the default configuration for those cases where the security policy itself requires configuration by the operational user.  Restrictive defaults mean that the system will operate “as-shipped” with adequate self- protection and be able to prevent security breaches before the intended security policy and system configuration is established. In cases where the protection provided by the “as- shipped” product is inadequate, stakeholders assess the risk of using it prior to establishing a secure initial state. Adherence to the principle of secure defaults guarantees that a system is established in a secure state upon successfully completing initialization. In situations where the system fails to complete initialization, either it will perform a requested operation using secure defaults or it will not perform the operation. Refer to the principles of continuous protection and secure failure and recovery that parallel this principle to provide the ability to detect and recover from failure.  The security engineering approach to this principle states that security mechanisms deny requests unless the request is found to be well-formed and consistent with the security policy. The insecure alternative is to allow a request unless it is shown to be inconsistent with the policy. In a large system, the conditions that are satisfied to grant a request that is denied by default are often far more compact and complete than those that would need to be checked in order to deny a request that is granted by default.  Related Controls: CM-2, CM-6, SA-4.   * + 1. security and privacy engineering principles | secure failure and recovery   Implement the security design principle of secure failure and recovery in organization-defined systems or system components.  Discussion: The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The principle of secure failure and recovery parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated. In addition, when specified, the system is capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operations while ensuring that a secure state is maintained such that security policies are not violated.  Failure is a condition in which the behavior of a component deviates from its specified or expected behavior for an explicitly documented input. Once a failed security function is detected, the system may reconfigure itself to circumvent the failed component while maintaining security and provide all or part of the functionality of the original system, or it may completely shut itself down to prevent any further violation of security policies. For this to occur, the reconfiguration functions of the system are designed to ensure continuous enforcement of security policy during the various phases of reconfiguration.  Another technique that can be used to recover from failures is to perform a rollback to a secure state (which may be the initial state) and then either shutdown or replace the service or component that failed such that secure operations may resume. Failure of a component may or may not be detectable to the components using it. The principle of secure failure indicates that components fail in a state that denies rather than grants access. For example, a nominally “atomic” operation interrupted before completion does not violate security policy and is designed to handle interruption events by employing higher-level atomicity and rollback mechanisms (e.g., transactions). If a service is being used, its atomicity properties are well-documented and characterized so that the component availing itself of that service can detect and handle interruption events appropriately. For example, a system is designed to gracefully respond to disconnection and support resynchronization and data consistency after disconnection.  Failure protection strategies that employ replication of policy enforcement mechanisms, sometimes called defense in depth, can allow the system to continue in a secure state even when one mechanism has failed to protect the system. If the mechanisms are similar, however, the additional protection may be illusory, as the adversary can simply attack in series. Similarly, in a networked system, breaking the security on one system or service may enable an attacker to do the same on other similar replicated systems and services. By employing multiple protection mechanisms whose features are significantly different, the possibility of attack replication or repetition can be reduced. Analyses are conducted to weigh the costs and benefits of such redundancy techniques against increased resource usage and adverse effects on the overall system performance. Additional analyses are conducted as the complexity of these mechanisms increases, as could be the case for dynamic behaviors. Increased complexity generally reduces trustworthiness. When a resource cannot be continuously protected, it is critical to detect and repair any security breaches before the resource is once again used in a secure context.  Related Controls: CP-10, CP-12, SC-7, SC-8, SC-24, SI-13.   * + 1. security and privacy engineering principles | economic security   Implement the security design principle of economic security in organization- defined systems or system components.  Discussion: The principle of economic security states that security mechanisms are not costlier than the potential damage that could occur from a security breach. This is the security-relevant form of the cost-benefit analyses used in risk management. The cost assumptions of cost-benefit analysis prevent the system designer from incorporating security mechanisms of greater strength than necessary, where strength of mechanism is proportional to cost. The principle of economic security also requires analysis of the benefits of assurance relative to the cost of that assurance in terms of the effort expended to obtain relevant and credible evidence as well as the necessary analyses to assess and draw trustworthiness and risk conclusions from the evidence.  Related Controls: RA-3.   * + 1. security and privacy engineering principles | performance security   Implement the security design principle of performance security in organization-defined systems or system components.  Discussion: The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized. For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers adhere to the specified constraints that capability performance needs place on protection needs. The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection. The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat.  The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory is granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode. Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.  Related Controls: SC-12, SC-13, SI-2, SI-7.   * + 1. security and privacy engineering principles | human factored security   Implement the security design principle of human factored security in organization-defined systems or system components.  Discussion: The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions that affect such policy and its enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made. Particular attention is given to interfaces through which personnel responsible for system administration and operation configure and set up the security policies. Ideally, these personnel are able to understand the impact of their choices. Personnel with system administrative and operational responsibilities are able to configure systems before start-up and administer them during runtime with confidence that their intent is correctly mapped to the system’s mechanisms. Security services, functions, and mechanisms do not impede or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the strictness necessary for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable them, avoid them, or use them in ways inconsistent with the security requirements and protection needs that the mechanisms were designed to satisfy.  Related Controls: None.   * + 1. security and privacy engineering principles | acceptable security   Implement the security design principle of acceptable security in organization-defined systems or system components.  Discussion: The principle of acceptable security requires that the level of privacy and performance that the system provides is consistent with the users’ expectations. The perception of personal privacy may affect user behavior, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces or meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.  Related Controls: None.   * + 1. security and privacy engineering principles | repeatable and documented procedures   Implement the security design principle of repeatable and documented procedures in organization-defined systems or system components.  Discussion: The principle of repeatable and documented procedures states that the techniques and methods employed to construct a system component permit the same component to be completely and correctly reconstructed at a later time. Repeatable and documented procedures support the development of a component that is identical to the component created earlier, which may be in widespread use. In the case of other system artifacts (e.g., documentation and testing results), repeatability supports consistency and the ability to inspect the artifacts. Repeatable and documented procedures can be introduced at various stages within the system development life cycle and contribute to the ability to evaluate assurance claims for the system. Examples include systematic procedures for code development and review, procedures for the configuration management of development tools and system artifacts, and procedures for system delivery.  Related Controls: CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.   * + 1. security and privacy engineering principles | procedural rigor   Implement the security design principle of procedural rigor in organization- defined systems or system components.  Discussion: The principle of procedural rigor states that the rigor of a system life cycle process is commensurate with its intended trustworthiness. Procedural rigor defines the scope, depth, and detail of the system life cycle procedures. Rigorous system life cycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the life cycle process such that the introduction of unspecified functionality is prevented.  Second, rigorous procedures applied to systems security engineering activities that produce specifications and other system design documents contribute to the ability to understand the system as it has been built rather than trusting that the component, as implemented, is the authoritative (and potentially misleading) specification.  Finally, modifications to an existing system component are easier when there are detailed specifications that describe its current design instead of studying source code or schematics to try to understand how it works. Procedural rigor helps ensure that security functional and assurance requirements have been satisfied, and it contributes to a better-informed basis for the determination of trustworthiness and risk posture. Procedural rigor is commensurate with the degree of assurance desired for the system. If the required trustworthiness of the system is low, a high level of procedural rigor may add unnecessary cost, whereas when high trustworthiness is critical, the cost of high procedural rigor is merited.  Related Controls: None.   * + 1. security and privacy engineering principles | secure system modification   Implement the security design principle of secure system modification in organization-defined systems or system components.  Discussion: The principle of secure system modification states that system modification maintains system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform secure systems into systems that are not secure. The procedures for system modification ensure that if the system is to maintain its trustworthiness, the same rigor that was applied to its initial development is applied to any system changes. Because modifications can affect the ability of the system to maintain its secure state, a careful security analysis of the modification is needed prior to its implementation and deployment. This principle parallels the principle of secure evolvability.  Related Controls: CM-3, CM-4.   * + 1. security and privacy engineering principles | sufficient documentation   Implement the security design principle of sufficient documentation in organization-defined systems or system components.  Discussion: The principle of sufficient documentation states that organizational personnel with responsibilities to interact with the system are provided with adequate documentation and other information such that the personnel contribute to rather than detract from system security. Despite attempts to comply with principles such as human factored security and acceptable security, systems are inherently complex, and the design intent for the use of security mechanisms and the ramifications of the misuse or misconfiguration of security mechanisms are not always intuitively obvious. Uninformed and insufficiently trained users can introduce vulnerabilities due to errors of omission and commission. The availability of documentation and training can help to ensure a knowledgeable cadre of personnel, all of whom have a critical role in the achievement of principles such as continuous protection.  Documentation is written clearly and supported by training that provides security awareness and understanding of security-relevant responsibilities.  Related Controls: AT-2, AT-3, SA-5.   * + 1. security and privacy engineering principles | minimization   Implement the privacy principle of minimization using organization-defined processes.  Discussion: The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.  Related Controls: PE-8, PM-25, SC-42, SI-12. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SA-9-COV-1

