COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Security Standard

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Please direct questions to Commonwealth Security and Risk Management (CSRM). CSRM will issue a Change Notice Alert and post on the VITA Website, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties CSRM considers interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
01	07/01/2023	Base Document
01.1	09/30/2024	Administrative changes: Identifying Changes in This Document: Replaced the word new with the word deleted; 2.4: Changed continuity plan to contingency plan; 2.5-7: Removed italics from URL; 8: Changed seventeen families to twenty families; AC-4-CE-20: Moved the period inside the bracket; AC-12: Removed "of inactivity"; AU-2-CE-1-4: Changed Control Name to Event Logging; AU-9: Changed bullets from number to letters; CA-2: Changed Control Name to Control Assessments; CA-3-CE-1-5: Changed Control Name to Information Exchange; CM-8-CE-1: Added the Discussion and Related Controls; IA-2: Removed extra space between user and and; IA-5-COV-2-b: Removed the word and; IA-5-COV-2-c: Changed the period to a semicolon and added the word and; IA-5-COV-2-c/d: Created bullet d; IR-3: Removed and Exercises from the Control Name; MP-5: Changed to FIPS 140-3; PE-18: Underlined Discussion; PE-18-CE-1: Removed Information from the Control Name; PL-1: Removed The Organization after Control:; PL-2: Changed Control Name to Plans; PL-8: Changed Control Name to Architectures; SA-4-CE-7: Removed the -1; SA-4-CE-12: Underlined Related Controls and Discussion; SA-4-COV-1: Removed the -1; SA-4-COV-1: Added Control:; SA-5-CE-1-5: Removed Information from the Control Name; SC-4-CE-1 & 2: Changed Control Name to include System; SC-8: Increased font size to 11; SC-12-COV: Changed bullets from numbers to letters; SC-12-COV-2: Removed the word And at the end and add it to number 1; SC-13: Changed Control Name to Cryptographic Protection; SC-13-COV: Added a period at the end of None after Control Enhancement; SC-21-CE: Removed the word None; SC-42-COV: Changed the bullets from numbers to letters and added Control: to the beginning; SI-2: Removed the words at least; SI-2-CE-2: Removed the words at least; SI-2-CE-3: Removed the words at least; SI-2-COV: Removed The Organization after Control:; SI-4-CE-8: Removed Information from the Control Name; SI-7: Added a comma after FIRMWARE; SI-10-CE-2: Removed the words at least;

Identifying Changes in This Document

- See the latest entry in the table above.
- Vertical lines in the left margin indicate that the paragraph has changes or additions.
- Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

~~**Example of *deleted* new section –** This section of text is *deleted* new.~~

Review Process

Commonwealth Security and Risk Management provided the initial review of this publication.

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation

COV ITRM Standard SEC530-01.1

Subject

Information Security

Effective Date

September 28, 2023

Compliance Date

March 31, 2024

Supersedes

ITRM Standard SEC525-05.0 dated August 25, 2022 and ITRM Standard SEC501-12.0 dated August 25, 2022

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia, §2.2-2009

(Additional Powers of the CIO relating to security)

Scope

In general, this standard is applicable to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education (collectively referred to as "Agency" or "Organization"). This standard is offered only as guidance to local government entities. Exemptions from the applicability of this standard are defined in detail in Section 1.6.

In addition, the Code of Virginia § 2.2-2009, specifies that policies, procedures, and standards that address security audits (Section 7 of this standard) apply only to "all executive branch and independent agencies and institutions of higher education." Similarly, the Code of Virginia § 2.2-603, specifies that requirements for reporting of information security incidents apply only to "every department in the executive branch of state government."

Purpose

To define the minimum requirements for each Agency's information security management program.

General Responsibilities

(Italics indicate quote from the Code of Virginia *requirements)*

Chief Information Officer of the Commonwealth (CIO)

Develops and approves statewide technical and data policies, standards and guidelines for information technology and related systems.

Chief Information Security Officer

The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

Virginia Information Technologies Agency (VITA)

At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budget requests and strategic plans, and when developing and managing IT related services.

Information Technology Advisory Council (ITAC)

Advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems

Executive Branch Agencies

Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems. Comply with the requirements established by COV policies and standards. Apply for exceptions to requirements when necessary.

Judicial and Legislative Branches

In accordance with the Code of Virginia §2.2-2009: the: “CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs.”

Commonwealth Security and Risk Management Directorate

In accordance with the Code of Virginia § 2.2-2009 the CIO has assigned the Commonwealth Security and Risk Management the following duties: Development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, standards, and guidelines shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies. International Standards

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27000 series

Definitions

Definitions are found in the single comprehensive glossary that supports Commonwealth Information Technology Resource Management (ITRM) documents (COV ITRM Glossary)

Related ITRM Policy

Current version of the COV ITRM Policy: Information Security Policy

Table of Contents

1. INTRODUCTION

1.1 INTENT

The intent of this information security standard is to establish a baseline for information security and risk management activities for agencies across the Commonwealth of Virginia (COV). These baseline activities include, but are not limited to, any regulatory requirements that an agency is subject to, information security best practices, and the requirements defined in this Standard. These information security and risk management activities will provide protection of, and mitigate risks to agency information systems and data.

This standard defines the minimum acceptable level of information security and risk management activities for the COV agencies that must implement an information security program that complies with requirements identified in this standard. Agencies may develop their own information security standards, based on needs specific to their environments. Agency standards must provide for protection of the agency's information systems and data, at a level greater than or equal to the baseline requirements set forth in this standard. As used in this standard, sensitivity encompasses the elements of confidentiality, integrity, and availability. See *RA-2*.

This standard has been created using the National Institute of Standards and Technology (NIST) Special Publication 800-53 rev. 5, Recommended Security Controls for Federal Information Systems and Organizations, as a framework.

Note: Where the Standard states that the "Organization" is designated as the responsible party for controls, implementation of certain controls can be delegated to a third party service provider given that proper documentation exists.

The COV Information Security Program consists of the following Control Families:

- AC - Access Control
- AT - Awareness and Training
- AU - Audit and Accountability
- CA – Assessment, Authorization, and Monitoring
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA – Maintenance
- MP - Media Protection
- PE - Physical and Environmental Protection
- PL – Planning
- PM – Program Management
- PS - Personnel Security
- PT - Personally Identifiable Information Processing and Transparency
- RA - Risk Assessment
- SA - System and Services Acquisition
- SC - System and Communications Protection

- SI - System and Information Integrity
- SR - Supply Chain Risk Management

These component areas provide a framework of minimal requirements that agencies shall use to develop their agency information security programs with a goal of allowing agencies to accomplish their missions in a safe and secure environment. Each component listed above contains requirements that, together, comprise this Information Security Standard.

This Standard recognizes that agencies may procure IT equipment, systems, and services covered by this standard from third parties. In such instances, Agency Heads remain accountable for maintaining compliance with this standard and agencies must enforce these compliance requirements through documented agreements with third-party providers and oversight of the services provided.

1.2 ORGANIZATION OF THIS STANDARD

The component areas of the COV Information Security Program provide the organizational framework for this standard. Each component area consists of one or more sections containing:

- Controls
- Discussion
- Related Controls
- Control Enhancements

1.3 ROLES AND RESPOSIBILITIES

Each agency should utilize an organization chart that depicts the reporting structure of employees when assigning specific responsibilities for the security of IT systems and data. Each agency shall maintain documentation regarding specific roles and responsibilities relating to information security.

1.4 INFORMATION SECURITY PROGRAM

Each agency shall establish, document, implement, and maintain its information security program appropriate to its business and technology environment in compliance with this standard.

1.5 EXCEPTION TO SECURITY REQUIREMENTS

If an Agency Head determines that compliance with the provisions of this standard or any related information security standards would adversely impact a business process of the agency, the Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the CISO. For each exception, the requesting agency shall fully document:

1. Business need
2. Scope and extent
3. Mitigating safeguards
4. Residual risks
5. Specific duration
6. Agency Head approval

Submission of an exception request stipulates that the Agency Head understands and accepts responsibility for the risks incurred in the environment. Each request shall be in writing to the CISO and approved by the Agency Head indicating acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken. An exception will not be

accepted for processing unless all residual risks have been documented and the Agency Head has approved, indicating acceptance of these risks. The exception request must be submitted by the Agency Head or Information Security Officer. Denied exception requests may be appealed to the CIO of the Commonwealth.

1.6 EXEMPTIONS FROM APPLICABILITY

The following are explicitly exempt from complying with the requirements defined in this document:

1. Systems under development and/or experimental systems that do not create additional risk to production systems

Note: Preproduction environments that utilize and/or contain production data (even if the data is an older copy of the data from the production environment) are not exempt from complying with the requirements defined in the document (Refence Control: SA-3-CE-2)

2. Surplus and retired systems

1.7 DETERMINIATION OF LIABILITY

All agreements between an agency and a service provider must include liability language commensurate with data sensitivity and risk. The CIO of the Commonwealth of Virginia or documented designee will evaluate and act as the approving authority for all such liability language to ensure that it is sufficient to account for all identified risks.

1.8 REVOCATION OF HOSTED COMPUTING PERMISSIONS

The CIO of the Commonwealth of Virginia reserves the right to revoke an agency's ability to service an application or business function within a hosted environment if the agency does not perform its due diligence to protect the data assigned to that agency. The agency must ensure the confidentiality, integrity, and availability of its data without concern for the data center's geographical location. The agency must complete all remediation actions required by an audit or approved security exception within the required timeframe. The agency must also ensure that the hosting vendor produce and provide to the agency all compliance reporting required by this standard within the timeframe specified by this standard.

2. INFORMATION SECURITY ROLES AND RESPONSIBILITIES

2.1 PURPOSE

This Section defines the key IT security roles and responsibilities included in the Commonwealth's Information Security Program. These roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

2.2 CHIEF INFORMATION OFFICER OF THE COMMONWEALTH (CIO)

The Code of Virginia §2-2.2009 states that *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information."*

2.3 CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO is responsible for development and coordination of the COV Information Security Program and, as such, performs the following duties:

1. Administers the COV Information Security Program and periodically assesses whether the program is implemented in accordance with COV Information Security Policies and Standards.
2. Reviews requested exceptions to COV Information Security Policies, Standards and Procedures.
3. Provides solutions, guidance, and expertise in IT security.
4. Maintains awareness of the security status of sensitive IT systems.
5. Facilitates effective implementation of the COV Information Security Program, by:
    a. Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;
    b. Collecting data relative to the state of IT security in the COV and communicating as needed;
    c. Providing consultation on balancing an effective information security program with business needs.
6. Provides networking and liaison opportunities to Information Security Officers (ISOs).

2.4 AGENCY HEAD

Each Agency Head is responsible for the security of the agency's IT systems and data. The Agency Head's IT security responsibilities include the following:

1. Designate an Information Security Officer (ISO) for the agency, no less than biennially.

    Note: Acceptable methods of communicating the designation to the CISO, include:

    - An email directly from the agency head, or
    - An email from an agency head designee which copies the agency head, or
    - A hard-copy letter or facsimile transmission signed by the agency head.
    - This designation must include the following information:

    a. ISO's name

    b. ISO's title

c. ISO's contact information

The ISO shall report directly to the Agency Head and must not simultaneously serve the function of a Chief Information Officer (CIO). The ISO is responsible for developing and managing the agency's information security program. Agencies with multiple geographic locations or specialized business units should also consider designating deputy ISOs as needed.

2. Ensure that an agency information security program is maintained, that is sufficient to protect the agency's IT systems, and that is documented and effectively communicated. Managers in all agencies and at all levels shall provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.
3. Review and approve the agency's Business Impact Analyses (BIAs), Risk Assessments (RAs), and *Contingency* ~~Continuity~~ Plan (previously referred to as Continuity of Operations Plan or COOP), to include an IT Disaster Recovery Plan, if applicable.
4. Review or have the designated ISO review the System Security Plans for all agency IT systems classified as sensitive, and:
   - Approve System Security Plans that provide adequate protections against security risks; or
   - Disapprove System Security Plans that do not provide adequate protections against security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against security risks.
5. Ensure compliance is maintained with the current version of the *IT Security Audit Standard* (COV ITRM Standard SEC502). This compliance must include, but is not limited to:
   a. Requiring development and implementation of an agency plan for IT security audits, and submitting this plan to the CISO;
   b. Requiring that the planned IT security audits are conducted;
   c. Receiving reports of the results of IT security audits;
   d. Requiring development of Corrective Action Plans to address findings of IT security audits; and
   e. Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.

   Note: If the IT security audit shows no findings, this is to be reported to the CISO as well.
6. Ensure a program of information security safeguards is established.
7. Ensure an information security awareness and training program is established.
8. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.
9. Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system.
10. Prevent or have designee prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:
    a. The ISO is not a System Owner or a Data Owner except in the case of compliance systems for information security;

b. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and

c. The ISO, System Owners, and Data Owners are COV employees.

Notes:

- Other roles may be assigned to contractors. For roles assigned to contractors, the contract language must include specific responsibility and background check requirements.
- A System Owner can own multiple IT systems.
- A Data Owner can own data on multiple IT systems.
- System Administrators can assume responsibility for multiple IT systems.

2.5 INFORMATION SECURITY OFFICER (ISO)

The ISO is responsible for developing and managing the agency's information security program. The ISO's duties are as follows:

1. Develop and manage an agency information security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.
2. Verify and validate that all agency IT systems and data are classified for sensitivity.
3. Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter.
4. Implement and maintain the appropriate balance of preventative, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality.
5. Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.
6. Maintain liaison with the CISO.
7. Annually meet the requirements to obtain or maintain the Commonwealth ISO certification outlined in the link below: https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/docs/COV-ISO-Certification-and-Continuing-Education-Requirements.pdf

2.6 PRIVACY OFFICER

An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise, these responsibilities are carried out by the ISO. The Privacy Officer provides guidance on:

1. The requirements of state and federal Privacy laws.
2. Disclosure of and access to sensitive data.
3. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

2.7 SYSTEM OWNER

The System Owner is the agency business manager responsible for having an IT system operated and maintained. With respect to IT security, the System Owner's responsibilities include the following:

1. Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
2. Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
3. Maintain compliance with COV Information Security policies and standards in all IT system activities.
4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
5. Designate a System Administrator for the system.

Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner, upon request, the CIO of the Commonwealth will determine the System Owner.

2.8 DATA OWNER

The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

1. Evaluate and classify sensitivity of the data.
2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the System Owner.
4. Define requirements for access to the data.

Note: The Data Owner must enforce all controls and processes required to protect all data classified as sensitive from compromise, unauthorized alteration, or loss. Therefore, the Data Owner is responsible for the protection of all data classified as sensitive regardless of the actions of any assigned data custodian and must ensure that each data custodian allowed access to the sensitive data has the knowledge and capabilities required to protect the confidentiality, integrity, and availability of the data.

2.9 SYSTEM ADMINISTRATOR

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.

2.10 DATA CUSTODIAN

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

1. Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

2. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.
3. Providing Data Owners with reports, when necessary and applicable.

2.11 IT SYSTEM USERS

All users of COV IT systems including, but not limited to, employees and contractors are responsible for the following:

1. Reading and complying with agency information security program requirements.
2. Reporting breaches of IT security, actual or suspected, to their agency management and/or the CISO.
3. Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

3. BUSINESS IMPACT ANALYSIS

3.1 PURPOSE

Business Impact Analysis (BIA) delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions.

Note: The requirements below address only the IT and data aspects of a BIA and **do not** require agencies to develop a BIA separate from the BIA that could be used to develop an agency's Continuity Plan (previously referred to as Continuity of Operations Plan). Agencies should create a single BIA that meets both the requirements of this standard and can be used to develop the agency Continuity Plan (previously referred to as Continuity of Operations Plan).

3.2 REQUIREMENTS

Each agency should:

1. Require the participation of System Owners and Data Owners in the development of the agency's BIA.
2. Identify agency business functions.
3. Identify mission essential functions (MEFs).

   Note: MEFs are functions that cannot be deferred during an emergency or disaster.
4. Identify dependent and supporting functions, known as primary business functions (PBFs), previously referred to as primary functions, on which each mission essential function (MEF) depends.
5. For each MEF and PBF, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover a MEF or PBF shall be considered sensitive relative to availability. For each such system, each agency shall:
   a. Document the required Recovery Time Objective (RTO), based on agency and COV goals, objectives, and MEFs, as outlined in the agency Continuity Plan
   b. Document the Recovery Point Objectives (RPO) as outlined in the agency Continuity Plan.
   c. Identify the IT resources that support each MEF and PBF
6. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 4), Risk Assessment (Section 6), Contingency Plan (Section CP-2) and System Security Plan (Section PL-2).
7. Conduct annual reviews of the agency BIAs, and conduct a full revision at least once every three years.

4. IT SYSTEM AND DATA SENSITIVITY CLASSIFICATION

4.1 PURPOSE

IT System and Data Sensitivity Classification requirements identify the steps necessary to classify all IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure;
- Integrity, which addresses sensitivity to unauthorized modification; and
- Availability, which addresses sensitivity to outages.

Sensitive data is any data of which the compromise with respect to confidentiality, integrity, or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. Agencies must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits.

When determining the sensitivity of a system, an agency must review the sensitivity of the data set that is transmitted, processed, or stored as well as the sensitivity of the business processes that are supported by the system.

4.2 REQUIREMENTS

Each Information Security Officer shall:

1. Identify or require that the Data Owner identify the type(s) of data handled by each agency IT system. Types of data handled by the agencies could include: personally identifiable information, medical information, banking or credit card information, tax information, legal or investigative information, or intellectual property.
2. Document completed data set template and attach to IT system security plan for each agency owned IT system.
3. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.

   Example: Some IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc.
4. Data Set - Require that the Data Owner determine the potential damages to the agency of a compromise of confidentiality (which addresses sensitivity to unauthorized disclosure), integrity (which addresses sensitivity to unauthorized modification) or availability (which addresses sensitivity to outages) of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

   Example: Data Owners may construct a table similar to the following table ranking each data set according to its impact to confidentiality, integrity and availability. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration of one way to accomplish this:

Sensitivity Criteria for Data Sets				
Type of Data	**Confidentiality**	**Integrity**	**Availability**	***Sensitive Yes or No***
HR Policies	Low	High	Moderate	Yes
Medical Records	High	High	High	Yes
Criminal Records	High	High	High	Yes
Travel Voucher	Moderate	Moderate	Moderate	Yes
Accounts Payable	Low	Moderate	Low	Yes
State Employee Names	Low	Low	Low	No

Table 1: Sample Sensitivity Analysis Results

Classify the IT system as sensitive based on the highest potential impact described in the table above.

Agencies should classify IT systems as sensitive if a type of data handled by the IT system has a sensitivity of moderate or high on the criteria of confidentiality, integrity, or availability.

5. Business Process - A system is sensitive if a critical business process or mission essential function relies on the system. A business process should be evaluated based on an analysis of confidentiality, integrity, and availability.

   Classify the IT system based on the highest potential impact described in the attributes evaluated above. Agencies should classify IT systems as sensitive if the business process that is dependent on the IT system has a sensitivity of moderate or high on the criteria of confidentiality, integrity, and availability.

6. Classify the IT system as sensitive if any type of the data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.

   Agencies should classify IT systems as “sensitive” if a type of data handled by the IT system has two or more classifications with a sensitivity of moderate on the criteria of confidentiality, integrity, and availability. Documentation should be developed and maintained by the agency in cases where this determination is identified as “non-sensitive.”

7. Review IT system and data classifications with the Agency Head or designee and obtain Agency Head or designee approval of these classifications.

