g. Changing/refreshing user-account authenticators at least every 90-days;

   a. Changing/refreshing administrative authenticators at least every 42-days.

   b. Changing/refreshing sensitive system authenticators at least every 42-days.

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Withdrawn: Not applicable to COV

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security 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 within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Control Enhancements for Sensitive Systems:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

(a) Enforces minimum password complexity of

1. At least eight characters in length; and
2. Utilize at least three of the following four;
   a. Special characters,
   b. Alphabetical characters,
   c. Numerical characters,
   d. Combination of upper case and lower case letters,

(b) [Withdrawn: Not applicable to COV]

(c) Stores and transmits only encrypted representations of passwords;

(d) Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum;

(e) Prohibits password reuse for 24 generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does *not* apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. Related control: IA-6.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Supplemental Guidance: For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that

representation is perhaps an encrypted version of something else (e.g., a password).

(8) [Withdrawn: Not applicable to COV]

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) [Withdrawn: Not applicable to COV]

(12) [Withdrawn: Not applicable to COV]

(13) [Withdrawn: Not applicable to COV]

(14) [Withdrawn: Not applicable to COV**]**

(15) [Withdrawn: Not applicable to COV]

IA-5-COV-1

Control: The organization manages information system authenticators for users and devices by:

a. requiring passwords with a minimum of four characters on smart phones or PDAs accessing or containing COV data.

b. requiring that forgotten initial passwords be replaced rather than reissued.

c. requiring passwords to be set on device management user interfaces for all network-connected devices.

d. documenting and storing hardware passwords securely.

e. requiring passwords not be cached or stored on the device.

f. requiring the suppression of passwords on the display as the password is entered into the device.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IA-5-COV-2

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:

- determine the appropriate validity period of the password, commensurate with sensitivity and risk.
- determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk.
- 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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18.

Control Enhancements for Sensitive Systems: None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Supplemental Guidance: [Withdrawn: Not applicable to COV]

Control Enhancements for Sensitive Systems: None.

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

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Control Enhancements for Sensitive Systems: [Withdrawn: Not applicable to COV]

Supplemental Guidance: [Withdrawn: Not applicable to COV]

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV]

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV]

IA-11 RE-AUTHENTICATION

[Withdrawn: Not applicable to COV]

8.8. FAMILY: INCIDENT RESPONSE CLASS: OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

   1. Incident response policy on an annual basis or more frequently if required to address an environmental change; and

   2. Incident response procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the IR family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

IR-1-COV

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:

    a. Designate an individual responsible for the agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.

    b. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

    c. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.

    d. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.

2. 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:

    a. Designate individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.

    b. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.

    c. Prohibit the installation or use of unauthorized monitoring devices.

    d. 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.

3. 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:

    a. Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.

    b. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.

    c. Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks and zero-day exploits.

    d. 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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within 30-days of assuming an incident response role or responsibility;

b. When required by information system changes; and

c. On an annual basis or more frequently if required to address an environmental change thereafter.

Supplemental Guidance: Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.

Control Enhancements for Sensitive Systems:

(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) [Withdrawn: Not applicable to COV]

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: The organization tests the incident response capability for the information system on an annual basis or more frequently if required to address an environmental change using organization-defined tests to determine the incident response effectiveness and documents the results.

Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

The organization coordinates incident response testing with organizational elements responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) INCIDENT HANDLING | INFORMATION CORRELATION

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

(5) [Withdrawn: Not applicable to COV]

(6) INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES

The organization implements incident handling capability for insider threats.

Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and

the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

(7) INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION

The organization coordinates incident handling capability for insider threats across all sensitive components or elements of the organization.

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies.

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

The organization coordinates with the appropriate external organizations to correlate and share incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multitiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.

(9) Withdrawn: Not applicable to COV

(10) Withdrawn: Not applicable to COV

IR-4-COV-1

Control:

1. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

2. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-4-COV-2

Control:

Where electronic records or IT infrastructure are involved, the following are requirements that each agency shall adhere to. Based on their business requirements, some agencies may need to comply with regulatory and/or industry requirements that are more restrictive.

Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended:

Each agency shall:

1. Identify and document all agency systems, processes, and logical or physical data storage locations (whether held by the agency or a third party) that contain personal information or medical information.

   a. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

      1) Social security number;

      2) Driver's license number or state identification card number issued in lieu of a driver's license number; or

      3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;

   b. Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

      1) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

      2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

2. "Redact" for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

   a. Five digits of a social security number; or

   b. The last four digits of a driver's license number, state identification card number, or account number.

3. "Redact" for medical information means alteration or truncation of data such that no information regarding the following are accessible as part of the medical information:

a. An individual's medical history; or

b. Mental or physical condition; or

c. Medical treatment or diagnosis; or

d. No more than four digits of a health insurance policy number, subscriber number; or

e. Other unique identifier.

4. Include provisions in any third party contracts requiring that the third party and third party subcontractors:

   a. Provide immediate notification to the agency of suspected breaches; and

   b. Allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.

5. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical information by any mechanism, including, but not limited to:

   a. Theft or loss of digital media including laptops, desktops, tablets, CDs, DVDs, tapes, USB drives, SD cards, etc.;

   b. Theft or loss of physical hardcopy; and

   c. Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).

6. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

7. If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.

8. The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #9, below.

9. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules. Agencies shall notify the CISO when notification of affected individuals has been completed.