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Establish the exact geographically location of all data if not stored within the Commonwealth. The Commonwealth will define the parameters and costs for data location options prior to making any contractual commitments; and 2. Confirm the exact geographically location of the sensitive data on at least a monthly basis and report the location to the appropriate regulatory authority at least every 90 days.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SA-9-COV-2

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   * 1. Establish a Data Escrow policy to address the data recovery process in case of system failure or facility issues and ensure all copies of data are returned to the Commonwealth at the end of contract; and   2. Establish a validated copy of any data elements classified as sensitive with respect to integrity or availability or are considered components in a system of record for the Commonwealth. The validated copy must be stored within a secured environment maintained by the Commonwealth.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SA-9-COV-3

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   * + - 1. Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis;       2. Perform at least a monthly review of activity logs related to the operation of the service. At a minimum, the activity review must include the access time and action of each individual using the system during the review period;       3. Receive reports from the vendor on vulnerability scans of the operating system and supporting software at least once every 90 days;       4. Ensure that the vendor conduct an independent vulnerability scan of the service at least once every 90 days and provide the results to Agency within 10 business days;       5. Submit a summary of all findings from the monthly activity log review once every 90 days to the appropriate regulatory authority;       6. Submit the vulnerability scan information within 30 days of receipt from the vendor to the appropriate regulatory authority; and       7. Submit the results from the Data Owning Agency vulnerability scan of the service within 30 days of scan completion.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# SC – SYSTEM AND COMMUNICATION PROTECTION

## SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Separate user functionality, including user interface services, from system management functionality.  Discussion: System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA- 8(13), SA-8(14), and SA-8(18).  Related Controls: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.  Control Enhancements:   1. separation of system and user functionality | disassociability   Store state information from applications and software separately.  Discussion: If a system is compromised, storing applications and software separately from state information about users’ interactions with an application may better protect individuals’ privacy.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-3 SECURITY FUNCTION ISOLATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Isolate security functions from nonsecurity functions.  Discussion: Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).  Related Controls: AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC- 32, SC-39, SI-16. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Prevent unauthorized and unintended information transfer via shared system resources.  Discussion: Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.  Related Controls: AC-3, AC-4, SA-8. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-5 DENIAL-OF-SERVICE PROTECTION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Protect against or limit the effects of the following types of denial-of-service events: resource exhaustion, amplification attack, and organization-defined types of denial-of-service events; and 2. Employ the following controls to achieve the denial-of-service objective: application firewall and additional organization-defined controls by type of denial-of-service events.   Discussion: Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.  Related Controls: CP-2, IR-4, SC-6, SC-7, SC-40.  Control Enhancements:   1. denial-of-service protection | restrict ability to attack other systems   Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: all denial-of-service attacks except for system testing purposes.  Discussion: Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial-of-service attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.  Related Controls: None.   1. denial-of-service protection | capacity, bandwidth, and redundancy   Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.  Discussion: Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.  Related Controls: None.   1. denial-of-service protection | detection and monitoring 2. Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: intrusion detection and application firewall; and 3. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: organization-defined system resources.   Discussion: Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles. Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.  Related Controls: CA-7, SI-4. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-6 RESOURCE AVAILABILITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Protect the availability of resources by allocating organization-defined resources by priority.  Discussion: Priority protection prevents lower-priority processes from delaying or interfering with the system that services higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources.  Related Controls: SC-5. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-7 BOUNDARY PROTECTION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; 2. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and 3. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.   Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. [SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).  Related Controls: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP- 8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.  Control Enhancements:   1. boundary protection | access points   Limit the number of external network connections to the system.  Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection [DHS TIC] initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.  Related Controls: None.  (5) boundary protection | deny by default -- allow by exception  Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.  Discussion: Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.  Related Controls: None.  (7) boundary protection | split tunneling for remote devices  Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using a Commonwealth Security and Risk Management approved solution.  Discussion: Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre- approved addresses, without user control.  Related Controls: None.  (8) boundary protection | route traffic to authenticated proxy servers  Route organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.  Discussion: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for “man-in-the-middle” attacks (depending on the implementation).  Related Controls: AC-3.  (9) boundary protection | restrict threatening outgoing communications traffic   1. Detect and deny outgoing communications traffic posing a threat to external systems; and 2. Audit the identity of internal users associated with denied communications.   Discussion: Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out within the system at managed interfaces. Extrusion detection includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code. Organizations have criteria to determine, update, and manage identified threats related to extrusion detection.  Related Controls: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.  (11) boundary protection | restrict incoming communications traffic  Only allows incoming communications from organization-defined authorized sources to be routed to organization-defined authorized destinations.  Discussion: General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs. Strong authentication of network addresses is not possible without the use of explicit security protocols, and thus, addresses can often be spoofed. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.  Related Controls: AC-3.  (12) boundary protection | host-based protection  Implement organization-defined host-based boundary protection mechanisms at the appropriate organization-defined information system component layer.  Discussion: Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.  Related Controls: None.  (13) boundary protection | isolation of security tools, mechanisms, and support components  Isolate organization-defined information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.  Discussion: Physically separate subnetworks with managed interfaces are useful in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques employed by organizations.  Related Controls: SC-2, SC-3.  (15) boundary protection | networked privileged accesses  Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.  Discussion: Privileged access provides greater accessibility to system functions, including security functions. Adversaries attempt to gain privileged access to systems through remote access to cause adverse mission or business impacts, such as by exfiltrating information or bringing down a critical system capability. Routing networked, privileged access requests through a dedicated, managed interface further restricts privileged access for increased access control and auditing.  Related Controls: AC-2, AC-3, AU-2, SI-4.  (18) boundary protection | fail secure  Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.  Discussion: Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.  Related Controls: CP-2, CP-12, SC-24.  (19) boundary protection | block communications from non-organizationally configured hosts  Block inbound and outbound communications traffic between organization- defined communication clients that are independently configured by end users and external service providers.  Discussion: Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.  Related Controls: None.  (29) boundary protection | separate subnets to isolate functions  Implement logically separate subnetworks to isolate the following critical system components and functions: organization-defined critical system components and functions.  Discussion: Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command and control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in the trustworthiness of critical system functions.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Protect the confidentiality andintegrity of transmitted information.  Discussion: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.  Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.  Related Controls: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC- 20, SC-23, SC-28.  Control Enhancements:   1. transmission confidentiality and integrity | cryptographic protection   Implement cryptographic mechanisms to preventunauthorized disclosure of information and detect changes to information during transmission.  Discussion: Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.  Related Controls: SC-12, SC-13. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-8-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:Require the use of data protection mechanisms for the transmission of allemail and attached data that is sensitive.   * + - 1. Require the use of encryption or digital signatures for the transmission of email and attached data that is sensitive relative to integrity; and       2. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-10 NETWORK DISCONNECT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Terminate the network connection associated with a communications session at the end of the session or after 15 minutes of inactivity.  Discussion: Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.  Related Controls: AC-17, SC-23. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: Commonwealth Security and Risk Management approved key management services, generation, distribution, storage, access, and destruction.  Discussion: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. [NIST CMVP] and [NIST CAVP] provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.  Related Controls: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC- 13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.  Control Enhancements:   1. cryptographic key establishment and management | availability   Maintain availability of information in the event of the loss of cryptographic keys by users.  Discussion: Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.  Related Controls: None.   1. cryptographic key establishment and management | symmetric keys   Produce, control, and distribute symmetric cryptographic keys using NIST FIPS 140-3 validated key management technology and processes.  Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and [SP 800-57-3] provide guidance on cryptographic key management.  Related Controls: None.   1. cryptographic key establishment and management | asymmetric keys   Produce, control, and distribute asymmetric cryptographic keys using certificates issued in accordance with organization-defined requirements.  Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and [SP 800-57-3] provide guidance on cryptographic key management.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-13 USE OF CRYPTOGRAPHY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Determine the cryptographic uses to protect sensitive data; and 2. Implement the following types of cryptography required for each specified cryptographic use: FIPS-validated cryptography for the uses prescribed in SC-13-a.   Discussion: Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation.  Generally applicable cryptographic standards include FIPS-validated cryptography and NSA- approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  Related Controls: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI- 7. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-13-COV