8. Verify and validate that all agency IT systems and data have been reviewed and classified as appropriate for sensitivity.

9. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.

10. Enter IT system and data sensitivity classification directly into the CSRM eGRC system. The agency shall ensure the information in eGRC is current and updated at least annually, or when substantive changes occur.

11. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process defined in this standard.

5. SENSITIVE IT SYSTEM INVENTORY AND DEFINITION

5.1 PURPOSE

Sensitive IT System Inventory and Definition requirements identify the steps in listing and marking the boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for IT systems, for the agency as a whole, and for the COV enterprise.

5.2 REQUIREMENTS

Each ISO or designated Sensitive System Owner(s) shall:

1. Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.

   Note: Data and homogeneous systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

   Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for the purposes of this standard, upon request, the CIO of the Commonwealth will determine the System Owner.

   Note: A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

2. Maintain or require that its service provider maintain updated network diagrams.

6. RISK ASSESSMENT

6.1 PURPOSE

Risk Assessment requirements delineate the steps agencies must take for each IT system classified as sensitive to:

- Identify potential threats to an IT system and the environment in which it operates;
- Determine the likelihood that threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Note: The Risk Assessment (RA) required by this standard differs from the RA required by the current version of the Project Management Standard (CPM112-nn). This standard requires an RA based on operational risk, while the Project Management Standard requires an RA based on project risk. Many of the RA techniques described in the Project Management Standard, however, may also be applicable to the RA required by this standard.

6.2 REQUIREMENTS

For each IT system classified as sensitive, the data-owning agency shall:

1. Conduct and document a RA of the IT system as needed, but not less than once every three years.
2. Conduct and document an annual self-assessment to determine the continued validity of the RA.

   Note: In addition, in agencies that own both sensitive IT systems and IT systems that are exempt from the requirements of this standard, the agency's RAs must include consideration of the added risk to sensitive IT systems from the exempt IT systems.
3. Prepare a report of each RA that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations. The report must be reviewed and approved by the ISO or ISO designee.

7. IT SECURITY AUDITS

7.1 PURPOSE

IT Security Audit requirements define the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective.

Note: In accordance with *the* Code of Virginia § 2.2-2009, the requirements of this section apply only to *"all executive branch and independent agencies and institutions of higher education."*

7.2 REQUIREMENTS

For each IT system classified as sensitive, the data-owning agency shall:

1. Require that the IT systems undergo an IT Security Audit as required by and in accordance with the current version of the IT Security Audit Standard (COV ITRM Standard SEC502).
2. Assign an individual to be responsible for managing IT Security Audits.
3. IT Security Audits should only be performed by independent parties who are not associated with the processes or procedures of the system.

8. SECURITY CONTROL CATALOG

Security controls described in this standard have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into *twenty* ~~seventeen~~ families. Each security control family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each security control family. In addition, there are three general classes of security controls: management, operational, and technical.

To identify each security control, a numeric identifier is appended to the family identifier to indicate the number of the control within the family. For example, CP-9 is the ninth control in the Contingency Planning family and AC-2 is the second control in the Access Control family. Additionally, security controls specific to the Commonwealth of Virginia (COV) are appended with "COV". For example, CP-9-COV indicates additional COV requirements related to the CP-9 control.

The security control structure consists of the following components: (i) a Control section; (ii) a Discussion section; and (iii) a Control Enhancements section.

The Control section provides a concise statement of the specific security capabilities needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system.

The Discussion section provides additional information related to a specific security control, but contains no requirements. Organizations are expected to apply the Discussion as appropriate, when defining, developing, and implementing security controls. The Discussion provides important considerations for implementing security controls in the context of an organization's operational environment, mission requirements, or assessment of risk. Security Control Enhancements may also contain a Discussion section. Enhancement Discussion is used in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement.

The Control Enhancements section provides statements of security capability to: (i) build in additional functionality to a control for sensitive systems; and/or (ii) increase the strength of a control for sensitive systems. In both cases, the Control Enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to the basic control functionality based on the results of a risk assessment. Control Enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. If the Control Enhancements are selected, those enhancements are additional control requirements. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among the enhancements.

8.1 ACCESS CONTROL

AC-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to all organization personnel, contractors, and service providers with a responsibility to implement access controls:

   1. Organization-level access control policy that:

      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls;

b. Designate the Information Security Officer to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

   1. Policy on an annual basis and following an environmental change; and

   2. Procedures on an annual basis and following an environmental change.

Discussion: Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: IA-1, PM-9, PM-24, PS-8, SI-12.

Control Enhancements: None.

AC-2 ACCOUNT MANAGEMENT

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require organization-defined prerequisites and criteria for group and role membership;

d. Specify:

   1. Authorized users of the system;

   2. Group and role membership; and

3. Access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Require approvals by the Agency Head, ISO, or designee for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with the agency-defined logical access control policy;

g. Monitor the use of accounts;

h. Notify account managers within:

1. One business day when accounts are no longer required;

2. Within 24 hours of when users are terminated or transferred; and

3. One business day when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Other attributes as required by the organization or associated missions/business functions;

j. Review accounts for compliance with account management requirements on an annual basis and following an environmental change;

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such

accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Support the management of system accounts using organization-defined automated mechanisms.

Discussion: Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage.

Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Related Controls: None.

(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

Automatically disable temporary and emergency accounts after no more than 30 days.

Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related Controls: None.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

Disable accounts within 24 hours when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for 90 days

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality, which reduce the attack surface of the system.

Related Controls: None.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls: AU-2, AU-6.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Require that users log out when the session inactivity time has exceeded 30 minutes.

Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls: AC-11.

(6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT

[Withdrawn: Not applicable to COV.]

(7) ACCOUNT MANAGEMENT | PRIVILEGED USER ACCOUNTS

(a) Establish and administer privileged user accounts in accordance with a role-based access scheme;

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

Discussion: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

Related Controls: None.

(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT

[Withdrawn: Not applicable to COV.]

(9) ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS

[Withdrawn: Not applicable to COV.]

(10) ACCOUNT MANAGEMENT | SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE

[Withdrawn: Incorporated into AC-2k.]

(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS

[Withdrawn: Not applicable to COV.]

(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE

(a) Monitor system accounts for atypical or suspicious usage; and

(b) Report atypical usage of system accounts to the Information Security Officer, Agency Head, or Chief Information Security Officer.

Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals.

Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Disable accounts of individuals within four hours of discovering of organization-defined significant risks.

Discussion: Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Related Controls: AU-6, SI-4.

AC-2-COV

Control: Each agency shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

Note: It is strongly recommended technical controls be implemented wherever possible to fulfill the following requirements, understanding that manual processes must sometimes be implemented to compensate for technical controls that might not be feasible.

a. For all internal and external IT systems:

   1. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.
   2. Disable unneeded accounts in a timely manner.
   3. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.
   4. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.
   5. Require that the System Administrator and the Information Security Officer or designee investigate any unusual system access activities.
   6. Require the System and Data Owner approve changes to access level authorizations.
   7. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
   8. Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined residual risks.
   9. Require that at least two individuals have administrative accounts to each IT system.
   10. The information system automatically audits account creation, disabling, and termination actions and notifies, as required, appropriate individuals.
   11. Temporarily disable logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.
   12. Disable logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

b. For all internal IT systems:

1. Require a documented request from the user to establish an account on any internal IT system.
2. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.
3. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the Data Owner, Data Owner or designee, or ISO to establish accounts for all sensitive IT systems.
4. Require secure delivery of access credentials to the user based on information already on file.
5. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.
6. Promptly remove access when no longer required.

c. For all external IT systems, require secure delivery of access credentials to users of all external IT systems.

d. For all service and hardware accounts:

1. Document account management practices for all agency created service accounts, including, but not limited to granting, administering and terminating accounts. If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the Password Management section of this Standard.

Discussion: None.

Related Controls: None.

Control Enhancements:

(1) If the IT system is classified as sensitive, prohibit the use of guest accounts.

(2) If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:

(a) Are documented according to standard practice and maintained on file;

(b) Include access attributes for the account.

(c) Are approved by the System Owner and communicated to the ISO; and

(d) Expire after a predetermined period, based on sensitivity and risk.

(3) For all external IT systems:

(a) Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.

(b) Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).

AC-3 ACCESS ENFORCEMENT

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of

mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Related Controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

Control Enhancements:

(1) ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6.]

(2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION

[Withdrawn: Not applicable to COV.]

(3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL

[Withdrawn: Not applicable to COV.]

(4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL

[Withdrawn: Not applicable to COV.]

(5) ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION

[Withdrawn: Not applicable to COV.]

(6) ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION

[Withdrawn: Incorporated into MP-4 and SC-28.]

(7) ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL

Enforce a role-based access control policy over defined subjects and objects and control access based upon organization-defined roles and users authorized to assume such roles.

Discussion: Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization- defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Related Controls: None.

(8) ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS

[Withdrawn: Not applicable to COV.]

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

Release information outside of the system only if:

(a) The receiving organization authorized system or system component provides security controls that meet Commonwealth security standards; and

(b) The organization-defined controls are used to validate the appropriateness of the information designated for release.

Discussion: Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigation measure, organizations procedurally determine whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy.

Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.

Related Controls: CA-3, PT-7, PT-8, SA-9, SC-16.

(10) ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS

[Withdrawn: Not applicable to COV.]

(11) ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES

Restrict access to data repositories containing organization-defined information types.

Discussion: Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.

Related Controls: CM-8, CM-12, CM-13, PM-5.

(12) ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS

[Withdrawn: Not applicable to COV.]

(13) ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL

[Withdrawn: Not applicable to COV.]

(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

[Withdrawn: Not applicable to COV.]

(15) ACCESS ENFORCEMENT | DISCRETIONARY AND MANDATORY ACCESS CONTROL

[Withdrawn: Not applicable to COV.]

AC-4 INFORMATION FLOW ENFORCEMENT

Control: Enforces approved authorizations for controlling the flow of information within the system and between connected systems based on the appropriate organization-defined information flow control policies.

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

Control Enhancements:

(1) INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY AND PRIVACY ATTRIBUTES

[Withdrawn: Not applicable to COV.]

(2) INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS

[Withdrawn: Not applicable to COV.]

(3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL

[Withdrawn: Not applicable to COV.]

(4) INFORMATION FLOW ENFORCEMENT | FLOW CONTROL OF ENCRYPTED INFORMATION

[Withdrawn: Not applicable to COV.]

(5) INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES

[Withdrawn: Not applicable to COV.]

(6) INFORMATION FLOW ENFORCEMENT | METADATA

[Withdrawn: Not applicable to COV.]

(7) INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS

[Withdrawn: Not applicable to COV.]

(8) INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS

[Withdrawn: Not applicable to COV.]

(9) INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS

[Withdrawn: Not applicable to COV.]

(10) INFORMATION FLOW ENFORCEMENT | ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS

[Withdrawn: Not applicable to COV.]

(11) INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS

[Withdrawn: Not applicable to COV.]

(12) INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS

[Withdrawn: Not applicable to COV.]

(13) INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS

[Withdrawn: Not applicable to COV.]

(14) INFORMATION FLOW ENFORCEMENT | SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS

[Withdrawn: Not applicable to COV.]

(15) INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION

[Withdrawn: Not applicable to COV.]

(16) INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS

[Withdrawn: Incorporated into AC-4.]

(17) INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION

[Withdrawn: Not applicable to COV.]

(18) INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING

[Withdrawn: Incorporated into AC-16.]

(19) INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA

[Withdrawn: Not applicable to COV.]

(20) INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS

[Withdrawn: Not applicable to COV.]

(21) INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS

[Withdrawn: Not applicable to COV.]

(22) INFORMATION FLOW ENFORCEMENT | ACCESS ONLY

[Withdrawn: Not applicable to COV.]

(23) INFORMATION FLOW ENFORCEMENT | MODIFY NON-RELEASABLE INFORMATION

[Withdrawn: Not applicable to COV.]

(24) INFORMATION FLOW ENFORCEMENT | INTERNAL NORMALIZATION FORMAT

[Withdrawn: Not applicable to COV.]

(25) INFORMATION FLOW ENFORCEMENT | DATA SANITIZATION

[Withdrawn: Not applicable to COV.]

(26) INFORMATION FLOW ENFORCEMENT | AUDIT FILTERING ACTIONS

[Withdrawn: Not applicable to COV.]

(27) INFORMATION FLOW ENFORCEMENT | REDUNDANT/INDEPENDENT FILTERING MECHANISMS

[Withdrawn: Not applicable to COV.]

(28) INFORMATION FLOW ENFORCEMENT | LINEAR FILTER PIPELINES

[Withdrawn: Not applicable to COV.]

(29) INFORMATION FLOW ENFORCEMENT | FILTER ORCHESTRATION ENGINES

[Withdrawn: Not applicable to COV.]

(30) INFORMATION FLOW ENFORCEMENT | FILTER MECHANISMS USING MULTIPLE PROCESSES

[Withdrawn: Not applicable to COV.]

(31) INFORMATION FLOW ENFORCEMENT | FAILED CONTENT TRANSFER PREVENTION

[Withdrawn: Not applicable to COV.]

(32) INFORMATION FLOW ENFORCEMENT | PROCESS REQUIREMENTS FOR INFORMATION TRANSFER

[Withdrawn: Not applicable to COV.]

AC-5 SEPARATION OF DUTIES

Control:

a. Identify and document separation of duties of individuals; and

b. Define system access authorizations to support separation of duties.

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

Control Enhancements: None.

AC-6 LEAST PRIVILEGE

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Authorize access for organization-defined individuals or roles to:

(a) Organization-defined security functions (deployed in hardware, software, and firmware); and

(b) Organization-defined security-relevant information.

Discussion: Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Require that users of system accounts (or roles) with access to organization-defined security functions or security-relevant information use non-privileged accounts or roles, when accessing nonsecurity functions.

Discussion: Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Related Controls: AC-17, AC-18, AC-19, PL-4.

(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

[Withdrawn: Not applicable to COV.]

(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS

[Withdrawn: Not applicable to COV.]

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Restrict privileged accounts on the system to administrative personnel.

Discussion: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls: IA-2, MA-3, MA-4.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

Prohibit privileged access to the system by non-organizational users or individuals not under the contractual control of the Commonwealth.

Discussion: An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policies and procedures for

granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.

Related Controls: AC-18, AC-19, IA-2, IA-8.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

(a) Review on an annual basis the privileges assigned to all users to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Discussion: The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls: CA-7.

(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION

[Withdrawn: Not applicable to COV.]

(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS

Log the execution of privileged functions.

Discussion: The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls: AU-2, AU-3, AU-12.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Prevent non-privileged users from executing privileged functions.

Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

Related Controls: None.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

a. Enforce a limit of 5 consecutive invalid logon attempts by a user during a 15 minute period; and

b. Automatically locks the account or node for a minimum of a 30 minute period or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts

initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related Controls: AC-2, AC-9, AU-2, AU-6, IA-5.

Control Enhancements:

(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK

[Withdrawn: Incorporated into AC-7.]

(2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE OR WIPE MOBILE DEVICE

Purge or wipe information from mobile devices based on organization-defined purging or wiping requirements and techniques after 10 consecutive, unsuccessful device logon attempts.

Discussion: A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

Related Controls: AC-19, MP-5, MP-6.

(3) UNSUCCESSFUL LOGON ATTEMPTS | BIOMETRIC ATTEMPT LIMITING

Limit the number of unsuccessful biometric logon attempts to 5.

Discussion: Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts for users based on organizationally-defined factors.

Related Controls: IA-3.

(4) UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR

(a) Allow the use of organization-defined authentication factors that are different from the primary authentication factors after the number of organization- defined consecutive invalid logon attempts have been exceeded; and

(b) Enforce a limit of 5 consecutive invalid logon attempts through use of the alternative factors by a user during a 15 minute period.

Discussion: The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.

Related Controls: IA-3.

AC-8 SYSTEM USE NOTIFICATION

Control:

a. Display organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and states that:

   1. Users are accessing a system;
   2. System usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
   4. Use of the system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

   1. Display system use information, before granting further access to the publicly accessible system;
   2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Include a description of the authorized uses of the system.

Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Related Controls: AC-14, PL-4, SI-4.

Control Enhancements: None.

AC-8-COV

Control: Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

AC-9 PREVIOUS LOGON NOTIFICATION

[Withdrawn: Not applicable to COV.]

AC-10 CONCURRENT SESSION CONTROL

Control: Limit the number of concurrent sessions for each server and database administrative account to 5.

Discussion: Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

Related Controls: SC-23.

Control Enhancements: None.

AC-11 DEVICE LOCK

Control:

a. Prevent further access to the system by initiating a device lock after 15 minutes of inactivity or upon receiving a request from a user; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11, PL-4.

Control Enhancements:

(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Related Controls: None.

AC-12 SESSION TERMINATION

Control: Automatically terminate a user session after 24 hours ~~of inactivity~~.

Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the

session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related controls: MA-4, SC-10, SC-23.

Control Enhancements:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to information resources.

Discussion: Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.

Related Controls: None.

(2) SESSION TERMINATION | TERMINATION MESSAGE

Display an explicit logout message to users indicating the termination of authenticated communications sessions.

Discussion: Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

Related Controls: None.

(3) SESSION TERMINATION | TIMEOUT WARNING MESSAGE

[Withdrawn: Not applicable to COV.]

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6.]

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control:

a. Identify organization-defined user actions that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Discussion: Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be “none.”

Related Controls: AC-8, IA-2, PL-2.

Control Enhancements: None.

(1) PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES

[Withdrawn: Incorporated into AC-14.]

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3.]

AC-16 SECURITY AND PRIVACY ATTRIBUTES

[Withdrawn: Not applicable to COV.]

AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize remote access to the system prior to allowing such connections.

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-2, AU-6, AU-12, AU-14.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related Controls: SC-8, SC-12, SC-13.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

Route all remote accesses through authorized and managed network access control points.

Discussion: Organizations consider the Trusted Internet Connections (TIC) initiative [DHS TIC] requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Related Controls: SC-7.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for organization-defined needs; and

(b) Document the rationale for remote access in the security plan for the system.

Discussion: Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related Controls: AC-6, SC-12, SC-13.

(5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4.]

(6) REMOTE ACCESS | PROTECTION OF MECHANISM INFORMATION

Protect information about remote access mechanisms from unauthorized use and disclosure.

Discussion: Remote access to organizational information by non-organizational entities can increase the risk of unauthorized use and disclosure about remote access mechanisms. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behavior (see PL-4) and access agreements (see PS-6).

Related Controls: AT-2, AT-3, PS-6.

(7) REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS

[Withdrawn: Incorporated into AC-3 (10).]

(8) REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS

[Withdrawn: Incorporated into CM-7.]

(9) REMOTE ACCESS | DISCONNECT OR DISABLE ACCESS

Provide the capability to disconnect or disable remote access to the system within 15 minutes.

Discussion: The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Related Controls: None.

(10) REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS

Implement organization-defined mechanisms to authenticate organization-defined remote commands.

Discussion: Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.

Related Controls: SC-12, SC-13, SC-23.

AC-17-COV

Control:

a. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling.

b. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of approved encryption.

c. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the Agency's remote access capabilities.

d. Document requirements for the physical and logical hardening of remote access devices.

e. Require maintenance of auditable records of all remote access.

f. Where supported by features of the system, session timeouts shall be implemented after a period of no longer than 15 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.

g. The organization ensures that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.

Discussion: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.

Related Controls: None.

Control Enhancements: None.