10. Provide notification that consists of:

    a. A general description of what occurred and when;

b. The type of Personal Information that was involved;

c. What actions have been taken to protect the individual's Personal Information from further unauthorized access;

d. A telephone number that the person may call for further information and assistance, if one exists; and

e. What actions the agency recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).

11. Provide this notification by one or more of the following methodologies, listed in order of preference:

a. Written notice to the last known postal address in the records of the individual or entity;

b. Telephone Notice;

c. Electronic notice; or

d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:

1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

2) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

3) Notice to major statewide media.

12. Hold the release of notification immediately following verification of unauthorized data disclosure only if law enforcement is notified and the law enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no long impede the investigation or jeopardize national or homeland security.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

IR-5-COV

Control: Monitor IT system event logs in real time, correlate information with other automated tools, identifying suspicious activities, and provide alert notifications.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-6 INCIDENT REPORTING

Control: The organization:

k. Requires personnel to report suspected security incidents to the organizational incident response capability within within 24 hours from when the agency discovered or should have discovered their occurrence; and

l. Reports security incident information to designated authorities.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for Commonwealth agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current Commonwealth policy requires that all Commonwealth agencies (unless specifically exempted from such requirements) report security incidents to the Commonwealth Security and Risk Management team within specified time frames designated in the Code of Virginia. Related controls: IR-4, IR-5, IR-8.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS

The organization reports information system vulnerabilities associated with reported security incidents to the appropriate organizational officials.

(3) [Withdrawn: Not applicable to COV]

IR-6-COV

Control: Organization shall:

1. Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.

2. Establish a process for reporting IT security incidents to the CISO. All COV agencies are encouraged to report security incidents; however, Executive Branch agencies must establish a reporting process for IT security incidents in accordance with §2.2-603(F) of the Code of Virginia so as to report "to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence,"… "all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities."

3. Report information security incidents only through channels that have not been compromised.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS

The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

a. Develops an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by designated officials within the organization.

b. Distributes copies of the incident response plan to the organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements;

c. Reviews the incident response plan on an annual basis or more frequently if required to address an environmental change;

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to the organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements; and

f. Protects the incident response plan from unauthorized disclosure and modification.

Supplemental Guidance: It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

Control Enhancements for Sensitive Systems: None.

IR-9 INFORMATION SPILLAGE RESPONSE

[Withdrawn: Not applicable to COV]

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

[Withdrawn: Not applicable to COV]

8.9. FAMILY: MAINTENANCE CLASS: OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization personnel or roles:

   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

   1. System maintenance policy on an annual basis or more frequently if required to address an environmental change; and

   2. System maintenance procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the MA family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that a designated organization official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes the appropriate maintenance-related information in organizational maintenance records.

Supplemental Guidance: This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

Control Enhancements for Sensitive Systems:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2].

(2) [Withdrawn: Not applicable to COV]

Supplemental Guidance: Related controls: CA-7, MA-3.

MA-3 MAINTENANCE TOOLS

[Withdrawn: Not applicable to COV]

MA-4 NON-LOCAL MAINTENANCE

[Withdrawn: Not applicable to COV]

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

a. [Withdrawn: Not applicable to COV]

b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Supplemental Guidance: [Withdrawn: Not applicable to COV]

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

MA-6 TIMELY MAINTENANCE

[Withdrawn: Not applicable to COV]

8.10. FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization personnel or roles:

1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:

1. Media protection policy on an annual basis or more frequently if required to address an environmental change; and

2. Media protection procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the MP family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

MP-1-COV

Control: The organization shall document and implement Data Storage Media protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored sensitive data as the responsibility of Data Owner.

2. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head accepting all residual risks. the exception shall include following elements:

   a. The business or technical justification;

   b. The scope, including quantification and duration (not to exceed one year) ;

   c. A description of all associated risks;

   d. Identification of controls to mitigate the risks, one of which must be encryption; and

   e. Identification of any residual risks.

3. Prohibit the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.

4. Prohibit the connection of any non-COV owned or leased data storage media or device to a COV-owned or leased resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.

5. Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the Agency Head.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

MP-2 MEDIA ACCESS

Control: The organization restricts access to digital and non-digital media to only authorized individuals using organization-defined security measures.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-

digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Control Enhancements for Sensitive Systems:

(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

[Withdrawn: Incorporated into MP-4 (2)].

(2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28 (1)].

MP-3 MEDIA MARKING

[Withdrawn: Not applicable to COV]

MP-4 MEDIA STORAGE

Control: The organization:

a. Physically controls and securely stores digital and non-digital media within organization-defined controlled areas using organization-defined security measures; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

Control Enhancements for Sensitive Systems:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28 (1)].

(2) [Withdrawn: Not applicable to COV]

MP-4-COV

Control: Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is sensitive as related to confidentiality. Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

MP-5 MEDIA TRANSPORT

Control: The organization:

a. Protects and controls digital and non-digital media during transport outside of controlled areas using organization-defined security measures;

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the

media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Control Enhancements for Sensitive Systems:

(1) MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS

[Withdrawn: Incorporated into MP-5].

(2) MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES

[Withdrawn: Incorporated into MP-5].

(3) MEDIA TRANSPORT | CUSTODIANS

The organization employs an identified custodian during transport of information system media outside of controlled areas.

Supplemental Guidance: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Supplemental Guidance: This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2.

MP-6 MEDIA SANITIZATION

Control: The organization:

a. Sanitizes information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that

destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. Related controls: MA-2, MA-4, RA-3, SC-4.