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data; 2. Document appropriate processes before implementing encryption. These processes must include the following components:    * 1. Instructions in the IT Security Agency’s Incident Response Plan on how to respond when encryption keys are compromised;      2. A secure key management system for the administration and distribution of encryption keys; and      3. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances; and 3. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data’s broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity.   Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: computer support that a user explicitly approves; and 2. Provide an explicit indication of use to users physically present at the devices.   Discussion: Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.  Related Controls: AC-21, SC-42.  Control Enhancements:   1. collaborative computing devices | physical or logical disconnect   Provide physical or logical disconnect of collaborative computing devices in a manner that supports ease of use.  Discussion: Failing to disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures. Disconnect from collaborative computing devices can be manual or automatic.  Related Controls: None.  (4) collaborative computing devices | explicitly indicate current participants  Provide an explicit indication of current participants in all online meetings and teleconferences.  Discussion: Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   * + - * 1. Issue public key certificates under an approved organization-defined certificate policy or obtain public key certificates from an approved service provider; and         2. Include only approved trust anchors in trust stores or certificate stores managed by the organization.   Discussion: Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.  Related Controls: AU-10, IA-5, SC-12. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and 2. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.   Discussion: Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.  Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.  Related Controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.  Control Enhancements:  (2) secure name / address resolution service (authoritative source) | data origin and integrity  Provide data origin and integrity protection artifacts for internal name/address resolution queries.  Discussion: None.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.  Discussion: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.  Related Controls: SC-20, SC-22. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.  Discussion: Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).  Related Controls: SC-2, SC-20, SC-21, SC-24. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-23 SESSION AUTHENTICITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Protect the authenticity of communications sessions.  Discussion: Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions.  Related Controls: AU-10, SC-8, SC-10, SC-11.  Control Enhancements:  (3) session authenticity | unique system-generated session identifiers  Generate a unique session identifier for each session with randomness and recognize only session identifiers that are system-generated.  Discussion: Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.  Related Controls: AC-10, SC-12, SC-13.  (5) session authenticity | allowed certificate authorities  Only allow the use of approved certificate authorities for verification of the establishment of protected sessions.  Discussion: Reliance on certificate authorities for the establishment of secure sessions includes the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.  Related Controls: SC-12, SC-13. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-28 PROTECTION OF INFORMATION AT REST

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Protect the confidentiality and integrity of the following information at rest: sensitive information.  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.  Related Controls: AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC- 8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.  Control Enhancements:   1. protection of information at rest | cryptographic protection   Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on any system or system components: sensitive information based on confidentiality or integrity.  Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.  Related Controls: AC-19, SC-12, SC-13. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-39 PROCESS ISOLATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Maintain a separate execution domain for each executing system process.  Discussion: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.  Related Controls: AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-42 SENSOR CAPABILITY AND DATA