AC-18 WIRELESS ACCESS

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

Discussion: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

Protect wireless access to the system using authentication of users, devices, and encryption.

Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: SC-8, SC-12, SC-13.

(2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4.]

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: None.

(4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Discussion: Organizational authorizations to allow selected users to configure wireless networking capability are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

Related Controls: SC-7, SC-15.

(5) WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Discussion: Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Related Controls: PE-19.

AC-18-COV

Control: Each Information Security Officer is accountable for ensuring the following steps are followed and documented:

Wireless LAN (WLAN) Connectivity on the COV Network

a. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal Commonwealth of Virginia network.

    1. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);

2. WLAN infrastructure must authenticate *each* client device prior to permitting access to the WLAN;
3. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;
4. Only COV owned or leased equipment shall be granted access to an internal WLAN;
5. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
6. Physical or logical separation between WLAN and wired LAN segments must exist;
7. All COV WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;
8. WLAN clients will only permit infrastructure mode communication.

WLAN Hotspot (Wireless Internet)

b. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:
   1. WLAN Hotspots must have logical or physical separation from the agency's LAN;
   2. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;
   3. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and
   4. Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.

Wireless Bridging

c. The following network configuration shall be used when bridging two wired LANs:
   1. All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
   2. Wireless bridging devices will not have a default gateway configured;
   3. Wireless bridging devices must be physically or logically separated from other networks;
   4. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;
   5. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

Discussion: None.

Related Controls: None.

Control Enhancements: None.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

Control Enhancements:

(1) ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7.]

(2) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7.]

(3) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER

[Withdrawn: Incorporated into MP-7.]

(4) ACCESS CONTROL FOR MOBILE DEVICES | RESTRICT CONFIGURATIONS BY USERS

[Withdrawn: Not applicable to COV.]

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

Employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices.

Discussion: Container-based encryption provides a more fine-grained approach to the data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls: SC-12, SC-13, SC-28.

AC-20 USE OF EXTERNAL SYSTEMS

Control:

a. Establish terms and conditions, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

   1. Access the system from external systems; and

   2. Process, store, or transmit organization-controlled information using external systems.

b. Prohibit the use of organizationally-defined types of external systems.

Discussion: External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations.

Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Control Enhancements:

(1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Discussion: Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls: CA-2.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES – RESTRICTED USE

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organization-defined restrictions.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls: MP-7, SC-41.

(3) USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS – RESTRICTED USE

Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information.

Discussion: Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see AC-20 b.). In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include requiring the implementation of approved controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage.

Related Controls: None.

(4) USE OF EXTERNAL SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES – PROHIBITED USE

Prohibit the use of network accessible storage devices in external systems.

Discussion: Network accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.

Related Controls: None

(5) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES – PROHIBITED USE

Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.

Related Controls: MP-7, PL-4, PS-6, SC-41.

AC-20-COV

Control: Identify whether personal IT assets are allowed onto premises that house IT systems and data, and if so, identify the controls necessary to protect these IT systems and data.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

AC-21 INFORMATION SHARING

Control:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for organization-defined information sharing circumstances where user discretion is required; and

b. Employ organization-defined automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

Control Enhancements:

(1) INFORMATION SHARING | AUTOMATED DECISION SUPPORT

Employ organization-defined automated mechanisms to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

Discussion: Automated mechanisms are used to enforce information sharing decisions.
Related Controls: None.

(2) INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL

Implement information search and retrieval services that enforce organization-defined information sharing restrictions.

Discussion: Information search and retrieval services identify information system resources relevant to an information need.

Related Controls: None.

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information prior to initial posting, quarterly, and remove such information, if discovered.

Discussion: In accordance with applicable Commonwealth laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the [PRIVACT] and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non- organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Related Controls: AC-3, AT-2, AT-3, AU-13.

Control Enhancements: None.

AC-23 DATA MINING PROTECTION

[Withdrawn: Not applicable to COV.]

AC-24 ACCESS CONTROL DECISIONS

[Withdrawn: Not applicable to COV.]

AC-25 REFERENCE MONITOR

[Withdrawn: Not applicable to COV.]

8.2 AWARENESS AND TRAINING

AT-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to all system users (including managers, senior executives, and contractors):
    1. Organization-level awareness and training policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines; and
    2. Procedures to facilitate the implementation of the awareness and training policy and associated awareness and training controls;
b. Designate an ISO or ISO designee to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
c. Review and update the current awareness and training:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

AT-2 LITERACY TRAINING AND AWARENESS

Control:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
    1. As part of initial training for new users and annually thereafter; and
    2. When required by system changes or following organization-defined events;
b. Employ the following techniques to increase the security and privacy awareness of system users: web-based learning, classroom learning, exercises, simulation, case studies, or gamification;

c. Update literacy training and awareness content annually and following organization-defined events; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

Control Enhancements:

(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES

Provide practical exercises in literacy training that simulate events and incidents.

Discussion: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related Controls: CA-2, CA-7, CP-4, IR-3.

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

Related Controls: PM-12.

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks.

Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Related Controls: None.

(4) LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using as specified in SEC527.

Discussion: A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications.

Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Related Controls: None.

(5) LITERACY TRAINING AND AWARENESS | ADVANCED PERSISTENT THREAT

Provide literacy training on the advanced persistent threat.

Discussion: An effective way to detect advanced persistent threats (APT) and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.

Related Controls: None.

(6) LITERACY TRAINING AND AWARENESS | CYBER THREAT ENVIRONMENT

(a) Provide literacy training on the cyber threat environment; and

(b) Reflect current cyber threat information in system operations.

Discussion: Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.

Related Controls: RA-3.

AT-2-COV

Control:

a. Develop an information security training program that meets or exceeds all of the following core requirements:
    1. Separation of Duties;
    2. Identifying and Reporting Security Incidents;
    3. Proper disposal of Data Storage Media;
    4. Proper Use of Encryption;
    5. Access Controls, Secure Passwords;
    6. Working Remotely;
    7. Intellectual Property Rights;
    8. Security of Data;
    9. Phishing and Email;
    10. Social Engineering;
    11. Least Privilege;
    12. Privileged Access;
    13. Insider Threat;
    14. Cloud Services;
    15. Browsing Safely;
    16. Physical Security;
    17. Hacking;
    18. Personal Identifiable Information (PII);
    19. Privacy;
    20. Social Network;
    21. Mobile Devices;
    22. Malware; and
    23. Ethics;
b. Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training including, but not limited to the following:
    1. Acceptable Use Policy;
    2. Remote Access Policy; and
    3. Other Applicable Policies; and
c. Provide training for all regulatory or contractual requirements that affect IT users.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

AT-3 ROLE-BASED TRAINING

Control:

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: System Owner, Data Owner, System Administrator, Data Custodian, Information Security Officer, and Agency Head;

1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
2. When required by system changes;

b. Update role-based training content annually and following organization-defined events; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

Control Enhancements:

(1) ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS

[Withdrawn: Not applicable to COV.]

(2) ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS

[Withdrawn: Not applicable to COV.]

(3) ROLE-BASED TRAINING | PRACTICAL EXERCISES

Provide practical exercises in security and privacy training that reinforce training objectives.

Discussion: Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

Related Controls: None.

(4) ROLE-BASED TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

[Withdrawn: Moved to AT-2(4).]

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

Provide organization-defined personnel or roles with initial and organization-defined frequency training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion: Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, [PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Related Controls: PT-2, PT-3, PT-5, PT-6.

AT-4 TRAINING RECORDS

Control:

a. Document and monitor individual system security training activities, including security literacy training and specific role-based security training; and

b. Retain individual training records for three years as identified in the Library of Virginia Record Retention Schedules.

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The Library of Virginia provides guidance on records retention for Commonwealth agencies.

Related Controls: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Control Enhancements: None.

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15.]

AT-6 TRAINING FEEDBACK

Control: Provide feedback on organizational training results to the following personnel on an annual basis: Agency Head.

Discussion: Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. Therefore, it is important that senior managers are made aware of such situations so that they can take appropriate response actions. Training feedback supports the evaluation and update of organizational training described in AT-2b and AT-3b.

Related Controls: None.

Control Enhancements: None.

8.3 AUDIT AND ACCOUNTABILITY

AU-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to all organization personnel, contractors, and service providers with a responsibility to implement audit and accountability controls:
    1. Organization-level audit and accountability policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls;
b. Designated Information Security Officer to manage the development, documentations, and dissemination of the audit and accountability policy and procedures; and
c. Review and update the current audit and accountability:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

AU-2 EVENT LOGGING

Control:

a. Identify the types of events the system is capable of logging in support of the audit function: please see the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management;
b. Coordinates the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging with the system: please see the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management;

d. Provides a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging on an annual basis and following an environmental change.

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

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization.

Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Control Enhancements:

(1) *EVENT LOGGING* ~~AUDIT EVENTS~~ | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

[Withdrawn: Incorporated into AU-12.]

(2) *EVENT LOGGING* ~~AUDIT EVENTS~~ | SELECTION OF AUDIT EVENTS BY COMPONENT

[Withdrawn: Incorporated into AU-12.]

(3) *EVENT LOGGING* ~~AUDIT EVENTS~~ | REVIEWS AND UPDATES

[Withdrawn: Incorporated into AU-2.]

(4) *EVENT LOGGING* ~~AUDIT EVENTS~~ | PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6(9).]

AU-3 CONTENT OF AUDIT RECORDS

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

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

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

Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Generate audit records containing the following additional information: please see the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management**.**

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

Related Controls: None.

(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

[Withdrawn: Incorporated into PL-9.]

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Withdrawn: Not applicable to COV.]

AU-4 AUDIT LOG STORAGE CAPACITY

Control: Allocate audit log storage capacity to accommodate the retention requirements identified in the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management.

Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Control Enhancements:

(1) AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

Transfer audit logs at least once every 30-days to a different system, system component, or media other than the system or system component conducting the logging.

Discussion: Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU- 9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.

Related Controls: None.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Control:

a. Alert designated organizational officials in near real-time in the event of an audit logging process failure; and

b. Take the following additional actions: investigate the cause of the disruption, take appropriate corrective actions, and shall escalate and report disruptions.

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Control Enhancements:

(1) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | STORAGE CAPACITY WARNING

[Withdrawn: Not applicable to COV.]

(2) RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS

Provide an alert within 15 minutes to appropriate personnel, to include information security personnel, system owner, and business owner when the following audit failure events occur: failure of any audit log types identified in the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management.

Discussion: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Related Controls: None.

(3) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

[Withdrawn: Not applicable to COV.]

(4) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | SHUTDOWN ON FAILURE

[Withdrawn: Not applicable to COV.]

(5) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | ALTERNATE AUDIT LOGGING CAPABILITY

[Withdrawn: Not applicable to COV.]

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Control:

a. Review and analyze system audit records at least every 30 days for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;

b. Reports findings to designated organizational officials; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

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

Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION

Integrate audit record review, analysis, and reporting processes using organization-defined automated mechanisms.

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

Related Controls: PM-7.

(2) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS

[Withdrawn: Incorporated into SI-4.]

(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

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

Related Controls: AU-12, IR-4.

(4) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

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

Related Controls: AU-2, AU-12.

(5) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS

Integrate analysis of audit records with analysis of vulnerability scanning information; performance data; system monitoring information to further enhance the ability to identify inappropriate or unusual activity.

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

Related Controls: AU-12, IR-4.

(6) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING

[Withdrawn: Not applicable to COV.]

(7) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS

Specify the permitted actions for each system process; role; and user associated with the review, analysis, and reporting of audit record information.

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

Related Controls: None

(8) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

[Withdrawn: Not applicable to COV.]

(9) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Discussion: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of

information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Related Controls: PM-12.

(10) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

[Withdrawn: Incorporated into AU-6.]

AU-7 AUDIT REDUCTION AND REPORT GENERATION

[Withdrawn: Not applicable to COV.]

AU-8 TIME STAMPS

Control:

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meets the organizational defined granularity of time measurement based on the sensitivity of the system and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g. clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls: AU-3, AU-12, AU-14, SC-45.

Control Enhancements:

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

[Withdrawn: Moved to SC-45(1).]

(2) TIME STAMPS | SECONDARY AUTHORIZATION TIME SOURCE

[Withdrawn: Moved to SC-45(2).]

AU-9 PROTECTION OF AUDIT INFORMATION

Control:

a. ~~1.~~ Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. ~~2.~~ Alert the Information Security Officer upon detection of unauthorized access, modification, or deletion of audit information.

Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related Controls: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Control Enhancements:

(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA

[Withdrawn: Not applicable to COV.]

(2) PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS

Store audit records at least once every 24 hours in a repository that is part of a physically different system or system component than the system or component being audited.

Discussion: Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Related Controls: AU-4, AU-5.

(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Not applicable to COV.]

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

Authorize access to management of audit functionality to only authorized administrators and security personnel.

Discussion: Individuals or roles with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls: AC-5.

(5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION

[Withdrawn: Not applicable to COV.]

(6) PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS

[Withdrawn: Not applicable to COV.]

(7) PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM

Store audit information on a component running a different operating system than the system or component being audited.

Discussion: Storing auditing information on a system component running a different operating system reduces the risk of a vulnerability specific to the system, resulting in a compromise of the audit records.

Related Controls: AU-4, AU-5, AU-11, SC-29.

AU-10 NON-REPUDIATION

[Withdrawn: Not applicable to COV.]

AU-11 AUDIT RECORD RETENTION

Control: Retain audit records for the retention schedule identified in the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management or the agency's records retention policy, whichever is more stringent, to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA_5, SI-12.

Control Enhancements:

(1) AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY

[Withdrawn: Not applicable to COV.]

AU-12 AUDIT RECORD GENERATION

Control:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on the operating system, services, applications, and network components;

b. Allow System Owner, Data Owner, or Information Security Officer to select event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion: Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

Control Enhancements:

(1) AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

Compile audit records from all systems and components into a system-wide (logical or physical) audit trail that is time-correlated to within 5 seconds COV authorized time server.

Discussion: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Related Controls: AU-8, SC-45.

(2) AUDIT RECORD GENERATION | STANDARDIZED FORMATS

Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Discussion: Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Related Controls: None.

(3) AUDIT RECORD GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

Provide and implement the capability for the Information Security Officer or designee to change the logging to be performed on all systems and components based on organization-defined selectable event criteria within organization-defined time thresholds.

Discussion: Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

Related Controls: AC-3.

(4) AUDIT RECORD GENERATION | QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION

[Withdrawn: Not applicable to COV.]

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control:

a. Monitor organization-defined open source information and/or information sites at the appropriate organization-defined frequency for evidence of unauthorized disclosure of organizational information; And

b. If an information disclosure is discovered:

   1. Notify the Information Security Officer; and

   2. Take the following additional actions: report to Commonwealth Security.

Discussion: Unauthorized disclosure of information is a form of data leakage. Open-source information includes social networking sites and code-sharing platforms and repositories. Examples of organizational information include personally identifiable information retained by the organization or proprietary information generated by the organization.

Related Controls: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

Control Enhancements:

(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS

[Withdrawn: Not applicable to COV.]

(2) MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES

[Withdrawn: Not applicable to COV.]

(3) MONITORING FOR INFORMATION DISCLOSURE | UNAUTHORIZED REPLICATION OF INFORMATION

[Withdrawn: Not applicable to COV.]

AU-14 SESSION AUDIT

[Withdrawn: Not applicable to COV.]

AU-15 ALTERNATE AUDIT CAPABILITY

[Withdrawn: Moved to AU-5(5).]

AU-16 CROSS-ORGANIZATIONAL AUDITING

[Withdrawn: Not applicable to COV.]

8.4 ASSESSMENT, AUTHORIZATION, AND MONITORING

CA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to authorized organization-defined personnel:
    1. Organization-level assessment, authorization, and monitoring policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and associated assessment, authorization, and monitoring controls;
b. Designate the Information Security Officer to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
c. Review and update the current assessment, authorization, and monitoring:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

CA-2 *CONTROL* ~~SECURITY~~ ASSESSMENTS

Control:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
b. Develop a control assessment plan that describes the scope of the assessment including:
    1. Controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation at least on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to the Information Security Officer and any other organization-defined individuals.

Discussion: Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-2.

Related Controls: AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

Control Enhancements:

(1) CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS

Employ independent assessors or assessment teams to conduct control assessments.

Discussion: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related Controls: None.

(2) CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS

[Withdrawn: Not applicable to COV.]

(3) CONTROL ASSESSMENTS | LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS

[Withdrawn: Not applicable to COV.]

CA-3 INFORMATION EXCHANGE

Control:

a. Approve and manage the exchange of information between the system and other systems using Interconnection Security Agreements; Memoranda of Understanding or Agreement; or Nondisclosure Agreements;

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreement on an annual basis and following an environmental change.

Discussion: System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications.

Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in CA-6(1) or CA-6(2), may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged. how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls: AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

Control Enhancements:

(1) *INFORMATION EXCHANGE* ~~SYSTEM CONNECTIONS~~ | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(25).]

(2) *INFORMATION EXCHANGE* ~~SYSTEM CONNECTIONS~~ | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(26).]

(3) *INFORMATION EXCHANGE* ~~SYSTEM CONNECTIONS~~ | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(27).]

(4) *INFORMATION EXCHANGE* ~~SYSTEM CONNECTIONS~~ | CONNECTIONS TO PUBLIC NETWORKS

[Withdrawn: Moved to SC-7(28).]

(5) *INFORMATION EXCHANGE* ~~SYSTEM CONNECTIONS~~ | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(5).]

(6) INFORMATION EXCHANGE | TRANSFER AUTHORIZATIONS

[Withdrawn: Not applicable to COV.]

(7) INFORMATION EXCHANGE | TRANSITIVE INFORMATION EXCHANGES

[Withdrawn: Not applicable to COV.]

CA-3-COV

Control: For every sensitive agency IT system that shares data with non-Commonwealth entities, the agency shall require or shall specify that its service provider require:

a. The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:
    1. The types of shared data;
    2. The direction(s) of data flow; and
    3. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.
b. The System Owners of interconnected systems must inform one another of connections with other systems.
c. The System Owners of interconnected systems must notify each other prior to establishing connections to other systems.
d. The written agreement shall specify if and how the shared data will be stored on each IT system.
e. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, including but not limited to, Data Breach requirements in this Standard.
f. The written agreement shall specify each Data Owner's authority to approve access to the shared data.
g. The System Owners shall approve and enforce the agreement.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2.]

CA-5 PLAN OF ACTION AND MILESTONES

Control:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
b. Update existing plan of action and milestones at least every 90 days based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

Control Enhancements:

(1) PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

[Withdrawn: Not applicable to COV.]

CA-6 AUTHORIZATION

Control:

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

   1. Accepts the use of common controls inherited by the system; and

   2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations on an annual basis and following an environmental change.

Discussion: Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. The authorization process is a federal responsibility, and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems.

Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls: CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.

Control Enhancements:

(1) AUTHORIZATION | JOINT AUTHORIZATION – INTRA-ORGANIZATION

[Withdrawn: Not applicable to COV.]

(2) AUTHORIZATION | JOINT AUTHORIZATION – INTER-ORGANIZATION

[Withdrawn: Not applicable to COV.]

CA-7 CONTINUOUS MONITORING

Control: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organizational-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: organization-defined system-level metrics;

b. Establishing organization-defined frequencies for monitoring and organization-defined frequencies for assessment control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy. Metrics include operating system scans on a monthly basis, database and web application scans on a monthly basis, and independent assessor scans performed annually;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessments and monitoring information; and

g. Reporting the security and privacy status of the system to appropriate organizational officials at least every 120 days.