Control Enhancements for Sensitive Systems:

(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental Guidance:

[Withdrawn: Not applicable to COV]

(2) MEDIA SANITIZATION | EQUIPMENT TESTING

The organization tests sanitization equipment and procedures on an annual basis or more frequently if required to address an environmental change to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other Commonwealth agencies or external service providers).

(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: prior to connecting such a device to the information system.

Supplemental Guidance: Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

(4) MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6].

(5) MEDIA SANITIZATION | CLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6].

(6) MEDIA SANITIZATION | MEDIA DESTRUCTION

[Withdrawn: Incorporated into MP-6].

(7) [Withdrawn: Not applicable to COV]

(8) [Withdrawn: Not applicable to COV]

MP-6-COV

Control: Remove data from IT assets prior to disposal 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).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

MP-7 MEDIA USE

Control: The organization restricts the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security safeguards.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4.

Control Enhancements for Sensitive Systems:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.

(2) MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA

The organization prohibits the use of sanitization-resistant media in organizational information systems.

Supplemental Guidance: Sanitation-resistance applies to the capability to purge information from media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitation-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media. Related control: MP-6.

MP-8 MEDIA DOWNGRADING

[Withdrawn: Not applicable to COV]

8.11. FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. Reviews and updates the current:

   1. Physical and environmental protection policy on an annual basis or more frequently if required to address an environmental change; and

   2. Physical and environmental protection procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the PE family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

PE-1-COV

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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals on an annual basis or more frequently if required to address an environmental change; and

d. Removes individuals from the facility access list when access is no longer required.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with Commonwealth standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3.

Control Enhancements for Sensitive Systems:

(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE

The organization authorizes physical access to the facility where the information system resides based on position or role.

Supplemental Guidance: Related controls: AC-2, AC-3, AC-6.

(2) [Withdrawn: Not applicable to COV]

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

The organization restricts unescorted access to the facility where the information system resides to personnel with security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;

PE-2-COV

Control: The organization:

a. Temporarily disables physical 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.

b. Disables physical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

Control Enhancements for Sensitive Systems: None

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations for all physical access points including organization-defined entry/exit points to the facility where the information system resides by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using organization-defined physical access control systems/devices; guards;
b. Maintains physical access audit logs for all organization-defined entry/exit points;
c. Provides organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity for organization-defined circumstances requiring visitor escorts and monitoring;
e. Secures keys, combinations, and other physical access devices;
f. Inventories organization-defined physical access devices every on an annual basis or more frequently if required to address an environmental change; and
g. Withdrawn: Not applicable to COV

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the

types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Control Enhancements for Sensitive Systems:

(1) PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at organization-defined physical spaces containing one or more components of the information system.

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components applicable Commonwealth laws, Executive Orders, (e.g., server rooms, media storage areas, data and communications centers). Related control: PS-2.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

(6) [Withdrawn: Not applicable to COV]

PE-3-COV

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).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

[Withdrawn: Not applicable to COV]

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing

access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b. Reviews physical access logs at least once every 60-days and upon occurrence of organization-defined events or potential indications of events; and

c. Coordinates results of reviews and investigations with the organizational incident response capability.

Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

Control Enhancements for Sensitive Systems:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

The organization monitors physical intrusion alarms and surveillance equipment.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3].

PE-8 ACCESS RECORDS

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides for a minimum period of one year; and

b. Reviews visitor access records at least once every 60-days.

Supplemental Guidance: Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS
[Withdrawn: Incorporated into PE-2].

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

PE-10 EMERGENCY SHUTOFF

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

b. Places emergency shutoff switches or devices in organization-defined location by information system or system component to facilitate safe and easy access for personnel; and

c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related control: PE-15.

Control Enhancements for Sensitive Systems:

(1) EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION
[Withdrawn: Incorporated into PE-10].

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system;] in the event of a primary power source loss.

Supplemental Guidance: Related controls: AT-3, CP-2, CP-7.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

PE-12 EMERGENCY LIGHTING

[Withdrawn: Not applicable to COV]

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements for Sensitive Systems:

(1) FIRE PROTECTION | DETECTION DEVICES / SYSTEMS

The organization employs fire detection devices/systems for the information system that activate automatically and notify the appropriate organization-defined personnel or roles and organization-defined emergency responders in the event of a fire.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(2) FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the appropriate organization-defined personnel.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

(4) [Withdrawn: Not applicable to COV]

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels; and

b. Monitors temperature and humidity levels on a daily basis.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3.

Control Enhancements for Sensitive Systems:

(1) TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS

The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

(2) TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

PE-15 WATER DAMAGE PROTECTION

[Withdrawn: Not applicable to COV]

PE-16 DELIVERY AND REMOVAL

[Withdrawn: Not applicable to COV]

PE-17 ALTERNATE WORK SITE

[Withdrawn: Not applicable to COV]

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.

Control Enhancements for Sensitive Systems:

(1) LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Supplemental Guidance: Related control: PM-8.