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Prohibit the remote activation of environmental sensing capabilities on organizational systems or system components with the following exception: Agency Head approved policy, indicating business functions that cannot be accomplished without the use of the capability; and 2. Provide an explicit indication of sensor use to the user of the device.   Discussion: Sensor capability and data applies to types of systems or system components characterized as mobile devices, such as cellular telephones, smart phones, and tablets. Mobile devices often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include microphones, cameras, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the movements of an individual. Organizations may prohibit individuals from bringing cellular telephones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.  Related Controls: SC-15. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-43 USAGE RESTRICTIONS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Establish usage restrictions and implementation guidance for the following system components: as defined in SEC528; and 2. Authorize, monitor, and control the use of such components within the system.   Discussion: Usage restrictions apply to all system components including but not limited to mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.  Related Controls: AC-18, AC-19, CM-6, SC-7, SC-18. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-44 DETONATION CHAMBERS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Employ a detonation chamber capability within systems supporting incident response activities.  Discussion: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.  Related Controls: SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-45 SYSTEM TIME SYNCHRONIZATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Synchronize system clocks within and between systems and system components.  Discussion: Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities—such as access control and identification and authentication—depending on the nature of the mechanisms used to support the capabilities.  Related Controls: AC-3, AU-8, IA-2, IA-8.  Control Enhancements:   1. system time synchronization | synchronization with authoritative time source 2. Compare the internal system clocks at least every 1024 seconds with Commonwealth approved time servers; and 3. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 100 milliseconds.   Discussion: Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.  Related Controls: None.   1. system time synchronization | secondary authoritative time source 2. Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and 3. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.   Discussion: It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-46 CROSS DOMAIN POLICY ENFORCEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Implement a policy enforcement mechanism logically between the physical and/or network interfaces for the connecting security domains.  Discussion: For logical policy enforcement mechanisms, organizations avoid creating a logical path between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation afforded by the physical implementation of policy enforcement to preclude the presence of logical covert channels penetrating the security domain may be needed.  Related Controls: AC-4, SC-7. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-47 ALTERNATE COMMUNICATIONS PATHS

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Establish organization-defined alternate communications paths for system operations organizational command and control.  Discussion: An incident, whether adversarial- or nonadversarial-based, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. To compound the problem, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communications path incident, can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communications paths for command and control purposes, including designating alternative decision makers if primary decision makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization’s ability to continue to operate and take appropriate actions during an incident.  Related Controls: CP-2, CP-8. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SC-50 SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Implement software-enforced separation and policy enforcement mechanisms between organization-defined security domains.  Discussion: System owners may require additional strength of mechanism to ensure domain separation and policy enforcement for specific types of threats and environments of operation.  Related Controls: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# SI – SYSTEM AND INFORMATION INTEGRITY