Discussion: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM-31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, and SI-4.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

Control Enhancements:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

[Withdrawn: Not applicable to COV.]

(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into CA-2.]

(3) CONTINUOUS MONITORING | TREND ANALYSES

Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Discussion: Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the organization or the Federal Government, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving

social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from Inspectors General or auditors.

Related Controls: None.

(4) CONTINUOUS MONITORING | RISK MONITORING

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related Controls: None.

(5) CONTINUOUS MONITORING | CONSISTENCY ANALYSIS

[Withdrawn: Not applicable to COV.]

(6) CONTINUOUS MONITORING | AUTOMATION SUPPORT FOR MONITORING

Ensure the accuracy, currency, and availability of monitoring results for the system using organization-defined automated mechanisms.

Discussion: Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.

Related Controls: None.

CA-8 PENETRATION TESTING

Control: Conduct penetration testing on an annual basis and following an environmental change on any system housing Commonwealth data.

Discussion: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules

of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

Related Controls: RA-5, RA-10, SA-11, SR-5, SR-6.

Control Enhancements:

(1) PENETRATION TESTING | INDEPENDENT PENETRATION TESTING AGENT OR TEAM

[Withdrawn: Not applicable to COV.]

(2) PENETRATION TESTING | RED TEAM EXERCISES

[Withdrawn: Not applicable to COV.]

(3) PENETRATION TESTING | FACILITY PENETRATION TESTING

[Withdrawn: Not applicable to COV.]

CA-9 INTERNAL SYSTEM CONNECTIONS

Control:

a. Authorize internal connections of organization-defined system components or classes of components to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after organization-defined conditions; and

d. Review organization-defined frequency the continued need for each internal connection.

Discussion: Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

Control Enhancements:

(1) INTERNAL SYSTEM CONNECTIONS | COMPLIANCE CHECKS

Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

Discussion: Compliance checks include verification of the relevant baseline configuration.

Related Controls: CM-6.

8.5 CONFIGURATION MANAGEMENT

CM-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to all individuals providing system support and all system owners:
    1. Organization-level, mission/business process-level, and/or system-level configuration management policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
    2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designate an organization-defined official to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
c. Review and update the current configuration management:
    1. Policy on an annual basis and following an environmental change and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed.

Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SA-8, SI-12.

Control Enhancements: None.

CM-2 BASELINE CONFIGURATION

Control:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system:
    1. On an annual basis
    2. When required due to an environmental change; and

3. When system components are installed and upgraded.

Discussion: Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

Control Enhancements:

(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

[Withdrawn: Incorporated into CM-2.]

(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

[Withdrawn: Not applicable to COV.]

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

[Withdrawn: Not applicable to COV.]

(4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7(4).]

(5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7(5).]

(6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS

Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.

Discussion: Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility. Configurations in the test environment mirror configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. Separate baseline configurations do not necessarily require separate physical environments.

Related Controls: CM-4, SC-3, SC-7.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS

(a) Issue temporary computing devices with an enhanced security hardening configuration to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: refer to SEC514.

Discussion: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the

increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Related Controls: MP-4, MP-5.

CM-2-COV

Control:

a. The organization:
    1. Identifies, documents, and applies more restrictive security configurations for sensitive agency IT systems, as necessary;
    2. Maintains records that document the application of baseline security configurations;
    3. Monitors systems for security baselines and policy compliance;
    4. Reviews and revises all security configuration standards annually, or more frequently, as needed;
    5. Reapplies all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade; and
    6. Modifies individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning;
b. Requires creation and periodic review of a list of agency hardware and software assets;
c. The organization reviews and updates the baseline configuration of all information system:
    1. Once a year at a minimum;
    2. When required due to a significant configuration change or a demonstrated vulnerability; and
    3. As an integral part of information system component installations and upgrades;
d. All COV users traveling outside of the United States of America (including territories and military bases) must utilize a loaner device in accordance with the organization-defined process; and
e. Information Security Officers will verify the loaner devices that will be used for international travel meet the following controls:
    1. All operating system security updates, web browser software, Commonwealth Security and Risk Management security software, and any necessary application software have been installed;
    2. Infrared ports, Bluetooth ports, web cameras, and any hardware features, not needed for the trip, are disabled;
    3. If VPN is necessary, ensure it is installed and configured appropriately;
    4. All laptops and mobile telecommunications devices are encrypted, have sharing of all file and print services disabled, and have ad-hoc wireless connections disabled; and
    5. All required cables and power adapters are packed with the devices.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

CM-3 CONFIGURATION CHANGE CONTROL

Control:

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for a minimum of one year;

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through Change Control Board that convenes on a regular basis to review changes prior to implementation.

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Control Enhancements:

(1) CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES

[Withdrawn: Not applicable to COV.]

(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion: Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur

during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Related Controls: None.

(3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION

[Withdrawn: Not applicable to COV.]

(4) CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVE

Require an information security representative to be a members of the Change Control Board.

Discussion: Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3g.

Related Controls: None.

(5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

[Withdrawn: Not applicable to COV.]

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: Commonwealth Security and Risk Management approved key management services.

Discussion: The controls referenced in the control enhancement refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

Related Controls: SC-12.

(7) CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES

[Withdrawn: Not applicable to COV.]

(8) CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES

[Withdrawn: Not applicable to COV.]

CM-3-COV

Control: Each agency shall, or shall require that its service provider, document and implement configuration management and change control practices so that changes to the IT environment do not compromise security controls.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

CM-4 IMPACT ANALYSIS

Control: Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Discussion: Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required.

Related Controls: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2.

Control Enhancements:

(1) IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Discussion: A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

Related Controls: SA-11, SC-7.

(2) IMPACT ANALYSIS | VERIFICATION OF CONTROLS

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Discussion: Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related Controls: SA-11, SC-3, SI-6.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

Related Controls: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

Control Enhancements:

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS

(a) Enforce access restrictions using organization-defined automated mechanisms; and

(b) Automatically generate audit records of the enforcement actions.

Discussion: Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Related Controls: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

(2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES

[Withdrawn: Incorporated into CM-3(7).]

(3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS

[Withdrawn: Incorporated into CM-14.]

(4) ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION

[Withdrawn: Not applicable to COV.]

(5) ACCESS RESTRICTIONS FOR CHANGE | PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION

(a) Limit privileges to change system components and system-related information within a production or operational environment; and

(b) Review and reevaluate privileges on a quarterly basis and following an environmental change.

Discussion: In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

Related Controls: AC-2.

(6) ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES

[Withdrawn: Not applicable to COV.]

(7) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS

[Withdrawn: Incorporated into SI-7.]

CM-6 CONFIGURATION SETTINGS

Control:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization defined hardening standards;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for system components based on operational requirements; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are

parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Control Enhancements:

(1) CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION

[Withdrawn: Not applicable to COV.]

(2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

[Withdrawn: Not applicable to COV.]

(3) CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION

[Withdrawn: Incorporated into SI-7.]

(4) CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION

[Withdrawn: Incorporated into CM-4.]

CM-7 LEAST FUNCTIONALITY

Control:

a. Configure the system to provide only mission essential capabilities; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services that are not required for the business function of the system.

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least

functionality can also be achieved as part of the fundamental design and development of the system (see SA- 8, SC-2, and SC-3).

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC- 2, SC-3, SC-7, SC-37, SI-4.

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

(a) Review the system on a monthly basis or more frequently if required to address an environmental change to identify unnecessary and/or non-secure functions, ports, protocols, software, and services; and

(b) Disable or remove functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or non-secure.

Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls: AC-18.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

[Withdrawn: Not applicable to COV.]

(3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE

[Withdrawn: Not applicable to COV.]

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE – DENY-BY-EXCEPTION

[Withdrawn: Not applicable to COV.]

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE – ALLOWED-BY-EXCEPTION

[Withdrawn: Not applicable to COV.]

(6) LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: organization-defined user- installed software.

Discussion: Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Related Controls: CM-11, SC-44.

(7) LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of Information Security Officer when such code is:

(a) Obtained from sources with limited or no warranty; and/or

(b) Without the provision of source code.

Discussion: Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.

Related Controls: CM-10, SC-44.

(8) LEAST FUNCTIONALITY | BINARY OR MACHINE EXECUTABLE CODE

(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and

(b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.

Discussion: Binary or machine executable code applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.

Related Controls: SA-5, SA-22.

(9) LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE

(a) Identify through the Commonwealth of Virginia Technology Roadmaps the hardware components authorized for system use;

(b) Prohibit the use or connection of unauthorized hardware components;

(c) Review and update the list of authorized hardware components at least on a monthly basis.

Discussion: Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security.

Related Controls: None.

CM-8 SYSTEM COMPONENT INVENTORY

Control:

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;
2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes organization-defined information deemed necessary to achieve effective system component accountability; and

b. Review and update the system component inventory on an annual basis and following an environmental change.

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized

system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6).

Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-8(7) can help to eliminate duplicate accounting of components.

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL- 9, PM-5, SA-4, SA-5, SI-2, SR-4.

Control Enhancements:

(1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL

Update the inventory of system components as part of component installations, removals, and system updates.

Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Related Controls: PM-16.

(2) SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

[Withdrawn: Not applicable to COV.]

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

[Withdrawn: Not applicable to COV.]

(4) SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

Include in the system component inventory information, a means for identifying by name, position, and role, individuals responsible and accountable for administering those components.

Discussion: Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Related Controls: AC-3.

(5) SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

[Withdrawn: Incorporated into CM-8.]

(6) SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

Discussion: Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

Related Controls: None.

(7) SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY

Provide a centralized repository for the inventory of system components.

Discussion: Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.

Related Controls: None.

(8) SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING

[Withdrawn: Not applicable to COV.]

(9) SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS

(a) Assign system components to a system; and

(b) Receive an acknowledgement from the System Owner, Agency Information Technology Resource, or other organization-defined personnel or roles of this assignment.

Discussion: System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.

Related Controls: None.

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by Information Security Officer; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management

plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

Control Enhancements:

(1) CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY

Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Discussion: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Related Controls: None.

CM-10 SOFTWARE USAGE RESTRICTIONS

Control:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Discussion: Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related Controls: AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

Control Enhancements:

(1) SOFTWARE USAGE RESTRICTIONS | OPEN-SOURCE SOFTWARE

Establish the following restrictions on the use of open source software: the software must be actively maintained by the software community, cannot contain proprietary code, and must be distributed by a legitimate source.

Discussion: Open-source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open-source software is that it provides organizations with the ability to examine the source code. In some cases, there is an online community associated with the software that inspects, tests, updates, and reports on issues found in software on an ongoing basis. However, remediating vulnerabilities in open-source software may be problematic. There may also be licensing issues associated with open-source software, including the constraints on derivative use of such software.

Open-source software that is available only in binary form may increase the level of risk in using such software.

Related Controls: SI-7.

CM-11 USER-INSTALLED SOFTWARE

Control:

a. Establish organization-defined policies governing the installation of software by users;

b. Enforce software installation policies through organization-defined methods; and

c. Monitor policy compliance at least quarterly.

Discussion: If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved “app stores.” Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

Control Enhancements:

(1) USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS

[Withdrawn: Incorporated into CM-8(3).]

(2) USER-INSTALLED SOFTWARE | SOFTWARE INSTALLATION WITH PRIVILEGED STATUS

Allow user installation of software only with explicit privileged status.

Discussion: Privileged status can be obtained, for example, by serving in the role of system administrator.

Related Controls: AC-5, AC-6.

(3) USER-INSTALLED SOFTWARE | AUTOMATED ENFORCEMENT AND MONITORING

[Withdrawn: Not applicable to COV.]

CM-12 INFORMATION LOCATION

Control:

a. Identify and document the location of Commonwealth information and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Discussion: Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8, SA-17).

Related Controls: AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.

Control Enhancements:

(1) INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

[Withdrawn: Not applicable to COV.]

CM-13 DATA ACTION MAPPING

[Withdrawn: Not applicable to COV.]

CM-14 SIGNED COMPONENTS

Control: Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Related Controls: CM-7, SC-12, SC-13, SI-7.

8.6 CONTINGENCY PLANNING

CP-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel or roles:

   1. Organization-level, mission/business process-level, and/or system-level contingency planning policy that:

      a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

b. Designate an organization-defined official to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

   1. Policy on an annual basis and following an environmental change; and

   2. Procedures on an annual basis and following an environmental change.

Discussion: Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

CP-1-COV-1

Control: Each agency shall:

a. Designate an employee to collaborate with the agency Continuity Plan (CP) coordinator as the focal point for IT aspects of CONTINUITY PLAN and related Disaster Recovery (DR) planning activities.

   Note: Designation of an agency CONTINUITY PLAN coordinator is included in the CONTINUITY PLAN planning requirements issued by VDEM.

b. Based on BIA and RA results, develop IT disaster components of the agency CONTINUITY PLAN which identifies:

1. Each IT system that is necessary to recover agency business functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and
2. Personnel contact information and incident notification procedures.

   Note: If the CONTINUITY PLAN contains sensitive data, those components with sensitive data should be protected and stored at a secure off-site location.

c. Require an annual exercise (or more often as necessary) of IT DR components to assess their adequacy and effectiveness.

d. Require review and revision of IT DR components following the exercise (and at other times as necessary).

Discussion: None.

Related Controls: None.

Control Enhancements: None.

CP-1-COV-2

Control: Each agency shall:

a. Based on the CONTINUITY PLAN, develop and maintain an IT DRP, which supports the restoration of mission essential functions and dependent business functions.

b. Require approval of the IT DRP by the Agency Head.

c. Require at least on an annual basis a review, reassessment, testing, and revision of the IT DRP to reflect changes in mission essential functions, services, IT system hardware and software, and personnel.

d. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

CP-2 CONTINGENCY PLAN

Control:

a. Develop a contingency plan for the system that:
   1. Identifies essential mission and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   6. Addresses the sharing of contingency information; and
   7. Is reviewed and approved by the Information Security Officer;

b. Distribute copies of the contingency plan to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system on an annual basis or more frequently if required to address an environmental change;

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements;

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

(2) CONTINGENCY PLAN | CAPACITY PLANNING

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Discussion: Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in

a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related Controls: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS

Plan for the resumption of essential mission and business functions within the organization-defined time period of contingency plan activation.

Discussion: Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls: None.

(4) CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS

[Withdrawn: Incorporated into CP-2(3).]

(5) CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS

Plan for the continuance of essential mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Discussion: Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

(6) CONTINGENCY PLAN | ALTERNATE PROCESSING AND STORAGE SITES

Plan for the transfer of essential mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Discussion: Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

Coordinate its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Discussion: When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Related Controls: SA-9.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

Identify critical system assets supporting all mission and business functions.

Discussion: Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.

Related Controls: CM-8, RA-9.

CP-3 CONTINGENCY TRAINING

Control:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

   1. Within 30-days of assuming a contingency role or responsibility;

   2. When required by system changes; and

   3. Annually thereafter; and

b. Review and update contingency training content annually and following environmental change.

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Control Enhancements:

(1) CONTINGENCY TRAINING | SIMULATED EVENTS

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Discussion: The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that

encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Related Controls: None.

(2) CONTINGENCY TRAINING | MECHANISMS USED IN TRAINING ENVIRONMENTS

[Withdrawn: Not applicable to COV.]

CP-4 CONTINGENCY PLAN TESTING

Control:

a. Test the contingency plan for the system at least on an annual basis and following an environmental change using organization-defined tests to determine the effectiveness of the plan and the readiness to execute the plan;

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations.

Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion: Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related Controls: IR-8, PM-8.

(2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE

Test the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Discussion: Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

Related Controls: CP-7.

(3) CONTINGENCY PLAN TESTING | AUTOMATED TESTING

[Withdrawn: Not applicable to COV.]

(4) CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION

Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Related Controls: CP-10, SC-24.

(5) CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION

[Withdrawn: Not applicable to COV.]

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2.]

CP-6 ALTERNATE STORAGE SITE

Control:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE STORAGE SITE | RECOVERY TIME AND RECOVERY POINT OBJECTIVES

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Discussion: Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Related Controls: None.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls: RA-3.

CP-7 ALTERNATE PROCESSING SITE

Control:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of system operations for essential mission and business functions within the organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient

degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

Identify potential accessibility problems to the alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Discussion: Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related Controls: None.

(4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Discussion: Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

Related Controls: CM-2, CM-6, CP-4.

(5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS

[Withdrawn: Incorporated into CP-7].

(6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

Plan and prepare for circumstances that preclude returning to the primary processing site.

Discussion: There may be situations that preclude an organization from returning to the primary processing site such as if a natural disaster (e.g., flood or a hurricane) damaged or destroyed a facility and it was determined that rebuilding in the same location was not prudent.

Related Controls: None.

CP-8 TELECOMMUNICATIONS SERVICES

Control: Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within 24 hours when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion: Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may

specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, CP-11, SC-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Discussion: Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

Related Controls: None.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion: In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related Controls: None.

(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Discussion: Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Related Controls: None.

(4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN

(a) Require primary and alternate telecommunications service providers to have contingency plans;

(b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtain evidence of contingency testing and training by providers on a frequency defined by the organization.

Discussion: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related Controls: CP-3, CP-4.

(5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING

[Withdrawn: Not applicable to COV.]

CP-9 SYSTEM BACKUP

Control:

a. Conduct backups of user-level information contained in the system within the organization-defined frequency consistent with recovery time and recovery point objectives;

b. Conducts backup of system-level information contained in the information system in accordance with organization-defined frequency consistent with recovery time and recovery point objectives;

c. Conduct backups of system documentation including security- and privacy-related documentation in accordance with organization-defined frequency consistent with recovery time and recovery point objectives; and

d. Protect the confidentiality, integrity, and availability of backup information.

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

Control Enhancements:

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

Test backup information at least every 30-days to verify media reliability and information integrity.

Discussion: Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of

backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls: CP-4.

(2) SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Discussion: Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended.

Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

Related Controls: CP-4.

(3) SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

Store backup copies of critical system software and other security-related information in a separate facility or in a fire rated container that is not collocated with the operational system.

Discussion: Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers.

Related Controls: CM-2, CM-6, CM-8.

(4) SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION

[Withdrawn: Incorporated into CP-9].

(5) SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE

Transfer system backup information to the alternate storage site at least on a daily basis or sooner based on organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives.

Discussion: System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

Related Controls: CP-7, MP-3, MP-4, MP-5.

(6) SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Discussion: The effect of system backup can be achieved by maintaining a redundant secondary system that mirrors the primary system, including the replication of information. If this type of redundancy is in place and there is sufficient geographic separation between the two systems, the secondary system can also serve as the alternate processing site.

Related Controls: CP-7.

(7) SYSTEM BACKUP | DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION

[Withdrawn: Not applicable to COV]

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of sensitive backup information.

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

CP-9-COV

Control: For every IT system identified as sensitive relative to availability, each agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, data and applications in accordance with agency requirements. At a minimum, these plans shall address the following:

a. Secure off-site storage for backup media.

b. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.

c. Performance of backups only by authorized personnel.

d. Review of backup logs after the completion of each backup job to verify successful completion.

e. Approval of backup schedules of a system by the System Owner.

f. Approval of emergency backup and operations restoration plans by the System Owner.

g. Protection of any backup media that is sent off-site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with agency requirements.

h. Authorization and logging of deposits and withdrawals of all media that is stored off-site.

i. Retention of the data handled by an IT system in accordance with the agency's records retention policy.

j. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.

k. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.

l. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with the agency's Continuity Plan.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

Control: Provide for the recovery and reconstitution of the system to a known state within organization-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Control Enhancements:

(1) SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING

[Withdrawn: Incorporated into CP-4.]