PE-19 INFORMATION LEAKAGE

[Withdrawn: Not applicable to COV]

PE-20 ASSET MONITORING AND TRACKING

[Withdrawn: Not applicable to COV]

8.12. FAMILY: PLANNING CLASS: MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:

   1. Security planning policy on an annual basis or more frequently if required to address an environmental change; and

   2. Security planning procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the PL family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:
    1. Is consistent with the organization's enterprise architecture;
    2. Explicitly defines the authorization boundary for the system;
    3. Describes the operational context of the information system in terms of missions and business processes;
    4. Provides the security categorization of the information system including supporting rationale;
    5. Describes the operational environment for the information system and relationships with or connections to other information systems;
    6. Provides an overview of the security requirements for the system;
    7. Identifies any relevant overlays, if applicable;
    8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
    9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distributes copies of the security plan and communicates subsequent changes to the plan to the appropriate organization-defined personnel;
c. Reviews the security plan for the information system on an annual basis or more frequently if required to address an environmental change;
d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e. Protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and Control Enhancements for Sensitive Systems. Security plans also describe, at a high level, how the security controls and Control Enhancements for Sensitive Systems meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly

or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Control Enhancements for Sensitive Systems:

(1) *SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*

[Withdrawn: Incorporated into PL-7].

(2) SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE

[Withdrawn: Incorporated into PL-8].

(3) SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

The organization plans and coordinates security-related activities affecting the information system with the appropriate organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.

PL-2-COV

Control: The organization shall:

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:

   a. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls;

   b. How these controls provide adequate mitigation of risks to which the IT system is subject.

2. Submit the IT System Security Plan to the Agency Head or designated ISO for approval.

3. 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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control: The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

c. Reviews and updates the rules of behavior on an annual basis or more frequently if required to address an environmental change; and

d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

Supplemental Guidance: This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from Commonwealth information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

Control Enhancements for Sensitive Systems:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining

and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.

PL-4-COV

Control: Organization shall:

1. Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management (DHRM) Policy 1.75 – Use of Internet and Electronic Communication Systems. Each Executive branch agency shall supplement the policy as necessary to address specific agency needs.

2. Prohibit users from:

   a. Installing or using proprietary encryption hardware/software on Commonwealth systems;

   b. Tampering with security controls configured on COV workstations;

   c. Installing personal software on a Commonwealth system;

   d. Adding hardware to, removing hardware from, or modifying hardware on a COV system; and

   e. Connecting non-COV-owned devices to a COV IT system or network, such as personal computers, laptops, or hand held devices, except in accordance with the current version of the Use of non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511).

3. Prohibit the storage, use or transmission of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.

4. The organization should consult with legal counsel when considering adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such.

   Supplemental guidance: The following text is an example of an email disclaimer for consideration when meeting with your agency's legal counsel:

   The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into Appendix J, AR-2].

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2].

PL-7 SECURITY CONCEPT OF OPERATIONS

[Withdrawn: Not applicable to COV]

PL-8 INFORMATION SECURITY ARCHITECTURE

[Withdrawn: Not applicable to COV]

PL-9 CENTRAL MANAGEMENT

[Withdrawn: Not applicable to COV]

8.13. FAMILY: PERSONNEL SECURITY CLASS: OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:

   1. Personnel security policy on an annual basis or more frequently if required to address an environmental change; and

   2. Personnel security procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control

Enhancements for Sensitive Systems in the PS family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

PS-2 POSITION RISK DESIGNATION

[Withdrawn: Not applicable to COV]

PS-3 PERSONNEL SCREENING

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. [Withdrawn: Not applicable to COV]

Control Enhancements for Sensitive Systems: [Withdrawn: Not applicable to COV]
Supplemental Guidance: Reference Code of Virginia § 2.2-1201.1 and Department of Human Resource Management (DHRM Policy).

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:

a. Disables information system access within 24-hours of employment termination;

b. Terminates/revokes any authenticators/credentials associated with the individual;

c. [Withdrawn: Not applicable to COV]

d. Retrieves all security-related organizational information system-related property;

e. Retains access to organizational information and information systems formerly controlled by terminated individual; and

f. Notifies the appropriate organization-defined personnel within an organizationally defined time-period.

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with

security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

PS-5 PERSONNEL TRANSFER

Control: The organization:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiates the transfer or reassignment actions within 24-hours of the formal transfer action;

c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notifies the appropriate organization-defined personnel within organization defined time period.

Supplemental Guidance: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4.

Control Enhancements for Sensitive Systems: None.

PS-6 ACCESS AGREEMENTS

Control: The organization:

a. Develops and documents access agreements for organizational information systems;

b. Reviews and updates the access agreements on an annual based or more frequently if required to address an environmental change; and

c. Ensures that individuals requiring access to organizational information and information systems:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Control Enhancements for Sensitive Systems:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL *PROTECTION*
[Withdrawn: Incorporated into PS-3].

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;

c. Documents personnel security requirements;

d. Requires third-party providers to notify the appropriate organization-defined personnel of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization defined time period.; and

e. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Control Enhancements for Sensitive Systems: None.

PS-8 PERSONNEL SANCTIONS

Control: The organization:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

b. [Withdrawn: Not applicable to COV]

Control Enhancements for Sensitive Systems: None.

Supplemental Guidance: Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

8.14. FAMILY: RISK ASSESSMENT CLASS: MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

   1. Risk assessment policy on an annual basis or more frequently if required to address an environmental change; and

   2. Risk assessment procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the RA family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are compromised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements for Sensitive Systems: None.

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in a Risk Assessment Report;

c. Reviews risk assessment results on an annual basis or more frequently if required to address an environmental change;

d. Disseminates risk assessment results to the appropriate organization-defined personnel; and

e. Updates the risk assessment on an annual basis or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities Organizational assessments of risk also address public access to Commonwealth information systems.

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk

Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.
Control Enhancements for Sensitive Systems: None.