## SI-2 FLAW REMEDIATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (4) flaw remediation | automated patch management tools  Employ automated patch management tools to facilitate flaw remediation to the following system components: organization-defined system components.  Discussion: Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.  Related Controls: None.  (5) flaw remediation | automatic software and firmware updates  Install security-relevant software and firmware updates automatically to system components.  Discussion: Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose.  Related Controls: None.  (6) flaw remediation | removal of previous versions of software and firmware  Remove previous versions of software and firmware components after updated versions have been installed.  Discussion: Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-3 MALICIOUS CODE PROTECTION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Implement signature or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; 2. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; 3. Configures malicious code protection mechanisms to: 4. Perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources at endpoint, network entry, and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and 5. Block malicious code and send alert to administrator and Information Security Officer in response to malicious code detection; and 6. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.   Discussion: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.  Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.  In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.  Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC- 28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-4 SYSTEM MONITORING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Monitor the system to detect: 2. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: organization-defined monitoring objectives; and 3. Unauthorized local, network, and remote connections; 4. Identify unauthorized use of the system through the following techniques and methods: organization-defined techniques and methods; 5. [Withdrawn: Not applicable to COV.]; 6. Analyze detected events and anomalies; 7. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; 8. Obtain legal opinion regarding system monitoring activities; and 9. Provide organization-defined system monitoring information to information security personnel as needed.   Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.  Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU- 13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.  Control Enhancements:   1. system monitoring | system-wide intrusion detection system   Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system.  Discussion: Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.  Related Controls: None.   1. system monitoring | automated tools and mechanisms for real-time analysis   Employ automated tools and mechanisms to support near real-time analysis of events.  Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.  Related Controls: PM-23, PM-25.  (4) system monitoring | inbound and outbound communications traffic   * + - * 1. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;         2. Monitor inbound and outbound communications traffic in real time for organization-defined unusual or unauthorized activities or conditions.   Discussion: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.  Related Controls: None.  (5) system monitoring | system-generated alerts  Alert information security personnel when the following system-generated indicators of compromise or potential compromise occur: organization-defined compromise indicators.  Discussion: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.  Related Controls: AU-4, AU-5, PE-6.  (11) system monitoring | analyze communications traffic anomalies  Analyze outbound communications traffic at the external interfaces to the system and selected organization-defined interior points within the system to discover anomalies.  Discussion: Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.  Related Controls: None.  (13) system monitoring | analyze traffic and event patterns   * 1. Analyze communications traffic and event patterns for the system;   2. Develop profiles representing common traffic and event patterns; and   3. Use the traffic and event profiles in tuning system-monitoring devices.   Discussion: Identifying and understanding common communications traffic and event patterns help organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.  Related Controls: None.  (14) system monitoring | wireless intrusion detection  Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.  Discussion: Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.  Related Controls: AC-18, IA-3.  (15) system monitoring | wireless to wireline communications  Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.  Discussion: Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given the greater facility of unauthorized network access via wireless access points compared to unauthorized wired network access from within the physical boundaries of the system, additional monitoring of transitioning traffic between wireless and wired networks may be necessary to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps to ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.  Related Controls: AC-18.  (16) system monitoring | correlate monitoring information  Correlate information from monitoring tools and mechanisms employed throughout the system.  Discussion: Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation—including malicious code protection software, host monitoring, and network monitoring—can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).  Related Controls: AU-6.  (22) system monitoring | unauthorized network services   1. Detect network services that have not been authorized or approved by information security personnel; and 2. Alert information security personnel when detected.   Discussion: Unauthorized or unapproved network services include services in service- oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.  Related Controls: CM-7.  (24) system monitoring | indicators of compromise  Discover, collect, and distribute to information security personnel, indicators of compromise provided by Commonwealth Security and Risk Management approved sources.  Discussion: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffic include Universal Resource Locator or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Threat indicators, signatures, tactics, techniques, procedures, and other indicators of compromise may be available via government and non-government cooperatives, including the Forum of Incident Response and Security Teams, the United States Computer Emergency Readiness Team, the Defense Industrial Base Cybersecurity Information Sharing Program, and the CERT Coordination Center.  Related Controls: AC-18. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Verify the correct operation of organization-defined security and privacy functions; 2. Perform this verification of the functions specified in SI-6a at organization-defined system transitional states, upon command by user with appropriate privilege, or at least once every 90 days; 3. Alert organization-defined personnel to failed security and privacy verification tests; and 4. Shut the system down when anomalies are discovered.   Discussion: Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.  Related Controls: CA-7, CM-4, CM-6, SI-7.  