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

Implement transaction recovery for systems that are transaction-based.

Discussion: Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Related Controls: None.

(3) SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS

[Withdrawn: Addressed through tailoring.]

(4) SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD

Provide the capability to restore system components within the organization-defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Discussion: Restoration of system components includes reimaging, which restores the components to known, operational states.

Related Controls: CM-2, CM-6.

(5) SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY

[Withdrawn: Incorporated into SI-13].

(6) SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION

Protect system components used for recovery and reconstitution.

Discussion: Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers, and other system software.

Related Controls: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: Provide the capability to employ organization-defined alternative communications protocols in support of maintaining continuity of operations.

Discussion: Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

Related Controls: CP-2, CP-8, CP-13.

Control Enhancements: None.

CP-12 SAFE MODE

[Withdrawn: Not applicable to COV.]

CP-13 ALTERNATIVE SECURITY MECHANISMS

[Withdrawn: Not applicable to COV]

8.7 IDENTIFICATION AND AUTHENTICATION

IA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level, mission/business process-level, and/or system-level configuration management policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable law, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;
b. Designate an Information Security Officer to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and
c. Review and update the current identification and authentication:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AC-1, PM-9, PS-8, SI-12.

Control Enhancements: None.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [HSPD 12]. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

Related Controls: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA- 5, PE-2, PL-4, SA-4, SA-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

Implement multi-factor authentication for access to privileged accounts.

Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5, AC-6.

(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

[Withdrawn: Not applicable to COV.]

(3) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS

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

(4) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

[Withdrawn: Incorporated into IA-2(2).]

(5) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Discussion: Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

Related Controls: None.

(6) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS – SEPARATE DEVICE

Implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets organization-defined strength of mechanism requirements.

Discussion: The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

Related Controls: AC-6.

(7) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS – SEPARATE DEVICE

[Withdrawn: Incorporated into IA-2(6).]

(8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS – REPLAY RESISTANT

Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

Discussion: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Related Controls: None.

(9) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS – REPLAY RESISTANT

[Withdrawn: Incorporated into IA-2(8).]

(10) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON

Provide a single sign-on capability for organization-defined system accounts and services.

Discussion: Single sign-on enables users to log in once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add multi-factor authentication for applications and systems (existing and new) that may not be able to natively support multi-factor authentication.

Related Controls: None.

(11) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS – SEPARATE DEVICE

[Withdrawn: Incorporated into IA-2(6).]

(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS

[Withdrawn: Not applicable to COV.]

(13) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | OUT-OF-BAND AUTHENTICATION

[Withdrawn: Not applicable to COV.]

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV.]

IA-4 IDENTIFIER MANAGEMENT

Control: Manage system identifiers by:

a. Receiving authorization from a designated organizational official to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for at least one year;

Discussion: Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Related Controls: AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS- 3, PS-4, PS-5, SC-37.

Control Enhancements:

(1) IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS

[Withdrawn: Not applicable to COV.]

(2) IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION

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

(3) IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION

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

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

[Withdrawn: Not applicable to COV.]

(5) IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT

[Withdrawn: Not applicable to COV.]

(6) IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT

[Withdrawn: Not applicable to COV.]

(7) IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION

[Withdrawn: Incorporated into IA-12(4).]

(8) IDENTIFIER MANAGEMENT | PAIRWISE PSEUDONYMOUS IDENTIFIERS

[Withdrawn: Not application to COV.]

(9) IDENTIFIER MANAGEMENT | ATTRIBUTE MAINTENANCE AND PROTECTION

Maintain the attributes for each uniquely identified individual, device, or service in organization-defined protected central storage.

Discussion: For each of the entities covered in IA-2, IA-3, IA-8, and IA-9, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.

Related Controls: None.

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators at least every 90 days and a minimum of 1 day or at least on an annual basis when multi-factor authentication occurs;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list at least on a quarterly basis and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) [Withdrawn: Not applicable to COV.]; and

(h) Enforce the following composition and complexity rules:

(1) When a password is the only authenticator:

(a) At least 14 characters in length;

(b) Utilize each of the following four:

(1) Special characters;

(2) Alphabetical characters;

(3) Numerical characters;

(4) Combination of upper case and lower case letters; and

(c) Prohibits password reuse for 24 generations.

(2) When used as a component of multi-factor authentication:

(a) At least 8 characters in length;

Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Related Controls: IA-6.

(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION

[Withdrawn: Not applicable to COV.]

(3) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION

[Withdrawn: Incorporated into IA-12(4).]

(4) AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

[Withdrawn: Incorporated into IA-5(1).]

(5) AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Discussion: Changing authenticators prior to the delivery and installation of system components extends the requirement for organizations to change default authenticators upon 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 developers of commercial off-the-shelf information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.

Related Controls: None.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Discussion: For systems that contain 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. Security categories of information are determined as part of the security categorization process.

Related Controls: RA-2.

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Discussion: In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when 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.

Related Controls: None.

(8) AUTHENTICATOR MANAGEMENT | MULTIPLE SYSTEM ACCOUNTS

Implement organization-defined security controls to manage the risk of compromise due to individuals having accounts on multiple systems.

Discussion: When individuals have accounts on multiple systems and use the same authenticators such as passwords, there is the risk that a compromise of one account may lead to the compromise of other accounts. Alternative approaches include having different authenticators (passwords) on all systems, employing a single sign-on or federation mechanism, or using some form of one-time passwords on all systems. Organizations can also use rules of behavior (see PL-4) and access agreements (see PS-6) to mitigate the risk of multiple system accounts.

Related Controls: PS-6.

(9) AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT

Use the following external organizations to federate credentials: Commonwealth Security and Risk Management approved external organizations.

Discussion: Federation provides organizations with the capability to authenticate individuals and devices when conducting cross-organization activities involving the processing, storage, or transmission of information. Using a specific list of approved external organizations for authentication helps to ensure that those organizations are vetted and trusted.

Related Controls: AU-7, AU-16.

(10) AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL BINDING

[Withdrawn: Not applicable to COV.]

(11) AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION

[Withdrawn: Incorporated into IA-2(1) and IA-2(2).]

(12) AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION PERFORMANCE

For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements as described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.

Discussion: Unlike password-based authentication, which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide exact matches. Depending on the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and the stored biometric that serves as the basis for comparison. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system.

Related Controls: AC-7.

(13) AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS

Prohibit the use of cached authenticators after organization-defined time period.

Discussion: Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.

Related Controls: None.

(14) AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES

For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.

Discussion: An organization-wide methodology for managing the content of PKI trust stores helps improve the accuracy and currency of PKI-based authentication credentials across the organization.

Related Controls: None.

(15) AUTHENTICATOR MANAGEMENT | GSA-APPROVED PRODUCTS AND SERVICES

[Withdrawn: Not applicable to COV.]

(16) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE

Require that the issuance of organization-defined types of and/or specific authenticators be conducted in person or by a trusted external party before organization-defined registration authority with authorization by organization-defined personnel or roles.

Discussion: Issuing authenticators in person or by a trusted external party enhances and reinforces the trustworthiness of the identity proofing process.

Related Controls: IA-12.

(17) AUTHENTICATOR MANAGEMENT | PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS

[Withdrawn: Not applicable to COV.]

(18) AUTHENTICATOR MANAGEMENT | PASSWORD MANAGERS

(a) Employ organization-defined password managers to generate and manage passwords; and

(b) Protect the passwords using organization-defined controls.

Discussion: For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords (see IA-5(1)(d)) and storing the collection offline in a token.

Related Controls: None.

IA-5-COV-1

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

a. Requiring passwords with a minimum of 6 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; and

g. Requiring that any authentication trust relation be structured such that the commonwealth's authentication mechanism is the only trusted source of information.

Discussion: None.

Related Controls: None.

Control Enhancements: 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:

a. Determine the appropriate validity period of the password, commensurate with sensitivity and risk;

b. Determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk; ~~and~~

c. 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~~;~~ *and*

d. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

IA-6 AUTHENTICATOR FEEDBACK

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Discussion: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Related Controls: AC-3.

Control Enhancements: None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Discussion: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13.

Control Enhancements: None.

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

Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Discussion: Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA- 3, SA-4, SC-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

[Withdrawn: Not applicable to COV.]

(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS

[Withdrawn: Incorporated into IA-8-COV.]

(3) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS

[Withdrawn: Incorporated into IA-8(2).]

(4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES

Conform to the following profiles for identity management as described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.

Discussion: Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the standards and technology implementations are assessed and scoped against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: None.

(5) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS

[Withdrawn: Not applicable to COV.]

(6) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | DISASSOCIABILITY

[Withdrawn: Not applicable to COV.]

IA-8-COV

a. Accept only external authenticators that are NIST-compliant; and

b. Document and maintain a list of accepted external authenticators.

Discussion: Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with [SP 800-63B]. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

Related Controls: None.

Control Enhancements: None.

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: Uniquely identify and authenticate on system services and applications before establishing communications with devices, users, or other services or applications.

Discussion: Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

Related Controls: IA-3, IA-4, IA-5, SC-8.

Control Enhancements:

(1) SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE

[Withdrawn: Incorporated into IA-9.]

(2) SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS

[Withdrawn: Incorporated into IA-9.]

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV.]

IA-11 RE-AUTHENTICATION

Control: Require users to re-authenticate when organization-defined circumstances or situations requiring re-authentication.

Discussion: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Related Controls: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

Control Enhancements: None.

IA-12 IDENTITY PROOFING

Control:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Discussion: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include [SP 800-63-3] and [SP 800-63A]. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Control Enhancements:

(1) IDENTITY PROOFING | SUPERVISOR AUTHORIZATION

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Discussion: Including supervisor or sponsor authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management chain is aware of the account, the account is essential to carry out organizational missions and functions, and the user's privileges are appropriate for the anticipated responsibilities and authorities within the organization.

Related Controls: None.

(2) IDENTITY PROOFING | IDENTITY EVIDENCE

Require evidence of individual identification be presented to the registration authority.

Discussion: Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

Related Controls: None.

(3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION

Require that the presented identity evidence be validated and verified through methods as described in the Enterprise Architecture Standard: Enterprise Solution Architecture: Identity Access Management.

Discussion: Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

Related Controls: None.

(4) IDENTITY PROOFING | IN-PERSON VALIDATION AND VERIFICATION

[Withdrawn: Not applicable to COV.]

(5) IDENTITY PROOFING | ADDRESS CONFIRMATION

Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Discussion: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

Related Controls: IA-12.

(6) IDENTITY PROOFING | ACCEPT EXTERNALLY-PROOFED IDENTITIES

Accept externally-proofed identities at organization-defined identity assurance level.

Discussion: To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and the identity assurance level appropriate for the system, application, or information accessed. Accepting externally-proofed identities is a fundamental component of managing federated identities across agencies and organizations.

Related Controls: IA-3, IA-4, IA-5, IA-8.

8.8 INCIDENT RESPONSE

IR-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level incident response policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls;
b. Designate the Information Security Officer to manage the development, documentation, and dissemination of the incident response policy and procedures; and
c. Review and update the current incident response:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

IR-1-COV

Control: The organization:

a. Shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following:
    1. Designate an individual responsible for the agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
    2. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
    3. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.
    4. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.

b. 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:

    1. Designate individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.
    2. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.
    3. Prohibit the installation or use of unauthorized monitoring devices.
    4. 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.

c. 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:

    1. Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.
    2. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.
    3. Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks and zero-day exploits.
    4. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

IR-2 INCIDENT RESPONSE TRAINING

Control:

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

    1. Within 30 days of assuming an incident response role or responsibility or acquiring system access;
    2. When required by system changes; and
    3. Annually thereafter; and

b. Review and update incident response training content on an annual basis and following environmental change or security incident.

Discussion: Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3.

Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

Control Enhancements:

(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Discussion: Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

Related Controls: None.

(2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

[Withdrawn: Not applicable to COV]

(3) INCIDENT RESPONSE TRAINING | BREACH

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Discussion: For agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-2(1).

Related Controls: None.

IR-3 INCIDENT RESPONSE TESTING ~~AND EXERCISES~~

Control: Test the effectiveness of the incident response capability for the system on an annual basis and following an environmental change using organization-defined tests.

Discussion: Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Control Enhancements:

(1) INCIDENT RESPONSE TESTING | AUTOMATED TESTING

[Withdrawn: Not applicable to COV.]

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion: Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Related Controls: None.

(3) INCIDENT RESPONSE TESTING | CONTINUOUS IMPROVEMENT

Use qualitative and quantitative data from testing to:

(a) Determine the effectiveness of incident response processes;

(b) Continuously improve incident response processes; and

(c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Discussion: To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

Related Controls: None.

IR-4 INCIDENT HANDLING

Control:

a. Implement an incident handling capability for security incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Discussion: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL- 2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Support the incident handling process using organization-defined automated mechanisms.

Discussion: Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Related Controls: None.

(2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION

[Withdrawn: Not applicable to COV.]

(3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Identify organization-defined classes of incidents and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: organization-defined actions to take in response to classes of incidents.

Discussion: Classes of incidents include malfunctions due to design or implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system degradation, system shutdown, fall back to manual mode or activation of alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved for when systems are under attack. Organizations consider whether continuity of operations requirements during an incident conflict with the capability to automatically disable the system as specified as part of IR-4(5).

Related Controls: None.

(4) INCIDENT HANDLING | INFORMATION CORRELATION

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

Discussion: Sometimes, a threat event, such as a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Related Controls: None.

(5) INCIDENT HANDLING | AUTOMATIC DISABLING OF SYSTEM

Implement a configurable capability to automatically disable the system if organization-defined security violations are detected.

Discussion: Organizations consider whether the capability to automatically disable the system conflicts with continuity of operations requirements specified as part of CP-2 or IR-4(3). Security violations include cyber-attacks that have compromised the integrity of the system or exfiltrated organizational information and serious errors in software programs that could adversely impact organizational missions or functions or jeopardize the safety of individuals.

Related Controls: None.

(6) INCIDENT HANDLING | INSIDER THREATS

Implement an incident handling capability for incidents involving insider threats.

Discussion: Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.

Related Controls: None.

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

Coordinate an incident handling capability for insider threats that includes the following organizational entities that are included in detecting and preventing insider threats.

Discussion: Incident handling for insider threat incidents (e.g., preparation, detection and analysis, containment, eradication, and recovery) requires coordination among many organizational entities, including mission or business owners, system owners, human resources offices, procurement offices, personnel offices, physical security offices, senior agency information security officer, operations personnel, risk executive (function), senior agency official for privacy, and legal counsel. In addition, organizations may require external support from federal, state, and local law enforcement agencies.

Related Controls: None.

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

Coordinate 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.

Discussion: The coordination of incident information with external organizations—including mission or business partners, military or coalition partners, customers, and developers—can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and breaches that could potentially affect the organization's operations, assets, and individuals.

Related Controls: AU-16, PM-16.

(9) INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY

[Withdrawn: Not applicable to COV.]

(10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION

Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents can occur anywhere through or to the supply chain and include compromises or breaches that involve primary or sub-tier providers, information technology products, system components, development processes or personnel, and distribution processes or warehousing facilities. Organizations consider including processes for protecting and sharing incident information in information exchange agreements and their obligations for reporting incidents to government oversight bodies (e.g., Federal Acquisition Security Council).

Related Controls: CA-3, MA-2, SA-9, SR-8.

(11) INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization within eight hours.

Discussion: An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security and privacy engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity. Deployment can be virtual or physical.

An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

Related Controls: AT-3.

(12) INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS

Analyze malicious code and/or other residual artifacts remaining in the system after the incident.

Discussion: When conducted carefully in an isolated environment, analysis of malicious code and other residual artifacts of a security incident or breach can give the organization insight into adversary tactics, techniques, and procedures. It can also indicate the identity or some defining characteristics of the adversary. In addition, malicious code analysis can help the organization develop responses to future incidents.

Related Controls: None.

(13) INCIDENT HANDLING | BEHAVIOR ANALYSIS

Analyze anomalous or suspected adversarial behavior in or related to organization environments and resources.

Discussion: If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial tactics, techniques, and procedures. External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight.

Related Controls: None.

(14) INCIDENT HANDLING | SECURITY OPERATIONS CENTER

Establish and maintain a security operations center.

Discussion: A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization’s systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources.

These sources include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a

dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.

Related Controls: None.

(15) INCIDENT HANDLING | PUBLIC RELATIONS AND REPUTATION REPAIR

(a) Manage public relations associated with an incident; and

(b) Employ measures to repair the reputation of the organization.

Discussion: It is important for an organization to have a strategy in place for addressing incidents that have been brought to the attention of the general public, have cast the organization in a negative light, or have affected the organization's constituents (e.g., partners, customers). Such publicity can be extremely harmful to the organization and affect its ability to carry out its mission and business functions. Taking proactive steps to repair the organization's reputation is an essential aspect of reestablishing the trust and confidence of its constituents.

Related Controls: None.

IR-4-COV-1

Control:

a. 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.

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

Discussion: None.

Related Controls: None.

Control Enhancements: 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.

Each agency must document incidents and investigations in the Commonwealth's incident handling system.

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

Each agency shall:

a. 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.

    1. 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:

        a. Social security number;

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

c. 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;

d. Passport number; or

e. Military identification number;

2. 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:

a. 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

b. 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.

b. "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:

1. Five digits of a social security number; or

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

c. "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:

1. An individual's medical history; or

2. Mental or physical condition; or

3. Medical treatment or diagnosis; or

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

5. Other unique identifier.

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

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

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

e. 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 the following below. If an agency is unable to determine if an unauthorized release occurred a determination will be made by VITA.

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

2. Theft or loss of physical hardcopy; and

3. 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.).

f. 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.

g. 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.

h. 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.

i. 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.

j. Provide notification that consists of:

    1. A general description of what occurred and when;

    2. The type of Personal Information that was involved;

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

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

    5. 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.).

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

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

    2. Telephone Notice;

    3. Electronic notice; or

    4. 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:

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

        b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

        c. Notice to major statewide media.

l. 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.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

IR-5 INCIDENT MONITORING

Control: Track and document incidents.

Discussion: Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

Related Controls: AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT MONITORING | AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS

Track incidents and collect and analyze incident information using Commonwealth Security and Risk Management approved and integrated tools.

Discussion: Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

Related Controls: None.

IR-6 INCIDENT REPORTING

Control:

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

b. Report incident information to the Commonwealth Chief Information Security Officer.

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products. The COV CISO will forward the applicable incidents to the Fusion Center according to § 2.2-5514.

Related Controls: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

Report incidents using the Commonwealth Incident Reporting Form.

Discussion: The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Related Controls: IR-7.

(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS

Report system vulnerabilities associated with reported incidents to the Information Security Officer.

Discussion: Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials,

and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.

Related Controls: None.

(3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related Controls: SR-8.

IR-6-COV

Control:

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

b. Establish a process for reporting IT security incidents that complies to the § 2.2-5514 of the Code of Virginia and verify that the IT security incident has been recorded into the Commonwealth Security and Risk Management approved system within 24 hours;

c. Report information security incidents only through channels that have not been compromised; and

d. Provide Commonwealth Security and Risk Management at least on an annual basis or when personnel changes occur the emergency contact information for agency personnel that should be contacted for security incidents that occur outside of normal working hours.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

IR-7 INCIDENT RESPONSE ASSISTANCE

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

Discussion: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Related Controls: AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

Increase the availability of incident response related information and support using organization-defined automated mechanisms.

