[AGENCY]

 [SYSTEM]

Security Plan

Non-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](#_Toc156907137)

[CONTENTS 1](#_Toc156907138)

[EXECUTIVE SUMMARY 2](#_Toc156907139)

[SYSTEM INVENTORY & DEFINITION 2](#_Toc156907140)

[DATA SET CLASSIFICATION INVENTORY 2](#_Toc156907141)

[BUSINESS PROCESSES 2](#_Toc156907142)

[SYSTEM BOUNDARY DIAGRAM 2](#_Toc156907143)

[INFORMATION FLOW DIAGRAM 3](#_Toc156907144)

[CSRM RESOURCES 4](#_Toc156907145)

[ITRM-SEC530 CONTROLS 4](#_Toc156907146)

[AC – ACCESS CONTROL 4](#_Toc156907147)

[AU - AUDIT AND ACCOUNTABILITY 13](#_Toc156907148)

[CA - SECURITY ASSESSMENT AND AUTHORIZATION 17](#_Toc156907149)

[CM – CONFIGURATION MANAGEMENT 18](#_Toc156907150)

[IA – IDENTIFICATION AND AUTHENTICATION 20](#_Toc156907151)

[IR – INCIDENT RESPONSE 27](#_Toc156907152)

[PE – PHYSICAL AND ENVIRONMENTAL PROTECTION 28](#_Toc156907153)

[PL – PLANNNING 30](#_Toc156907154)

[RA – RISK ASSESSMENT 30](#_Toc156907155)

[SA – SYSTEM AND SERVICES ACQUISITION 31](#_Toc156907156)

[SC – SYSTEM AND COMMUNICATION PROTECTION 36](#_Toc156907157)

[SI – SYSTEM AND INFORMATION INTEGRITY 54](#_Toc156907158)

[POAM/Remediation Plan Template 61](#_Toc156907159)

# 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

[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-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. |
| **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. |
| **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-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. |
| **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. |
| **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. |
| **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.** |  |

# 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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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-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. |
| **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-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. |
| **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. |
| **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. |
| **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. |
| **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.** |  |

# 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-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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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. |
| **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-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. |
| **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. |
| **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. |
| **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. |
| **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]