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3]

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   1. Enumerating platforms, software flaws, and improper configurations;

   2. Formatting checklists and test procedures; and

   3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities within 90-days in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with the appropriate organization-defined personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control

mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

Control Enhancements for Sensitive Systems:

(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.

(2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

The organization updates the information system vulnerabilities scanned at least once every 90-days, prior to a new scan, or when new vulnerabilities are identified and reported.

Supplemental Guidance: Related controls: SI-3, SI-5.

(3) VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE

The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

(4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION

The organization determines what information about the information system is discoverable by adversaries and subsequently takes the appropriate corrective actions.

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries. Related control: AU-13.

(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

The information system implements privileged access authorization to information system components for selected vulnerability scanning activities.

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

(6) [Withdrawn: Not applicable to COV]

(7) VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS

[Withdrawn: Incorporated into CM-8].

(8) VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

Supplemental Guidance: Related control: AU-6.

(9) VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES

[Withdrawn: Incorporated into CA-8].

(10) VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

RA-5-COV

Control: The organization:

Scans for vulnerabilities in the sensitive information systems and hosted applications at least once every 90-days and when new vulnerabilities potentially affecting the system/applications are identified and reported;

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

[Withdrawn: Not applicable to COV]

8.15. FAMILY: SYSTEM AND SERVICES ACQUISITION CLASS: MANAGEMENT

SYSTEM AND SERVICES ACQUISITION CONTROLS

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, this publication provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with such development whether the development is conducted by internal organizational personnel or by external developers through the contracting/acquisition process. Affected controls include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

   1. System and services acquisition policy on an annual basis or more frequently if required to address an environmental change; and

   2. System and services acquisition procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the SA family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information

systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Withdrawn: Not applicable to COV

Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.

Control Enhancements for Sensitive Systems: None.

SA-3 LIFE CYCLE SUPPORT

Control: The organization:

a. Manages the information system using system development life cycle methodology that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and

d. Integrates the organizational information security risk management process into system development life cycle activities.

Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of

security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.

Control Enhancements for Sensitive Systems: None.

SA-3-COV-1

Control: Each Agency shall:

1. Project Initiation

   a. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.

   b. 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.

   c. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.

   d. 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

   a. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.

   b. Incorporate IT security requirements in IT system design specifications.

   c. Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.

   d. 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.

   e. 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

   a. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

b. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.

c. Require that the system comply with all relevant Risk Management requirements in this Standard.

d. 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

a. 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.

b. 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.

c. 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).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SA-3-COV-2

Control: Each agency ISO is accountable for ensuring the following steps are documented and followed:

1. Application Planning

a. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.

b. 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.

c. 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.

d. 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:

i. Encrypted communication channels shall be established for the transmission of sensitive information;

ii. Sensitive information shall not be transmitted in plain text between the client and the application; and

iii. 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.

a. 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.

b. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.

c. Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).

d. 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).

e. 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.

f. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted

g. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.

h. 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.

i. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

3. Production and Maintenance

a. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.

b. 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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SA-4 ACQUISITIONS

[Withdrawn: Not applicable to COV]

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and implements the appropriate organization-defined actions in response;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to the appropriate organization-defined personnel.

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for

example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements for Sensitive Systems:

(1) INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
[Withdrawn: Incorporated into SA-4 (1)].

(2) INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES
[Withdrawn: Incorporated into SA-4 (2)].

(3) INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN
[Withdrawn: Incorporated into SA-4 (2)].

(4) INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN

(5) [Withdrawn: Incorporated into SA-4 (2)]. INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE
[Withdrawn: Incorporated into SA-4 (2)].

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7].

SA-6-COV

Control: Each Agency shall or shall require that its service provider document software license management practices that address the following components, at a minimum:

a. Require the use of only agency approved software and service provider approved systems management software on IT systems.

b. Assess periodically whether all software is used in accordance with license agreements.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SA-7 USER-INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7].

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Control Enhancements for Sensitive Systems: None.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs appropriate processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

Supplemental Guidance: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define

expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during information system design, development, implementation, and operation;

b. Document, manage, and control the integrity of changes to the configuration items under configuration management;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to the appropriate organization-defined personnel.

Supplemental Guidance: This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;

b. Perform unit, integration, system, and regression testing/evaluation at the appropriate depth and coverage;

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems,

components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.

(3) [Withdrawn: Not applicable to COV]

(4) DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS

The organization requires the developer of the information system, system component, or information system service to perform a manual code review of specific code using the appropriate processes, procedures, and/or techniques.

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application's requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.

(5) DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS

The organization requires the developer of the information system, system component, or information system service to perform penetration testing at the appropriate breadth/depth and with documented organization-defined constraints.

Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

(6) DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS

The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

Supplemental Guidance: Attack surfaces of information systems are exposed areas that make those systems more vulnerable to cyber attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.

(7) DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION

The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at the appropriate depth of testing/evaluation.

Supplemental Guidance: Verifying that security testing/evaluation provides complete coverage of required security controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating security control coverage at the highest levels of assurance can be provided by the use of formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.

(8) [Withdrawn: Not applicable to COV]

SA-12 SUPPLY CHAIN PROTECTION

[Withdrawn: Not applicable to COV]

SA-13 TRUSTWORTHINESS

[Withdrawn: Not applicable to COV]

SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS

[Withdrawn: Not applicable to COV]

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations on an annual basis or more frequently if required to address an environmental change to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security requirements.

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design,

development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SA-16 DEVELOPER-PROVIDED TRAINING

Control: The organization requires the developer of the information system, system component, or information system service to provide organization-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.