Discussion: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to

query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Related Controls: None.

(2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS

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

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

Discussion: External providers of a system protection capability include 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. It may be beneficial to have agreements in place with external providers to clarify the roles and responsibilities of each party before an incident occurs.

Related Controls: None.

IR-8 INCIDENT RESPONSE PLAN

Control:

a. Develop 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;
   8. Addresses the sharing of incident information;
   9. Is reviewed and approved by the Agency Head or designee and the Chief Information Security Officer annually; and
   10. Explicitly designates responsibility for incident response to the Information Security Officer and designees.
b. Distribute 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. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
d. Communicate incident response plan changes to the organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements; and
e. Protect the incident response plan from unauthorized disclosure and modification.

Discussion: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations

consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

Control Enhancements:

(1) INCIDENT RESPONSE PLAN | BREACHES

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

- **(a)** A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
- **(b)** An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
- **(c)** Identification of applicable privacy requirements.

Discussion: Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Related Controls: PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.

IR-9 INFORMATION SPILLAGE RESPONSE

[Withdrawn: Not applicable to COV.]

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

[Withdrawn: Moved to IR-4(11).]

8.9 MAINTENANCE

MA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization personnel or roles:
    1. Organization-level maintenance policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the maintenance policy and associated maintenance controls;
b. Designate an organization-defined personnel to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
c. Review and update the current maintenance:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

MA-2 CONTROLLED MAINTENANCE

Control:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
c. Require that the Information Security Officer or designee explicitly approves the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;

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

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

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

Control Enhancements:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2.]

(2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES

[Withdrawn: Not applicable to COV.]

MA-3 MAINTENANCE TOOLS

Control:

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools at least annually.

Discussion: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer- used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related Controls: MA-2, PE-16.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion: Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor’s website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or

the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Discussion: If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls: SI-3.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

Prevent the removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from Information Security Officer or designee explicitly authorizing removal of the equipment from the facility.

Discussion: Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls: MP-6.

(4) MAINTENANCE TOOLS | RESTRICTED TOOL USE

Restrict the use of maintenance tools to authorized personnel only.

Discussion: Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.

Related Controls: AC-3, AC-5, AC-6.

(5) MAINTENANCE TOOLS | EXECUTION WITH PRIVILEGE

Monitor the use of maintenance tools that execute with increased privilege.

Discussion: Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.

Related Controls: AC-3, AC-6.

(6) MAINTENANCE TOOLS | SOFTWARE UPDATES AND PATCHES

Inspect maintenance tools to ensure the latest software updates and patches are installed.

Discussion: Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.

Related Controls: AC-3, AC-6.

MA-4 NONLOCAL MAINTENANCE

Control:

a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

Discussion: Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls. [SP 800-63B] provides additional guidance on strong authentication and authenticators.

Related Controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

Control Enhancements:

(1) NONLOCAL MAINTENANCE | LOGGING AND REVIEW

(a) Log organization-define audit events for nonlocal maintenance and diagnostic sessions; and

(b) Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

Discussion: Audit logging for nonlocal maintenance is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-6, AU-12.

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

[Withdrawn: Incorporated into MA-1 and MA-4.]

(3) NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION

(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitizes the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

Discussion: Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related Controls: MP-6, SI-3, SI-7.

(4) NONLOCAL MAINTENANCE | AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS

Protect nonlocal maintenance sessions by:

(a) Employing organization-defined authenticators that are replay resistant; and

(b) Separating the maintenance sessions from other network sessions with the system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths.

Discussion: Communications paths can be logically separated using encryption.

Related Controls: None.

(5) NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS

(a) Require the approval of each nonlocal maintenance session by organization-defined personnel; and

(b) Notify the following personnel or roles of the date and time of planned nonlocal maintenance: organization-defined personnel or roles.

Discussion: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance is accomplished by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Related Controls: None.

(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

Implements the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: organization-defined cryptographic mechanisms.

Discussion: Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized access during remote maintenance sessions can result in a variety of hostile actions, including malicious code insertion, unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.

Related Controls: SC-8, SC-12, SC-13.

(7) NONLOCAL MAINTENANCE | DISCONNECT VERIFICATION

Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

Discussion: Verifying the termination of a connection once maintenance is completed ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.

Related Controls: AC-12.

MA-5 MAINTENANCE PERSONNEL

Control:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

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

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as

information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

Control Enhancements:

(1) MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

[Withdrawn: Not applicable to COV.]

(2) MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS

[Withdrawn: Not applicable to COV.]

(3) MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS

[Withdrawn: Not applicable to COV.]

(4) MAINTENANCE PERSONNEL | FOREIGN NATIONALS

[Withdrawn: Not applicable to COV.]

(5) MAINTENANCE PERSONNEL | NON-SYSTEM MAINTENANCE

[Withdrawn: Not applicable to COV.]

MA-5-COV

Control: The organization shall develop and publish a maintenance personnel policy that requires all system/service maintenance and support be performed by United States citizens or individuals with a valid H1B visa.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

MA-6 TIMELY MAINTENANCE

Control: Obtain maintenance support and/or spare parts for organization-defined business-critical information system components to resolve issues within the acceptable organization-defined time period of failure.

Discussion: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls: CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

Control Enhancements:

(1) TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE

Perform preventive maintenance on organization-defined information system components at the appropriate organization-defined time intervals to ensure that the business need is met.

Discussion: Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid or mitigate the consequences of equipment failures. Preventive

maintenance is designed to preserve and restore equipment reliability by replacing worn components before they fail. Methods of determining what preventive (or other) failure management policies to apply include original equipment manufacturer recommendations; statistical failure records; expert opinion; maintenance that has already been conducted on similar equipment; requirements of codes, laws, or regulations within a jurisdiction; or measured values and performance indications.

Related Controls: None.

(2) TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE

Perform predictive maintenance on information system components at least on an annual basis and following an environmental change.

Discussion: Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the objective of predicting the future trend of the equipment's condition. The predictive maintenance approach employs principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thus minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability.

Related Controls: None.

(3) TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

Transfer predictive maintenance data to a maintenance management system using organization-defined automated mechanisms.

Discussion: A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates the processing of equipment condition data to trigger maintenance planning, execution, and reporting.

Related Controls: None.

MA-7 FIELD MAINTENANCE

[Withdrawn: Not applicable to COV.]

8.10 MEDIA PROTECTION

MP-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization personnel or roles:
    1. Organization-level media protection policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
b. Designate an organization-defined personnel to manage the development, documentation, and dissemination of the media protection policy and procedures; and
c. Review and update the current media protection:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: 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:

a. Define protection of stored sensitive data as the responsibility of Data Owner.
b. 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. (Note: This type of exception is an agency level exception only and does not need to be approved by Commonwealth Security). The exception shall include following elements:
    1. The business or technical justification;

2. The scope, including quantification and duration (not to exceed one year) ;
3. A description of all associated risks;
4. Identification of controls to mitigate the risks, one of which must be encryption; and
5. Identification of any residual risks.

c. 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.

d. 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.

e. 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.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

MP-2 MEDIA ACCESS

Control: Restrict access to digital and non-digital media to only authorized individuals.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Related Controls: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.

Control Enhancements:

(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

Control:

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt organization-defined types of system media from marking if the media remain within organization-defined controlled areas.

Discussion: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-

digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002]. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: AC-16, CP-9, MP-5, PE-22, SI-12.

Control Enhancements: None.

MP-4 MEDIA STORAGE

Control:

a. Physically control and securely store digital and non-digital media within organization-defined controlled areas; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.

Control Enhancements:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

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

(2) MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS

[Withdrawn: Not applicable to COV.]

MP-5 MEDIA TRANSPORT

Control:

a. Protect and control digital and non-digital media during transport outside of controlled areas using FIPS 140-*3*~~2~~ validated encryption module for all digital media and a secured locked container for non-digital media;

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

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

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

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and

magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport.

Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining 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 system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

Control Enhancements:

(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

Employ an identified custodian during transport of system media outside of controlled areas.

Discussion: 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 if an unambiguous custodian is identified.

Related Controls: None.

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

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

MP-6 MEDIA SANITIZATION

Control:

a. Sanitize system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures; and

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

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, 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 that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

Control Enhancements:

(1) MEDIA SANITIZATION | REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY

Review, approve, track, document, and verify media sanitization and disposal actions.

Discussion: Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Related Controls: None.

(2) MEDIA SANITIZATION | EQUIPMENT TESTING

Test sanitization equipment and procedures at least on an annual basis and following an environmental change to ensure that the intended sanitization is being achieved.

Discussion: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

Related Controls: None.

(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: newly purchased or originating from a non-Commonwealth system.

Discussion: Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

Related Controls: None.

(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) MEDIA SANITIZATION | DUAL AUTHORIZATION

[Withdrawn: Not applicable to COV.]

(8) MEDIA SANITIZATION | REMOTE PURGING OR WIPING OF INFORMATION

[Withdrawn: Incorporated into MP-6-COV.]

MP-6-COV

Control: Purge or wipe information/data from all technology assets as authorized by the Information Security Officer, when the device is no longer controlled by the Commonwealth, or prior to disposal in accordance with SEC514.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

MP-7 MEDIA USE

Control:

a. Restrict the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security controls; And

b. Prohibit the use of portable storage devices in organization systems when such devices have no identifiable owner.

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of 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 or 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 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, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls: AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

Control Enhancements:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

[Withdrawn: Incorporated into MP-7.]

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

Prohibit the use of sanitization-resistant media that do not have a secure erase function/feature/tool in organizational systems.

Discussion: Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media.

Certain types of media do not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media that do not have a secure erase function/feature/tool from their manufacturer.

Related Controls: MP-6.

MP-8 MEDIA DOWNGRADING

[Withdrawn: Not applicable to COV.]

8.11 PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level physical and environmental protection policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable law, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;
b. Designate an organization-defined official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
c. Review and update the current physical and environmental protection:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AT-3, PM-9, PS-8, SI-12.

Control Enhancements: None.

PE-1-COV

Control:

a. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.
b. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.
c. All data centers must meet the requirements of a Tier III data center as defined by the Uptime Institute.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals on an annual basis and following an environmental change; and

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

Discussion: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Related Controls: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

Control Enhancements:

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

Authorize physical access to the facility where the system resides based on position or role.

Discussion: Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.

Related Controls: AC-2, AC-3, AC-6.

(2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION

[Withdrawn: Not applicable to COV.]

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

Restrict unescorted access to the facility where the 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;

Discussion: Individuals without required security clearances, access approvals, or need to know are escorted by individuals with appropriate physical access authorizations to ensure that information is not exposed or otherwise compromised.

Related Controls: PS-2, PS-6.

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.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

PE-3 PHYSICAL ACCESS CONTROL

Control:

a. Enforce physical access authorizations at all physical access points including organization-defined entry/exit points to the facility where the system resides by;

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using organization-defined physical access control systems or devices; guards;

b. Maintain physical access audit logs for all organization-defined entry or exit points;

c. Control access to areas within the facility designated as publicly accessible by implementing the organization-defined physical access controls;

d. Escort visitors and control visitor activity for organization-defined circumstances requiring visitor escorts and control of visitor activity;

e. Secure keys, combinations, and other physical access devices;

f. Inventory organization-defined physical access devices on an annual basis or more frequently if required and following an environmental change; and

g. [Withdrawn: Not applicable to COV.]

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas.

Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related Controls: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

Control Enhancements:

(1) PHYSICAL ACCESS CONTROL | SYSTEM ACCESS

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

Discussion: Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related Controls: None.

(2) PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS

Perform security checks every 30 days and following an environmental change at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

Discussion: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Related Controls: AC-4, SC-7.

(3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS

[Withdrawn: Not applicable to COV.]

(4) PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS

[Withdrawn: Not applicable to COV.]

(5) PHYSICAL ACCESS CONTROL | TAMPER PROTECTION

[Withdrawn: Not applicable to COV.]

(6) PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING

[Withdrawn: Incorporated into CA-8.]

(7) PHYSICAL ACCESS CONTROL | PHYSICAL BARRIERS

[Withdrawn: Not applicable to COV.]

(8) PHYSICAL ACCESS CONTROL | ACCESS CONTROL VESTIBULES

[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).

Discussion: None.

Related Controls: None.

Control Enhancements: None.

PE-4 ACCESS CONTROL FOR TRANSMISSION

Control: Control physical access to cabling within organizational facilities using the appropriate organization-defined security controls.

Discussion: Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Control Enhancements: None.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

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

Discussion: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored

by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements:

(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS

[Withdrawn: Incorporated into PE-5.]

(2) ACCESS CONTROL FOR OUTPUT DEVICES | LINK TO INDIVIDUAL IDENTITY

[Withdrawn: Not applicable to COV.]

(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES

[Withdrawn: Incorporated into PE-22.]

PE-6 MONITORING PHYSICAL ACCESS

Control:

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

b. Review physical access logs at least once every 30 days and upon occurrence of organization-defined events or potential indications of events; and

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

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related Controls: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Control Enhancements:

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

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion: Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Related Controls: None.

(2) MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES

[Withdrawn: Not applicable to COV.]

(3) MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE

[Withdrawn: Not applicable to COV.]

(4) MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS

Monitor physical access to the system in addition to the physical access monitoring of the facility at organization-defined physical spaces containing one or more components of the system.

Discussion: Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Related Controls: None.

PE-7 VISITOR CONTROL

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

PE-8 VISITOR ACCESS RECORDS

Control:

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

b. Reviews visitor access records at least once every 30 days; and

c. Report anomalies in visitor access records to Information Security Officer and organization-defined personnel.

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls: PE-2, PE-3, PE-6.

Control Enhancements:

(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW

[Withdrawn: Not applicable to COV.]

(2) VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS

[Withdrawn: Incorporated into PE-2.]

(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Withdrawn: Not applicable to COV.]

PE-9 POWER EQUIPMENT AND CABLING

Control: Protect power equipment and power cabling for the system from damage and destruction.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls: PE-4.

Control Enhancements:

(1) POWER EQUIPMENT AND CABLING | REDUNDANT CABLING

Employ redundant power cabling paths that are physically separated by organization-defined distance.

Discussion: Physically separate and redundant power cables ensure that power continues to flow in the event that one of the cables is cut or otherwise damaged.

Related Controls: None.

(2) POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS

Employ automatic voltage controls for organization-defined critical system components.

Discussion: Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.

Related Controls: None.

PE-10 EMERGENCY SHUTOFF

Control:

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

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

c. Protect emergency power shutoff capability from unauthorized activation.

Discussion: Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls: PE-15.

Control Enhancements:

(1) EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION

[Withdrawn: Incorporated into PE-10.]

PE-11 EMERGENCY POWER

Control: Provide an uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY POWER | ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY

Provide an alternate power supply for the system that is activated manually and automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Discussion: Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Related Controls: None.

(2) EMERGENCY POWER | ALTERNATE POWER SUPPLY —SELF-CONTAINED

Provide an alternate power supply for the system that is activated manually and automatically and that is:

(a) Self-contained;

(b) Not reliant on external power generation; and

(c) Capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Discussion: The provision of a long-term, self-contained power supply can be satisfied by using one or more generators with sufficient capacity to meet the needs of the organization.

Related Controls: None.

PE-12 EMERGENCY LIGHTING

[Withdrawn: Not applicable to COV.]

PE-13 FIRE PROTECTION

Control: Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Related Controls: AT-3.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION DEVICES – AUTOMATIC ACTIVATION AND NOTIFICATION

Employ fire detection systems that activate automatically and notify the appropriate organization-defined personnel or roles and organization-defined emergency responders in the event of a fire.

Discussion: Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

(2) FIRE PROTECTION | SUPPRESSION DEVICES – AUTOMATIC ACTIVATION AND NOTIFICATION

(a) Employ fire suppression systems that activate automatically and notify organization-defined personnel or roles and organization-defined emergency responders; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

Discussion: Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

[Withdrawn: Incorporated into PE-13(2).]

(4) FIRE PROTECTION | INSPECTIONS

[Withdrawn: Not applicable to COV.]

PE-14 ENVIRONMENTAL CONTROLS

Control:

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

b. Monitor environmental control levels on a daily basis.

Discussion: The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related Controls: AT-3, CP-2.

Control Enhancements:

(1) ENVIRONMENTAL CONTROLS | AUTOMATIC CONTROLS

Employ organization-defined automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system.

Discussion: The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.

Related Controls: None.

(2) ENVIRONMENTAL CONTROLS | MONITORING WITH ALARMS AND NOTIFICATIONS

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to organization-defined personnel or roles.

Discussion: The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

Related Controls: None.

PE-15 WATER DAMAGE PROTECTION

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of

master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls: AT-3, PE-10.

Control Enhancements:

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

Detect the presence of water near the system and alerts the appropriate organization-defined personnel using organization-defined automated mechanisms.

Discussion: Automated mechanisms include notification systems, water detection sensors, and alarms.

Related Controls: None.

PE-16 DELIVERY AND REMOVAL

Control:

a. Authorize and control organization-defined types of system components entering and exiting the facility; and

b. Maintain records of the system components.

Discussion: Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related Controls: CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

Control Enhancements: None.

PE-17 ALTERNATE WORK SITE

Control:

a. Determine and document the organization-defined alternate work sites allowed for use by employees;

b. Employ the following controls at alternate work sites: all equivalent controls of the primary site;

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls: AC-17, AC-18, CP-7.

Control Enhancements: None.

PE-18 LOCATION OF SYSTEM COMPONENTS

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

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points

where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Related Controls: CP-2, PE-5, PE-19, PE-20, RA-3.

Control Enhancements:

(1) LOCATION OF ~~INFORMATION~~ SYSTEM COMPONENTS | FACILITY SITE

[Withdrawn: Moved to PE-23.]

PE-18-COV

Control: The organization shall develop and publish a policy that requires all information system components such that:

a. All information system components and services remain within the United States.

b. All data and system information associated with the information system components and services remain within the Unites States.

c. All physical components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must be housed within approved storage locations and clearly marked.

d. All virtual components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must reside in hypervisors that are hardened to meet or exceed commonwealth security requirements for the guest VMs or data being processed or stored within the hypervisors control.

e. Each hypervisor can only host one tier of the application architecture and no hypervisor may host the application interface and the data storage component for any information system, even if the components in question do not interact within the same information system.

PE-19 INFORMATION LEAKAGE

[Withdrawn: Not applicable to COV.]

PE-20 ASSET MONITORING AND TRACKING

[Withdrawn: Not applicable to COV.]

PE-21 ELECTROMAGNETIC PULSE PROTECTION

[Withdrawn: Not applicable to COV.]

PE-22 COMPONENT MARKING

[Withdrawn: Not applicable to COV.]

PE-23 FACILITY LOCATION

Control:

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and

b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. The location of system components within the facility is addressed in PE-18.

Related Controls: CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

8.12 PLANNING

PL-1 POLICY AND PROCEDURES

Control: ~~The organization:~~

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level planning policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;
b. Designate an Information Security Officer to manage the development, documentation, and dissemination of the planning policy and procedures; and
c. Review and update the current planning:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

Control:

a. Develop security and privacy plans for the system that:
    1. Are consistent with the organization’s enterprise architecture;
    2. Explicitly define the constituent system component;
    3. Describe the operational context of the system in terms of mission and business processes;
    4. Identify the individuals that fulfill system roles and responsibilities;
    5. Identify the information types processed, stored, and transmitted by the system;
    6. Provide the security categorization of the system, including supporting rationale;

7. Describe any specific threats to the system that are of concern of the organization;
8. [Withdrawn: Not applicable to COV.];
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for the tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with organization-defined individuals or groups; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distribute copies of the plans and communicate subsequent changes to the plans to the System Owners and appropriate organization-defined personnel;

c. Review the plans at least on an annual basis and following an environmental change;

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Discussion: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). Section 2.1 describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations 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.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs

and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.