Control Enhancements:  (2) security and privacy function verification | automation support for distributed testing  Implement automated mechanisms to support the management of distributed security and privacy function testing.  Discussion: The use of automated mechanisms to support the management of distributed function testing helps to ensure the integrity, timeliness, completeness, and efficacy of such testing.  Related Controls: SI-2. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:  Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: organization-defined software, firmware, and information.  Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify the Information Security Officer.  Discussion: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.  Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.  Control Enhancements:   1. software, firmware, and information integrity | integrity checks   Perform an integrity check of organization-defined software, firmware, and information at startup; at organization-defined transitional states or security-relevant events, and at least once every 7 days.  Discussion: Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.  Related Controls: None.   1. software, firmware, and information integrity | automated notifications of integrity violations   Employ automated tools that provide notification to the Information Security Officer upon discovering discrepancies during integrity verification.  Discussion: The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.  Related Controls: None.  (5) software, firmware, and information integrity | automated response to integrity violations  Automatically implement organization-defined controls when integrity violations are discovered.  Discussion: Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.  Related Controls: None.  (6) software, firmware, and information integrity | cryptographic protection  Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.  Discussion: Cryptographic mechanisms used to protect integrity include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.  Related Controls: SC-12, SC-13.  (8) software, firmware, and information integrity | auditing capability for significant events  Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: generates an audit record and alert the Information Security Officer.  Discussion: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.  Related Controls: AU-2, AU-6, AU-12.  (9) software, firmware, and information integrity | verify boot process  Verify the integrity of the boot process of the following system components: organization-defined system components.  Discussion: Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.  Related Controls: SI-6.  (10) software, firmware, and information integrity | protection of boot firmware  Implement the following mechanisms to protect the integrity of boot firmware in organization-defined system components: organization-defined mechanisms.  Discussion: Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.  Related Controls: SI-6.  (12) software, firmware, and information integrity | integrity verification  Require that the integrity of the following user-installed software be verified prior to execution: organization-defined user-installed software.  Discussion: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or programs that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity, including the availability of trustworthy checksums from software developers and vendors.  Related Controls: CM-11.  (15) software, firmware, and information integrity | code authentication  Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: organization-defined software or firmware components.  Discussion: Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.  Related Controls: CM-5, SC-12, SC-13.  (17) software, firmware, and information integrity | runtime application self-protection  Implement organization-defined controls for application self-protection at runtime.  Discussion: Runtime application self-protection employs runtime instrumentation to detect and block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections such as guards and firewalls which can only detect and block attacks by using network information without contextual awareness. Runtime application self-protection technology can reduce the susceptibility of software to attacks by monitoring its inputs and blocking those inputs that could allow attacks. It can also help protect the runtime environment from unwanted changes and tampering. When a threat is detected, runtime application self-protection technology can prevent exploitation and take other actions (e.g., sending a warning message to the user, terminating the user's session, terminating the application, or sending an alert to organizational personnel). Runtime application self-protection solutions can be deployed in either a monitor or protection mode.  Related Controls: SI-16. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-8 SPAM PROTECTION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control Enhancements:  (2) spam protection | automatic updates  Automatically update spam protection mechanisms at least on a daily basis.  Discussion: Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.  Related Controls: None.  (3) spam protection | continuous learning capability  Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.  Discussion: Learning mechanisms include Bayesian filters that respond to user inputs that identify specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.  Related Controls: None. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-10 INFORMATION INPUT VALIDATION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Check the validity of the following information inputs: organization-defined information inputs to the system.  Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of “387,” “abc,” or “%K%” are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker- supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.  Related Controls: None.  Control Enhancements:  (3) information input validation | predictable behavior  Verify that the system behaves in a predictable and documented manner when invalid inputs are received.  Discussion: A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. Verification of system predictability helps ensure that the system behaves as expected when invalid inputs are received. This occurs by specifying system responses that allow the system to transition to known states without adverse, unintended side effects. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).  Related Controls: None.  (6) information input validation | injection prevention  Prevent untrusted data injections.  Discussion: Untrusted data injections may be prevented using a parameterized interface or output escaping (output encoding). Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter’s parser whether data is trusted. Prevention of untrusted data injections are with respect to the information inputs defined by the organization in the base control (SI-10).  Related Controls: AC-3, AC-6. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-11 ERROR HANDLING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control:   1. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and 2. Reveal error messages only to the Information Security Officer and appropriate organization-defined personnel.   Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.  Related Controls: AU-2, AU-3, SC-31, SI-2, SI-15. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-16 MEMORY PROTECTION