Control Enhancements for Sensitive Systems: None.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance: [Withdrawn: Not applicable to COV]
Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SA-18 TAMPER RESISTANCE AND DETECTION

[Withdrawn: Not applicable to COV]

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

[Withdrawn: Not applicable to COV]

SA-21 DEVELOPER SCREENING

[Withdrawn: Not applicable to COV]

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control: The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Supplemental Guidance: Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Related controls: PL-2, SA-3.

Control Enhancements for Sensitive Systems:

(1) UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT

The organization provides either in-house support or organization-defined support from external providers for unsupported information system components.

Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

8.16. FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION CLASS: TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

1. System and communications protection policy on an annual basis or more frequently if required to address an environmental change; and

2. System and communications protection procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the SC family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, for example, 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 serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception. Related controls: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

SC-4 INFORMATION IN SHARED RESOURCES

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.

Control Enhancements for Sensitive Systems:

(1) INFORMATION IN SHARED RESOURCES | SECURITY LEVELS

[Withdrawn: Incorporated into SC-4].

(2) [Withdrawn: Not applicable to COV]

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of denial of service attacks by employing security safeguards.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7.

Control Enhancements for Sensitive Systems:

(1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS

The information system restricts the ability of individuals to launch denial of service attacks against other information systems.

Supplemental Guidance: Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have successfully breached the information system and are using the system as a platform to launch cyber attacks on third parties. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). Organizations can also limit the ability of individuals to use excessive information system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.

(2) DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY

The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

Supplemental Guidance: Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

(3) DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING

The organization:

(a) Employs monitoring tools to detect indicators of denial of service attacks against the information system; and

(b) Monitors information system resources to determine if sufficient resources exist to prevent effective denial of service attacks.

Supplemental Guidance: Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data. Related controls: CA-7, SI-4.

SC-6 RESOURCE PRIORITY

[Withdrawn: Not applicable to COV]

SC-7 BOUNDARY PROTECTION

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Control Enhancements for Sensitive Systems:

(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS
[Withdrawn: Incorporated into SC-7].

(2) BOUNDARY PROTECTION | PUBLIC ACCESS
[Withdrawn: Incorporated into SC-7].

(3) BOUNDARY PROTECTION | ACCESS POINTS
The organization limits the number of external network connections to the information system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES
The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy on an annual basis or more frequently if required to address an environmental change and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: Related control: SC-8.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

(6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES

[Withdrawn: Incorporated into SC-7 (18)].

(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

(8) [Withdrawn: Not applicable to COV]

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

The information system only allows incoming communications from organization-

defined authorized sources routed to organization-defined authorized destinations.

Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more general rules for authorized/allowed source/destination pairs. Related control: AC-3.

(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

The organization implements organization-defined host-based boundary protection mechanisms at the appropriate organization-defined information system component layer.

Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

(13) [Withdrawn: Not applicable to COV]

(14) [Withdrawn: Not applicable to COV]

(15) [Withdrawn: Not applicable to COV]

(16) [Withdrawn: Not applicable to COV]

(17) [Withdrawn: Not applicable to COV]

(18) [Withdrawn: Not applicable to COV]

(19) [Withdrawn: Not applicable to COV]

(20) [Withdrawn: Not applicable to COV]

(21) [Withdrawn: Not applicable to COV]

(22) [Withdrawn: Not applicable to COV]

(23) [Withdrawn: Not applicable to COV]

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine

what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Enhancements for Sensitive Systems:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by equivalent physical safeguards.

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

SC-8-COV

Control: Require the use of data protection mechanisms for the transmission of all email 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.
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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

[Withdrawn: Not applicable to COV]

SC-11 TRUSTED PATH

[Withdrawn: Not applicable to COV]

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the organization-defined requirements for key generation, distribution, storage, access, and destruction.

Supplemental Guidance: 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 Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Control Enhancements for Sensitive Systems:

(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

(2) [Withdrawn: Not applicable to COV]

(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES

[Withdrawn: Incorporated into SC-12].

(4) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS

[Withdrawn: Incorporated into SC-12].

SC-13 USE OF CRYPTOGRAPHY

Control: The information system implements cryptography in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on

organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements for Sensitive Systems: None.

(1) CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY

[Withdrawn: Incorporated into SC-13].

(2) CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY

[Withdrawn: Incorporated into SC-13].

(3) CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS

[Withdrawn: Incorporated into SC-13].

(4) CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SC-13].

SC-13-COV

Control: The organization shall:

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:

   a. Instructions in the IT Security Agency's Incident Response Plan on how to respond when encryption keys are compromised;

   b. A secure key management system for the administration and distribution of encryption keys; and

   c. 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.

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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 COLLABORATIVE COMPUTING DEVICES

[Withdrawn: Not applicable to COV]

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

[Withdrawn: Not applicable to COV]

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under a approved organization-defined certificate policy or obtains public key certificates from an approved service provider.

Supplemental Guidance: For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12.

Control Enhancements for Sensitive Systems: None.

SC-18 MOBILE CODE

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: Related controls: CM-6, SC-7, SC-15.

Control Enhancements for Sensitive Systems: None.

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

Control: The information system:

a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provides 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.

Supplemental Guidance: This control enables external clients including, for example, 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. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements for Sensitive Systems:

(1) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES
[Withdrawn: Incorporated into SC-20].