Control Enhancements:

(1) SYSTEM SECURITY AND PRIVACY PLANS | CONCEPT OF OPERATIONS

[Withdrawn: Incorporated into PL-7.]

(2) SYSTEM SECURITY AND PRIVACY PLANS | FUNCTIONAL ARCHITECTURE

[Withdrawn: Incorporated into PL-8.]

(3) SYSTEM SECURITY AND PRIVACY PLANS | PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

[Withdrawn: Incorporated into PL-2.]

PL-2-COV

Control:

a. 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:

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

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

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

c. Plan, document, and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2.]

PL-4 RULES OF BEHAVIOR

Control:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented 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 system;

c. Review and update the rules of behavior at least on an annual basis and following an environmental change; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

Discussion: Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate 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 individuals who receive information from federal 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 organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

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, SI-12.

Control Enhancements:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

Include in the rules of behavior, restrictions on:

(a) Use of social media, social networking sites, and external sites/applications;

(b) Posting organizational information on public websites; and

(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Discussion: Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Related Controls: AC-22, AU-13.

PL-4-COV

Control:

a. 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.

b. Prohibit users from:

1. Installing or using proprietary encryption hardware/software on Commonwealth systems;
2. Tampering with security controls configured on COV workstations;
3. Installing personal software on a Commonwealth system;
4. Adding hardware to, removing hardware from, or modifying hardware on a COV system; and
5. 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).

c. 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.

d. 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.

Discussion: 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.

e. Prohibit the installation or use of software that may cause harm to the commonwealth as identified by Commonwealth Security and Risk Management.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into RA-8.]

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2.]

PL-7 CONCEPT OF OPERATIONS

[Withdrawn: Not applicable to COV.]

PL-8 SECURITY AND PRIVACY ARCHITECTURES

Control:

a. Develop security and privacy architecture for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. [Withdrawn: Not applicable to COV.];

3. Describe how the architectures are integrated into and support the enterprise architecture; and

4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures at least on an annual basis and following an environmental change to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Discussion: The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-7, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-8 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Related Controls: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

Control Enhancements:

(1) SECURITY AND PRIVACY ARCHITECTURES | DEFENSE IN DEPTH

Design the security and privacy architectures for the system using a defense-in-depth approach that:

(a) Allocates organization-defined controls to organization-defined locations and architectural layers; and

(b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

Discussion: Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defense-in-depth architectural approaches include modularity and layering (see SA-8(3)), separation of system and user functionality (see SC-2), and security function isolation (see SC-3).

Related Controls: SC-2, SC-3, SC-29, SC-36.

(2) SECURITY AND PRIVACY ARCHITECTURES | SUPPLIER DIVERSITY

Require that organization-defined controls allocated to organization-defined locations and architectural layers are obtained from different suppliers.

Discussion: Information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By deploying different products at different locations, there is an increased likelihood that at least one of the products will detect the malicious code. With respect to privacy, vendors may offer products that track personally identifiable information in systems. Products may use different tracking methods. Using multiple products may result in more assurance that personally identifiable information is inventoried.

Related Controls: SC-29, SR-3.

PL-9 CENTRAL MANAGEMENT

Control: Centrally manage organization-defined controls and related processes.

Discussion: Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.

As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-

3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

Related Controls: PL-8, PM-9.

Control Enhancements: None.

PL-10 BASELINE SELECTION

Control: Select a control baseline for the system.

Discussion: Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in [SP 800-53B]. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in [SP 800-53B] are based on the requirements from [FISMA] and [PRIVACT]. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. [CNSSI 1253] provides guidance on control baselines for national security systems.

Related Controls: PL-2, PL-11, RA-2, RA-3, SA-8.

Control Enhancements: None.

PL-11 BASELINE TAILORING

Control: Tailor the selected control baseline by applying specified tailoring actions.

Discussion: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in [SP 800-53B] can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in [SP 800-53B] in accordance with the security and privacy requirements from [FISMA], [PRIVACT], and [OMB A-130]. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in [SP 800-53B] to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related Controls: PL-10, RA-2, RA-3, RA-9, SA-8.

Control Enhancements: None.

8.13 PROGRAM MANAGEMENT

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control:

a. Develop and disseminate an organization-wide information security program plan that:
    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    3. Reflects the coordination among organizational entities responsible for information security; and
    4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
b. Review and update the organization-wide information security program plan at least on an annual basis and following an environmental or organizational change; and
c. Protect the information security program plan from unauthorized disclosure and modification.

Discussion: An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-2, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended.

Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or business process level, and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system.

Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

Control Enhancements: None.

PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

Control: Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Discussion: The senior agency information security officer is an organizational official. For Commonwealth agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or information security officer.

Related Controls: None.

Control Enhancements: None.

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

Control:

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

Discussion: Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

Related Controls: PM-4, SA-2.

Control Enhancements: None.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control:

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:

    1. Are developed and maintained;

    2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

    3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion: The plan of action and milestones is a key organizational document. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level.

While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-5.

Related Controls: CA-5, CA-7, PM-3, RA-7, SI-12.

Control Enhancements: None.

PM-5 SYSTEM INVENTORY

Control: Develop and update at least on an annual basis an inventory of organizational systems.

Discussion: System inventory refers to an organization-wide inventory of systems, not system components as described in CM-8.

Related Controls: None.

Control Enhancements:

(1) SYSTEM INVENTORY | INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Establish, maintain, and update at least on an annual basis an inventory of all systems, applications, and projects that process personally identifiable information.

Discussion: An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

Related Controls: AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

PM-6 MEASURES OF PERFORMANCE

Control: Develop, monitor, and report on the results of information security and privacy measures of performance.

Discussion: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.

Related Controls: CA-7, PM-9.

Control Enhancements: None.

PM-7 ENTERPRISE ARCHITECTURE

Control: Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Discussion: The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization’s mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture and the organization’s security and privacy architectures consistent with the organizational risk management strategy. For PM-7, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level that represents an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control

integration are most effectively accomplished through the rigorous application of the Risk Management Framework [SP 800-37] and supporting security standards and guidelines.

Related Controls: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

Control Enhancements:

(1) ENTERPRISE ARCHITECTURE | OFFLOADING

[Withdrawn: Not applicable to COV.]

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Discussion: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

Control Enhancements: None.

PM-9 RISK MANAGEMENT STRATEGY

Control:

a. Develops a comprehensive strategy to manage:

   1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and

   2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement the risk management strategy consistently across the organization; and

c. Review and update the risk management strategy at least on an annual basis or as required, to address organizational changes.

Discussion: An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

Related Controls: AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

Control Enhancements: None.

PM-10 AUTHORIZATION PROCESS

Control:

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

Discussion: Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Related Controls: CA-6, CA-7, PL-2.

Control Enhancements: None.

PM-11 MISSION AND BUSINESS PROCESS DEFINITION

Control:

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes at least on an annual basis.

Discussion: Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent to defining protection and personally identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of the processing of personally identifiable information at any stage of the information life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

Related Controls: CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

Control Enhancements: None.

PM-12 INSIDER THREAT PROGRAM

[Withdrawn: Not applicable to COV.]

PM-13 SECURITY AND PRIVACY WORKFORCE

Control: Establish a security and privacy workforce development and improvement program.

Discussion: Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

Related Controls: AT-2, AT-3.

Control Enhancements: None.

PM-14 TESTING, TRAINING, AND MONITORING

Control:

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

   1. Are developed and maintained; and

   2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion: A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Related Controls: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Control Enhancements: None.

PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

[Withdrawn: Not applicable to COV.]

PM-16 THREAT AWARENESS PROGRAM

[Withdrawn: Not applicable to COV.]

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

[Withdrawn: Not applicable to COV.]

PM-18 PRIVACY PROGRAM PLAN

[Withdrawn: Not applicable to COV.]

PM-19 PRIVACY PROGRAM LEADERSHIP ROLE

[Withdrawn: Not applicable to COV.]

PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

[Withdrawn: Not applicable to COV.]

PM-21 ACCOUNTING OF DISCLOSURES

[Withdrawn: Not applicable to COV.]

PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT

[Withdrawn: Not applicable to COV.]

PM-23 DATA GOVERNANCE BODY

[Withdrawn: Not applicable to COV.]

PM-24 DATA INTEGRITY BOARD

[Withdrawn: Not applicable to COV.]

PM-25 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

Control:

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures at least on an annual basis.

Discussion: The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Related Controls: PM-23, PT-3, SA-3, SA-8, SI-12.

Control Enhancements: None.

PM-26 COMPLAINT MANAGEMENT

[Withdrawn: Not applicable to COV.]

PM-27 PRIVACY REPORTING

[Withdrawn: Not applicable to COV.]

PM-28 RISK FRAMING

Control:

a. Identify and document:

   1. Assumptions affecting risk assessments, risk responses, and risk monitoring;

   2. Constraints affecting risk assessments, risk responses, and risk monitoring;

   3. Priorities and trade-offs considered by the organization for managing risk; and

   4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to System Owners and Agency Head; and

c. Review and update risk framing considerations at least on an annual basis and following an environmental change.

Discussion: Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

Related Controls: CA-7, PM-9, RA-3, RA-7.

Control Enhancements: None.

PM-29 RISK MANAGEMENT PROGRAM LEADERSHIP ROLES

[Withdrawn: Not applicable to COV.]

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

[Withdrawn: Not applicable to COV.]

PM-31 CONTINUOUS MONITORING STRATEGY

Control: Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing the following organization-wide metrics to be monitored: risk mitigation, vulnerabilities, audit record coverage, and other organization-defined metrics;

b. Establishing at least on a monthly basis for monitoring and at least on a quarterly basis for assessment of control effectiveness;

c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of organizational systems to the Information Security Officer and organization-defined personnel or roles at least on a monthly basis.

Discussion: Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy. Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC- 7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.

PM-32 PURPOSING

Control: Analyze organization-defined systems or systems components supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Discussion: Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

Related Controls: CA-7, PL-2, RA-3, RA-9.

Control Enhancements: None.

8.14 PERSONNEL SECURITY

PS-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level personnel security policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; and
b. Designate an organization-defined official to manage the development, documentation, and dissemination of the personnel security policy and procedures; and
c. Review and update the current personnel security:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

PS-2 POSITION RISK DESIGNATION

[Withdrawn: Not applicable to COV.]

PS-3 PERSONNEL SCREENING

Control:

a. Screen individuals prior to authorizing access to the system; and
b. Rescreen individuals in accordance with organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.

Discussion: Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Control Enhancements:

(1) PERSONNEL SCREENING | CLASSIFIED INFORMATION

[Withdrawn: Not applicable to COV.]

(2) PERSONNEL SCREENING | FORMAL INDOCTRINATION

[Withdrawn: Not applicable to COV.]

(3) PERSONNEL SCREENING | INFORMATION REQUIRING SPECIAL PROTECTIVE MEASURES

[Withdrawn: Not applicable to COV.]

(4) PERSONNEL SCREENING | CITIZENSHIP REQUIREMENTS

[Withdrawn: Not applicable to COV.]

PS-4 PERSONNEL TERMINATION

Control: Upon termination of individual employment:

a. Disable system access within 24 hours of employment termination or immediately for high risk personnel;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. [Withdrawn: Not applicable to COV.]

d. Retrieve all security-related organizational system-related property; and

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

Discussion: System property includes 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 system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Control Enhancements:

(1) PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS

[Withdrawn: Not applicable to COV.]

(2) PERSONNEL TERMINATION | AUTOMATED ACTIONS

[Withdrawn: Not applicable to COV.]

PS-5 PERSONNEL TRANSFER

Control:

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

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

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

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

Discussion: Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration 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 returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Control Enhancements: None.

PS-6 ACCESS AGREEMENTS

Control:

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements at least on an annual basis and following an environmental change; and

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

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

   2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated, on at least an annual basis.

Discussion: Access agreements include 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 systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

Control Enhancements:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION

[Withdrawn: Incorporated into PS-3.]

(2) ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

[Withdrawn: Not applicable to COV.]

(3) ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS

[Withdrawn: Not applicable to COV.]

PS-7 EXTERNAL PERSONNEL SECURITY

Control:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify the appropriate organization-defined personnel of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 24 hours or immediately for high risk individuals; and

e. Monitor provider compliance with personnel security requirements.

Discussion: External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Related Controls: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Control Enhancements: None.

PS-8 PERSONNEL SANCTIONS

Control:

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

b. [Withdrawn: Not applicable to COV.]

Discussion: Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related Controls: All XX-1 Controls, PL-4, PM-12, PS-6, PT-1.

Control Enhancements: None.

PS-9 POSITION DESCRIPTIONS

Control: Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion: Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Related Controls: None.

Control Enhancements: None.

8.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

[Withdrawn: Not applicable to COV.]

8.16 RISK ASSESSMENT

RA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level risk assessment policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;
b. Designate the Information Security Officer to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
c. Review and update the current risk assessment:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

RA-2 SECURITY CATEGORIZATION

Control:

a. Categorize the system and information it processes, stores, and transmits;
b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Discussion: Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality,

integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. [CNSSI 1253] provides additional guidance on categorization for national security systems.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with [USA PATRIOT] and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Related Controls: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC- 38, SI-12.

Control Enhancements:

(1) SECURITY CATEGORIZATION | IMPACT-LEVEL PRIORITIZATION

Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

Discussion: Organizations apply the “high-water mark” concept to each system categorized in accordance with [FIPS 199], resulting in systems designated as low impact, moderate impact, or high impact. Organizations that desire additional granularity in the system impact designations for risk-based decision-making, can further partition the systems into sub-categories of the initial system categorization. For example, an impact-level prioritization on a moderate-impact system can produce three new sub-categories: low-moderate systems, moderate-moderate systems, and high-moderate systems. Impact-level prioritization and the resulting sub-categories of the system give organizations an opportunity to focus their investments related to security control selection and the tailoring of control baselines in responding to identified risks. Impact-level prioritization can also be used to determine those systems that may be of heightened interest or value to adversaries or represent a critical loss to the federal enterprise, sometimes described as high value assets. For such high value assets, organizations may be more focused on complexity, aggregation, and information exchanges. Systems with high value assets can be prioritized by partitioning high-impact systems into low-high systems, moderate-high systems, and high-high systems.

Alternatively, organizations can apply the guidance in [CNSSI 1253] for security objective-related categorization.

Related Controls: None.

RA-3 RISK ASSESSMENT

Control:

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;
2. Determining the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in a risk assessment report;

d. Review risk assessment results at least on an annual basis and following an environmental change;

e. Disseminate risk assessment results to the appropriate organization-defined personnel; and

f. Update the risk assessment on an annual basis or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Discussion: Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Related Controls: CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.

Control Enhancements:

(1) RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT

(a) Assess supply chain risks associated with high-risk systems, high-risk system components, and cloud-based service providers; and

(b) Update the supply chain risk assessment at least on an annual basis, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Discussion: Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls: RA-2, RA-9, PM-17, PM-30, SR-2.

(2) RISK ASSESSMENT | USE OF ALL-SOURCE INTELLIGENCE

Use all-source intelligence to assist in the analysis of risk.

Discussion: Organizations employ all-source intelligence to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of information derived from all available sources, including publicly available or open-source information, measurement and signature intelligence, human intelligence, signals intelligence, and imagery intelligence. All-source intelligence is used to analyze the risk of vulnerabilities (both intentional and unintentional) from development, manufacturing, and delivery processes, people, and the environment. The risk analysis may be performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Organizations may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.

Related Controls: None.

(3) RISK ASSESSMENT | DYNAMIC THREAT AWARENESS

Determine the current cyber threat environment on an ongoing basis using threat information provided by Commonwealth Security and Risk Management.

Discussion: The threat awareness information that is gathered feeds into the organization's information security operations to ensure that procedures are updated in response to the changing threat environment. For example, at higher threat levels, organizations may change the privilege or authentication thresholds required to perform certain operations.

Related Controls: AT-2.

(4) RISK ASSESSMENT | PREDICTIVE CYBER ANALYTICS

[Withdrawn: Not applicable to COV.]

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3.]

RA-5 VULNERABILITY MONITORING AND SCANNING

Control:

a. Monitor and scan for vulnerabilities in the system and hosted applications at least once every 30 days, and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring 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. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities within 30 days unless otherwise specified by Commonwealth Security Risk Management in accordance with an organizational assessment of risk;

e. Shares information obtained from the vulnerability monitoring process and control assessments with the appropriate organization-defined personnel to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors),

networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)- validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as “bug bounties”) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization’s needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related Controls: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

Control Enhancements:

(1) VULNERABILITY MONITORING AND SCANNING | UPDATE TOOL CAPABILITY

[Withdrawn: Incorporated into RA-5.]

(2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE UPDATED

Update the system vulnerabilities to be scanned at least once every 30 days, prior to a new scan, or when new vulnerabilities are identified and reported.

Discussion: Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related Controls: SI-5.

(3) VULNERABILITY MONITORING AND SCANNING | BREADTH AND DEPTH OF COVERAGE

Define the breadth and depth of vulnerability scanning coverage.

Discussion: The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element). Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage. [SP 800-53A] provides additional information on the breadth and depth of coverage.

Related Controls: None.

(4) VULNERABILITY MONITORING AND SCANNING | DISCOVERABLE INFORMATION

Determine information about the system is discoverable and take the appropriate corrective actions and align with architectural standards.

Discussion: Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

Related Controls: AU-13, SC-26.

(5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS

Implement privileged access authorization to system components for selected vulnerability scanning activities.

Discussion: In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related Controls: None.

(6) VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSES

Compare the results of multiple vulnerability scans using Commonwealth Security and Risk Management authorized automated mechanisms.

Discussion: Using automated mechanisms to analyze multiple vulnerability scans over time can help determine trends in system vulnerabilities and identify patterns of attack.

Related Controls: None.

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

[Withdrawn: Incorporated into CM-8.]

(8) VULNERABILITY MONITORING AND SCANNING | REVIEW HISTORIC AUDIT LOGS

Review historic audit logs to determine if a vulnerability identified in the system has been previously exploited within an organization-defined time period.

Discussion: Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been previously exploited by an adversary can provide important information for forensic analyses. Such analyses can help identify, for example, the extent of a previous intrusion, the trade craft employed during the attack, organizational information exfiltrated or modified, mission or business capabilities affected, and the duration of the attack.

Related Controls: AU-6, AU-11.

(9) VULNERABILITY MONITORING AND SCANNING | PENETRATION TESTING AND ANALYSES

[Withdrawn: Incorporated into CA-8.]

(10) VULNERABILITY MONITORING AND SCANNING | CORRELATE SCANNING INFORMATION

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

Discussion: An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation.

Related Controls: None.

(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM

[Withdrawn: Not applicable to COV.]

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

[Withdrawn: Not applicable to COV.]

RA-7 RISK RESPONSE

[Withdrawn: Not applicable to COV.]

RA-8 PRIVACY IMPACT ASSESSMENTS

[Withdrawn: Not applicable to COV.]

RA-9 CRITICALITY ANALYSIS

Control: Identify critical system components and functions by performing a criticality analysis for sensitive systems, sensitive system components, or sensitive system services at least on an annual basis and following an environmental change.

Discussion: Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Related Controls: CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5.

Control Enhancements: None.