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Implement the following controls to protect the system memory from unauthorized code execution: malicious code protection and other organization-defined controls.  Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.  Related Controls: AC-25, SC-3, SI-7. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

## SI-20 TAINTING

|  |  |
| --- | --- |
| **CONTROL REQUIREMENT** | Control: Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: organization-defined systems or system components.  Discussion: Many cyber-attacks target organizational information, or information that the organization holds on behalf of other entities (e.g., personally identifiable information), and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system that is in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any packets it includes potentially contain malicious code, and that the unauthorized entity may have potentially obtained a copy of the database. Another tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open-source analysis. Finally, an active tainting approach can include embedding software in the data that is able to “call home,” thereby alerting the organization to its “capture,” and possibly its location, and the path by which it was exfiltrated or removed.  Related Controls: AU-13. |
| **IMPLEMENTATION STATUS:**  Implemented  Not Implemented  Partially Implemented  Inherited  Not Applicable | |
| In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.** |  |

# POAM/Remediation Plan Template

When a control is not implemented, it must be tracked as a finding and have an associated plan of action and milestone documented. Please use the template located at the following URL.

[Risk-Treatment-Plan-Template-2021.xlsm (live.com)](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.vita.virginia.gov%2Fmedia%2Fvitavirginiagov%2Fcommonwealth-security%2Fdocs%2FRisk-Treatment-Plan-Template-2021.xlsm&wdOrigin=BROWSELINK)

[Attach the document as an appendix to the SSP or insert the file object in this section. Submit updates quarterly to [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)]