(2) [Withdrawn: Not applicable to COV]

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

[Withdrawn: Not applicable to COV]

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

[Withdrawn: Not applicable to COV]

SC-23 SESSION AUTHENTICITY

Control: The information system protects the authenticity of communications sessions.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Related controls: SC-8, SC-10, SC-11.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Incorporated into AC-12 (1)].

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Incorporated into SC-23 (3)].

SC-24 FAIL IN KNOWN STATE

[Withdrawn: Not applicable to COV]

SC-25 THIN NODES

[Withdrawn: Not applicable to COV]

SC-26 HONEYPOTS

[Withdrawn: Not applicable to COV]

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

[Withdrawn: Not applicable to COV]

SC-28 PROTECTION OF INFORMATION AT REST

Control: The information system protects the confidentiality and integrity of information at rest.

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. 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. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]
(2) [Withdrawn: Not applicable to COV]

SC-29 HETEROGENEITY

[Withdrawn: Not applicable to COV]

SC-30 VIRTUALIZATION TECHNIQUES

[Withdrawn: Not applicable to COV]

SC-31 COVERT CHANNEL ANALYSIS

[Withdrawn: Not applicable to COV]

SC-32 INFORMATION SYSTEM PARTITIONING

[Withdrawn: Not applicable to COV]

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

[Withdrawn: Not applicable to COV]

SC-35 HONEYCLIENTS

[Withdrawn: Not applicable to COV]

SC-36 DISTRIBUTED PROCESSING AND STORAGE

[Withdrawn: Not applicable to COV]

SC-37 OUT-OF-BAND CHANNELS

Control: The organization employs organization-defined out-of-band channels for the physical delivery or electronic transmission of organization-defined information, information system components, or devices to organization-defined individuals or information systems.

Supplemental Guidance: Out-of-band channels include, for example, local (nonnetwork) accesses to information systems, network paths physically separate from network paths used for operational traffic, or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers/authenticators, configuration management changes for hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates. Related controls: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements for Sensitive Systems:

(1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION

The organization employs organization-defined security safeguards to ensure that only organization-defined individuals or information systems receive the organization-defined information, information system components, or devices.

Supplemental Guidance: Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

SC-38 OPERATIONS SECURITY

[Withdrawn: Not applicable to COV]

SC-39 PROCESS ISOLATION

[Withdrawn: Not applicable to COV]

SC-40 WIRELESS LINK PROTECTION

[Withdrawn: Not applicable to COV]

SC-41 PORT AND I/O DEVICE ACCESS

Control: The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined information systems or information system components.

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example,

Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.

SC-42 SENSOR CAPABILITY AND DATA

Control: The information system:

a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: agency head approved policy, indicating business functions that cannot be accomplished without the use of the capability; and

b. Provides an explicit indication of sensor use to the user of the device.

Supplemental Guidance: [Withdrawn: Not applicable to COV]

Control Enhancements: [Withdrawn: Not applicable to COV]

Supplemental Guidance: This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems 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, for example, cameras, microphones, 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 specific movements of an individual.

Control Enhancements for Sensitive Systems:

(1) SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES

The organization ensures that the information system is configured so that data or information collected by the organization-defined sensors is only reported to authorized individuals or roles.

Supplemental Guidance: In situations where sensors are activated by authorized individuals (e.g., end users), it is still possible that the data/information collected by the sensors will be sent to unauthorized entities.

(2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

The organization employs appropriate organization-defined measures, so that data or information collected by organization-defined sensors is only used for authorized purposes.

Supplemental Guidance: Information collected by sensors for a specific authorized purpose potentially could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track movements of individuals. Measures to mitigate such activities include, for example, additional training to ensure that authorized parties do not abuse their authority, or (in the case where sensor data/information is maintained by external parties) contractual restrictions on the use of the data/information.

(3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES

The organization prohibits the use of devices possessing organization-defined environmental sensing capabilities in organization-defined facilities, areas, or systems.

Supplemental Guidance: For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain facilities or specific controlled areas within facilities where sensitive information is stored or sensitive conversations are taking place.

SC-42-COV

1) Permits the remote activation of environmental sensing capabilities if required as part of an authorized incident response activity; and
2) Only provides an explicit indication of the sensor use if authorized by the incident response team.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SC-43 USAGE RESTRICTIONS

Control: The organization:

a. Establishes usage restrictions and implementation guidance for organization-defined information system components based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of such components within the information system.

Supplemental Guidance: Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices). Related controls: CM-6, SC-7.

Control Enhancements: None.

SC-44 DETONATION CHAMBERS

[Withdrawn: Not applicable to COV]

8.17. FAMILY: SYSTEM AND INFORMATION INTEGRITY CLASS: OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:
    1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:

1. System and information integrity policy on an annual basis or more frequently if required to address an environmental change; and

2. System and information integrity procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the SI family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

SI-2 FLAW REMEDIATION

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within 90-days of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of

the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Incorporated into SI-2].

(6) [Withdrawn: Not applicable to COV]

SI-2-COV

Control: The organization:

a. Applies all software publisher security updates to the associated software products.

b. Applies all security updates as soon as possible after appropriate testing, not to exceed 90 days for implementation.

c. Prohibits the use of software products that the software publisher has designated as End-of-Life/End-of-Support (i.e. software publisher no longer provides security patches for the software product).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system at least once a week and real-time scans of files from external sources at network entry/exit points as well as the destination host as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. Quarantine malicious code; send alert to administrator in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help 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, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Control Enhancements for Sensitive Systems:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages malicious code protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

The information system automatically updates malicious code protection mechanisms.

Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.

(3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6 (10)].

(4) [Withdrawn: Not applicable to COV]

(5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7].

(6) [Withdrawn: Not applicable to COV]

(7) [Withdrawn: Not applicable to COV]

(8) [Withdrawn: Not applicable to COV]

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

SI-3-COV

Control: Each Agency shall, or shall require that its service provider:

1. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.).

2. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.

3. Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

4. Provide protection against malicious program through the use of mechanisms that:

   a. Eliminates or quarantines malicious programs that it detects;

   b. Provides an alert notification;

   c. Automatically and periodically runs scans on memory and storage devices;

   d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device;

   e. Allows only authorized personnel to modify program settings; and

   f. Maintains a log of protection activities.

5. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program

6. Require all forms of malicious code protection to start automatically upon system boot.

7. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.

8. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shut-down, restoration, notification, and reporting requirements.

9. Require use of only new media (e.g. diskettes, CD-ROM) or sanitized media for making copies of software for distribution.

10. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.

11. By written policy, prohibit the installation of software on Agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.

12. Establish Operating System (OS) update schedules commensurate with sensitivity and risk.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

a. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through organization-defined techniques and methods;

c. [Withdrawn: Not applicable to COV]

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. [Withdrawn: Not applicable to COV]

f. [Withdrawn: Not applicable to COV]

g. [Withdrawn: Not applicable to COV]

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, 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 may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

The information system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(5) [Withdrawn: Not applicable to COV]

(6) INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6 (10)].

(7) [Withdrawn: Not applicable to COV]

(8) INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION

[Withdrawn: Incorporated into SI-4].

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) [Withdrawn: Not applicable to COV]

(12) [Withdrawn: Not applicable to COV]

(13) *INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*

The organization:

(a) *Analyzes communications traffic/event patterns for the information system;*

(b) *Develops profiles representing common traffic patterns and/or events; and*

(c) *Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.*

(14) INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Supplemental Guidance: Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems. Related controls: AC-18, IA-3.

(15) INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Supplemental Guidance: Related control: AC-18.

(16) INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

The organization correlates information from monitoring tools employed throughout the information system.

Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.

(17) [Withdrawn: Not applicable to COV]

(18) [Withdrawn: Not applicable to COV]

(19) [Withdrawn: Not applicable to COV]

(20) [Withdrawn: Not applicable to COV]

(21) [Withdrawn: Not applicable to COV]

(22) [Withdrawn: Not applicable to COV]

(23) [Withdrawn: Not applicable to COV]

(24) [Withdrawn: Not applicable to COV]

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

a. Receives information system security alerts, advisories, and directives from the appropriate external organizations on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to organization-defined list of personnel identified by name and/or by role; and

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: Related control: SI-2.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SI-6 SECURITY FUNCTIONALITY VERIFICATION

[Withdrawn: Not applicable to COV]

SI-7 SOFTWARE AND INFORMATION INTEGRITY

[Withdrawn: Not applicable to COV]

SI-8 SPAM PROTECTION

Control: The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].

SI-10 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of information inputs.

Supplemental Guidance: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software 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 tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS

The organization ensures that input validation errors are reviewed and resolved within 30-days of discovery.

Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.

(3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR

The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

Supplemental Guidance: A common vulnerability in organizational information systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying information system responses that facilitate transitioning the system to known states without adverse, unintended side effects.

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

SI-11 ERROR HANDLING

[Withdrawn: Not applicable to COV]

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

[Withdrawn: Not applicable to COV]

SI-13 PREDICTABLE FAILURE PREVENTION

[Withdrawn: Not applicable to COV]

SI-14 NON-PERSISTENCE

[Withdrawn: Not applicable to COV]

SI-15 INFORMATION OUTPUT FILTERING

[Withdrawn: Not applicable to COV]

SI-16 MEMORY PROTECTION

[Withdrawn: Not applicable to COV]

SI-17 FAIL-SAFE PROCEDURES

[Withdrawn: Not applicable to COV]

FAMILY: *PM – Program Management*

[Withdrawn: Not applicable to COV]

This page intentionally left blank

GLOSSARY OF SECURITY DEFINITIONS

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at
http://www.vita.virginia.gov/library/default.aspx?id=537.

INFORMATION SECURITY ACRONYMS

AITR: Agency Information Technology Representative

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan, now referred to as Continuity Plan.

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

ISO: Information Security Officer

ISO/IEC: International Organization for Standardization/

International Electrotechnical Commission

ITIES: Information Technology Investment and Enterprise

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

PCI: Payment Card Industry

PDA: Personal Digital Assistant

PI: Personal Information

PIN: Personal Identification Number

RA: Risk Assessment

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SDLC: Systems Development Life Cycle

Solutions Directorate (VITA)

SSID: Service Set Identifier

SSP: Security Program Plan

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX A – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

The form an Agency must submit to request an exception to any requirement of this Standard and the related Information Security Policy is on the following page.

COV Information Security Policy & Standard Exception Request Form

Agency Name: _____Contact for Additional Information: _____

Policy/Standard requirement to which an exception is requested:_____

Note: This request is for an exception(s) to a component of the Commonwealth policy and/or standard(s) and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.

1. Provide the **Business or Technical Justification:**

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify all residual risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

_____ _____ _____

Printed name Agency Head **Signature** **Date**

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____

CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____

Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Appeal

Approved_____ Denied_____ Comments:

_____ _____
CIO Date