RA-10 THREAT HUNTING

Control:

a. Establish and maintain a cyber threat hunting capability to:

   1. Search for indicators of compromise in organizational systems; and

   2. Detect, track, and disrupt threats that evade existing controls; and

b. Employ the threat hunting capability at least on an annual basis.

Discussion: Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

Related Controls: CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

Control Enhancements: None.

8.17 SYSTEM AND SERVICES ACQUISITION

SA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel and procurement personnel:
    1. Organization-level system and services acquisition policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;
b. Designate an Information Security Officer to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and
c. Review and update the current system and services acquisition:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SA-8, SI-12.

Control Enhancements: None.

SA-2 ALLOCATION OF RESOURCES

Control:

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;
b. Determine, document, and allocate the resources required to protect the system or system service as part of the organization capital planning and investment control process; and
c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

Discussion: Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls: PL-7, PM-3, PM-11, SA-9, SR-3, SR-5.

Control Enhancements: None.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Control:

a. Acquire, develop, and manage the system using system development life cycle methodology that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Discussion: A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

Related Controls: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR- 5, SR-9.

Control Enhancements:

(1) SYSTEM DEVELOPMENT LIFE CYCLE | MANAGE PREPRODUCTION ENVIRONMENT

Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.

Discussion: The preproduction environment includes development, test, and integration environments. The program protection planning processes established by the Department of Defense are examples of managing the preproduction environment for defense contractors. Criticality analysis and the application of controls on developers also contribute to a more secure system development environment.

Related Controls: CM-2, CM-4, RA-3, RA-9, SA-4.

(2) SYSTEM DEVELOPMENT LIFE CYCLE | USE OF LIVE OR OPERATIONAL DATA

(a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and

(b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

Discussion: Live data is also referred to as operational data. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risks to organizations. In addition, the use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Therefore, it is important for the organization to manage any additional risks that may result from the use of live or operational data. Organizations can minimize such risks by using test or dummy data during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable.

Related Controls: PM-25, RA-3.

(3) SYSTEM DEVELOPMENT LIFE CYCLE | TECHNOLOGY REFRESH

Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

Discussion: Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components, counterfeit or repurposed components, components unable to implement security or privacy requirements, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity. Technology refreshes typically occur during the operations and maintenance stage of the system development life cycle.

Related Controls: MA-6.

SA-3-COV-1

Control:

a. Project Initiation:

1. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.
2. Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system.
3. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.
4. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.

b. Project Definition:

1. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.
2. Incorporate IT security requirements in IT system design specifications.

3. Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.
4. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.
5. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

c. Implementation:

1. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.
2. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.
3. Require that the system comply with all relevant Risk Management requirements in this Standard.
4. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see IT Systems Security Plans) of this document.

d. Disposition:

1. Require retention of the data handled by an IT system in accordance with the agency's records retention policy prior to disposing of the IT system.
2. Require that electronic media is sanitized prior to disposal, as documented (see Data Storage Media Protection), so that all data is removed from the IT system.
3. Verify the disposal of hardware and software in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SA-3-COV-2

Control: Each Information Security Officer is accountable for ensuring the following steps are documented and followed:

a. Application Planning:

1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.
2. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.
3. Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.
4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:

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

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

c. Sensitive information shall not be stored in hidden fields that are part of the application interface.

b. Application Development:

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development:

1. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.
2. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.
3. Data storage shall be separated physically from the application interface (i.e., design two or three tier architectures where the same hypervisor does not host both the application interface and the data storage instance).
4. Agencies shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).
5. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.
6. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted
7. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.
8. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.
9. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

c. Production and Maintenance:

1. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.
2. Internet-facing applications classified as sensitive shall have periodic, not to exceed 90 days, vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SA-4 ACQUISITION PROCESS

Control: Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements;

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibilities or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Discussion: Security and privacy functional requirements are typically derived from the high- level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. [SP 800-160-1] describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Related Controls: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF CONTROLS

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Discussion: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the

controls and specifically exclude functionality and data structures internal to the operation of the controls.

Related Controls: None.

(2) ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; and design and implementation information at the appropriate level of detail.

Discussion: Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Related Controls: None.

(3) ACQUISITION PROCESS | DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES

Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle that includes:

(a) Organization-defined systems engineering methods;

(b) Organization-defined systems and privacy engineering methods; and

(c) Organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes.

Discussion: Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Transparency in the methods and techniques that developers select and implement for systems engineering, systems security and privacy engineering, software development, component and system assessments, and quality control processes provides an increased level of assurance in the trustworthiness of the system, system component, or system service being acquired.

Related Controls: None.

(4) ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS

[Withdrawn: Incorporated into CM-8 (9).]

(5) ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS

Require the developer of the system, system component, or system service to:

(a) Deliver the system, component, or service with the organization-defined security configurations implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Discussion: Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

Related Controls: None.

(6) ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS

[Withdrawn: Not applicable to COV.]

(7) ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES

[Withdrawn: Incorporated into SA-4-COV-1.]

(8) ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS

Require the developer of the system, system component, or system service to produce a plan for the continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

Discussion: The objective of continuous monitoring plans is to determine if the planned, required, and deployed controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into continuous monitoring programs implemented by organizations.

Continuous monitoring plans can include the types of control assessment and monitoring activities planned, frequency of control monitoring, and actions to be taken when controls fail or become ineffective.

Related Controls: CA-7.

(9) ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Discussion: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related Controls: CM-7, SA-9.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

Employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Discussion: Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations.

Related Controls: IA-2, IA-8, PM-9.

(11) ACQUISITION PROCESS | SYSTEM OF RECORDS

Include COV data breach requirements in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.

Discussion: When, by contract, an organization provides for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirements of the [PRIVACT] to be applied to the system of records.

Related Controls: PT-6.

(12) ACQUISITION PROCESS | DATA OWNERSHIP

(a) Include organizational data ownership requirements in the acquisition contract; and

(b) Require all data to be removed from the contractor's system and returned to the organization within a maximum of 30 days.

Discussion: Contractors who operate a system that contains data owned by an organization initiating the contract have policies and procedures in place to remove the data from their systems and/or return the data in a time frame defined by the contract.

Related Controls: None.

SA-4-COV-~~1~~

Control:

a. Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against Commonwealth security processed and standards; and

b. Requires, if no Commonwealth approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

Discussion: None.

Related Controls: SC-12, SC-13.

Control Enhancements: None.

SA-5 SYSTEM DOCUMENTATION

Control:

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; and

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take actions to report to Commonwealth Security and Risk Management; and

d. Distribute documentation to the appropriate organization-defined personnel.

Discussion: System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system.

Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

Control Enhancements:

(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

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

(5) ~~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.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SA-7 USER-INSTALLED SOFTWARE

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

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

Control: Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: Commonwealth Security and Risk Management and organization-defined system security and privacy engineering principles.

Discussion: Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

Related Controls: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC- 32, SC-39, SR-2, SR-3, SR-4, SR-5.

Control Enhancements:

(1) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CLEAR ABSTRACTIONS

Implement the security design principle of clear abstractions.

Discussion: The principle of clear abstractions states that a system has simple, well-defined interfaces and functions that provide a consistent and intuitive view of the data and how the data is managed. The clarity, simplicity, necessity, and sufficiency of the system interfaces—combined with a precise definition of their functional behavior—promotes ease of analysis, inspection, and testing as well as the correct and secure use of the system. The clarity of an abstraction is subjective. Examples that reflect the application of this principle include avoidance of redundant, unused interfaces; information hiding; and avoidance of semantic overloading of interfaces or their parameters. Information hiding (i.e., representation-independent programming), is a design discipline used to ensure that the internal representation of information in one system component is not visible to another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.

Related Controls: None.

(2) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST COMMON MECHANISM

Implement the security design principle of least common mechanism in organization-defined systems or system components.

Discussion: The principle of least common mechanism states that the amount of mechanism common to more than one user and depended on by all users is minimized [POPEK74].

Mechanism minimization implies that different components of a system refrain from using the same mechanism to access a system resource. Every shared mechanism (especially a mechanism involving shared variables) represents a potential information path between users and is designed with care to ensure that it does not unintentionally compromise security [SALTZER75]. Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing the system state among different programs. A single program that corrupts a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels [LAMPSON73].

Related Controls: None.

(3) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MODULARITY AND LAYERING

Implement the security design principles of modularity and layering in organization-defined systems or system components.

Discussion: The principles of modularity and layering are fundamental across system engineering disciplines. Modularity and layering derived from functional decomposition are effective in managing system complexity by making it possible to comprehend the structure of the system. Modular decomposition, or refinement in system design, is challenging and resists general statements of principle. Modularity serves to isolate functions and related data structures into well-defined logical units. Layering allows the relationships of these units to be better understood so that dependencies are clear and undesired complexity can be avoided. The security design principle of modularity extends functional modularity to include considerations based on trust, trustworthiness, privilege, and security policy.

Security-informed modular decomposition includes the allocation of policies to systems in a network, separation of system applications into processes with distinct address spaces, allocation of system policies to layers, and separation of processes into subjects with distinct privileges based on hardware-supported privilege domains.

Related Controls: SC-2, SC-3.

(4) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PARTIALLY ORDERED DEPENDENCIES

Implement the security design principle of partially ordered dependencies in organization-defined systems or system components.

Discussion: The principle of partially ordered dependencies states that the synchronization, calling, and other dependencies in the system are partially ordered. A fundamental concept in system design is layering, whereby the system is organized into well-defined, functionally related modules or components. The layers are linearly ordered with respect to inter-layer dependencies, such that higher layers are dependent on lower layers. While providing functionality to higher layers, some layers can be self-contained and not dependent on lower layers. While a partial ordering of all functions in a given system may not be possible, if circular dependencies are constrained to occur within layers, the inherent problems of circularity can be more easily managed. Partially ordered dependencies and system layering contribute significantly to the simplicity and coherency of the system design. Partially ordered dependencies also facilitate system testing and analysis.

Related Controls: None.

(5) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | EFFICIENTLY MEDIATED ACCESS

Implement the security design principle of efficiently mediated access in organization-defined systems or system components.

Discussion: The principle of efficiently mediated access states that policy enforcement mechanisms utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints. The mediation of access to system resources (i.e., CPU, memory, devices, communication ports, services, infrastructure, data, and information) is often the predominant security function of secure systems. It also enables the realization of protections for the capability provided to stakeholders by the system. Mediation of resource access can result in performance bottlenecks if the system is not designed correctly. For example, by using hardware mechanisms, efficiently mediated access can be achieved. Once access to a low-level resource such as memory has been obtained, hardware protection mechanisms can ensure that out-of-bounds access does not occur.

Related Controls: AC-25.

(6) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SHARING

Implement the security design principle of minimized sharing in organization-defined systems or system components.

Discussion: The principle of minimized sharing states that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify system design and implementation. In order to protect user-domain resources from arbitrary active entities, no resource is shared unless that sharing has been explicitly requested and granted. The need for resource sharing can be motivated by the design principle of least common mechanism in the case of internal entities or driven by stakeholder requirements. However, internal sharing is carefully designed to avoid performance and covert storage and timing channel problems. Sharing via common mechanism can increase the susceptibility of data and information to unauthorized access, disclosure, use, or modification and can adversely affect the inherent capability provided by the system. To minimize sharing induced by common mechanisms, such mechanisms can be designed to be reentrant or virtualized to preserve separation.

Moreover, the use of global data to share information is carefully scrutinized. The lack of encapsulation may obfuscate relationships among the sharing entities.

Related Controls: SC-31.

(7) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REDUCED COMPLEXITY

Implement the security design principle of reduced complexity in organization-defined systems or system components.

Discussion: The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more analyzable, and less prone to error. The reduced complexity principle applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential. Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain; that is, simpler systems contain fewer vulnerabilities. An benefit of reduced complexity is that it is easier to understand whether the intended security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and the existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex.

Transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6) may require implementing the older and newer technologies simultaneously during the

transition period. This may result in a temporary increase in system complexity during the transition.

Related Controls: None.

(8) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE EVOLVABILITY

Implement the security design principle of secure evolvability in organization-defined systems or system components.

Discussion: The principle of secure evolvability states that a system is developed to facilitate the maintenance of its security properties when there are changes to the system's structure, interfaces, interconnections (i.e., system architecture), functionality, or configuration (i.e., security policy enforcement). Changes include a new, enhanced, or upgraded system capability; maintenance and sustainment activities; and reconfiguration. Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic direction, anticipated changes in the threat environment, and anticipated maintenance and sustainment needs. It is unrealistic to expect that complex systems remain secure in contexts not envisioned during development, whether such contexts are related to the operational environment or to usage. A system may be secure in some new contexts, but there is no guarantee that its emergent behavior will always be secure. It is easier to build trustworthiness into a system from the outset, and it follows that the sustainment of system trustworthiness requires planning for change as opposed to adapting in an ad hoc or non-methodical manner. The benefits of this principle include reduced vendor life cycle costs, reduced cost of ownership, improved system security, more effective management of security risk, and less risk uncertainty.

Related Controls: CM-3.

(9) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMPONENTS

Implement the security design principle of trusted components in organization-defined systems or system components.

Discussion: The principle of trusted components states that a component is trustworthy to at least a level commensurate with the security dependencies it supports (i.e., how much it is trusted to perform its security functions by other components). This principle enables the composition of components such that trustworthiness is not inadvertently diminished and the trust is not consequently misplaced. Ultimately, this principle demands some metric by which the trust in a component and the trustworthiness of a component can be measured on the same abstract scale. The principle of trusted components is particularly relevant when considering systems and components in which there are complex chains of trust dependencies. A trust dependency is also referred to as a trust relationship and there may be chains of trust relationships.

The principle of trusted components also applies to a compound component that consists of subcomponents (e.g., a subsystem), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is that of its least trustworthy subcomponent. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than the conservative assumption. However, any such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives as well as relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defense-in-depth layering within the component or a replication of components. Defense-in-depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.

Related Controls: None.

(10) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL TRUST

Implement the security design principle of hierarchical trust in organization- defined systems or system components.

Discussion: The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for trustworthiness reasoning or an assurance case (assurance argument) when composing a secure system from heterogeneously trustworthy components. To analyze a system composed of heterogeneously trustworthy components for its trustworthiness, it is essential to eliminate circular dependencies with regard to the trustworthiness. If a more trustworthy component located in a lower layer of the system were to depend on a less trustworthy component in a higher layer, this would, in effect, put the components in the same “less trustworthy” equivalence class per the principle of trusted components. Trust relationships, or chains of trust, can have various manifestations. For example, the root certificate of a certificate hierarchy is the most trusted node in the hierarchy, whereas the leaves in the hierarchy may be the least trustworthy nodes. Another example occurs in a layered high-assurance system where the security kernel (including the hardware base), which is located at the lowest layer of the system, is the most trustworthy component. The principle of hierarchical trust, however, does not prohibit the use of overly trustworthy components. There may be cases in a system of low trustworthiness where it is reasonable to employ a highly trustworthy component rather than one that is less trustworthy (e.g., due to availability or other cost-benefit driver). For such a case, any dependency of the highly trustworthy component upon a less trustworthy component does not degrade the trustworthiness of the resulting low-trust system.

Related Controls: None.

(11) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | INVERSE MODIFICATION THRESHOLD

Implement the security design principle of inverse modification threshold in organization-defined systems or system components.

Discussion: The principle of inverse modification threshold builds on the principle of trusted components and the principle of hierarchical trust and states that the degree of protection provided to a component is commensurate with its trustworthiness. As the trust placed in a component increases, the protection against unauthorized modification of the component also increases to the same degree. Protection from unauthorized modification can come in the form of the component’s own self-protection and innate trustworthiness, or it can come from the protections afforded to the component from other elements or attributes of the security architecture (to include protections in the environment of operation).

Related Controls: None.

(12) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL PROTECTION

Implement the security design principle of hierarchical protection in organization-defined systems or system components.

Discussion: The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted component, it protects itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it protects itself from all untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel. The trustworthiness of users is a consideration for applying the principle of hierarchical protection. A trusted system need not protect itself from an equally trustworthy user, reflecting use of untrusted systems in “system high” environments where users are highly trustworthy and where other protections are put in place to bound and protect the “system high” execution environment.

Related Controls: None.

(13) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SECURITY ELEMENTS

Implement the security design principle of minimized security elements in organization-defined systems or system components.

Discussion: The principle of minimized security elements states that the system does not have extraneous trusted components. The principle of minimized security elements has two aspects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally costlier to construct and implement, owing to the increased rigor of development processes. Trusted components require greater security analysis to qualify their trustworthiness. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. The analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to ascertain than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.

Related Controls: None.

(14) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST PRIVILEGE

Implement the security design principle of least privilege in organization- defined systems or system components.

Discussion: The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified.

Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has need to view the audit data that has been collected but no need to perform operations on that data.

In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated on by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality and that the access modes for the elements (e.g., read, write) are minimal.

Related Controls: AC-6, CM-7.

(15) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PREDICATE PERMISSION

Implement the security design principle of predicate permission in organization-defined systems or system components.

Discussion: The principle of predicate permission states that system designers consider requiring multiple authorized entities to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is allowed to proceed.

[SALTZER75] originally named predicate permission the separation of privilege. It is also equivalent to separation of duty. The division of privilege among multiple parties decreases the likelihood of abuse and provides the safeguard that no single accident, deception, or breach of trust is sufficient to enable an unrecoverable action that can lead to significantly damaging effects. The design options for such a mechanism may require simultaneous action (e.g., the firing of a nuclear weapon requires two different authorized individuals to give the correct command within a small time window) or a sequence of operations where each successive action is enabled by some prior action, but no single individual is able to enable more than one action.

Related Controls: AC-5.

(16) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-RELIANT TRUSTWORTHINESS

Implement the security design principle of self-reliant trustworthiness in organization-defined systems or system components.

Discussion: The principle of self-reliant trustworthiness states that systems minimize their reliance on other systems for their own trustworthiness. A system is trustworthy by default, and any connection to an external entity is used to supplement its function. If a system were required to maintain a connection with another external entity in order to maintain its trustworthiness, then that system would be vulnerable to malicious and non-malicious threats that could result in the loss or degradation of that connection. The benefit of the principle of self-reliant trustworthiness is that the isolation of a system will make it less vulnerable to attack. A corollary to this principle relates to the ability of the system (or system component) to operate in isolation and then resynchronize with other components when it is rejoined with them.

Related Controls: None.

(17) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DISTRIBUTED COMPOSITION

Implement the security design principle of secure distributed composition in organization-defined systems or system components.

Discussion: The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy result in a system that enforces that policy at least as well as the individual components do. Many of the design principles for secure systems deal with how components can or should interact. The need to create or enable a capability from the composition of distributed components can magnify the relevancy of these principles. In particular, the translation of security policy from a stand-alone to a distributed system or a system-of-systems can have unexpected or emergent results. Communication protocols and distributed data consistency mechanisms help to ensure consistent policy enforcement across a distributed system. To ensure a system-wide level of assurance of correct policy enforcement, the security architecture of a distributed composite system is thoroughly analyzed.

Related Controls: None.

(18) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMMUNICATION CHANNELS

Implement the security design principle of trusted communications channels in organization-defined systems or system components.

Discussion: The principle of trusted communication channels states that when composing a system where there is a potential threat to communications between components (i.e., the interconnections between components), each communication channel is trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions). Trusted communication channels are achieved by a combination of restricting access to the communication channel (to ensure an acceptable match in the trustworthiness of the endpoints involved in the communication) and employing end-to-end protections for the data transmitted over the

communication channel (to protect against interception and modification and to further increase the assurance of proper end-to-end communication).

Related Controls: SC-8, SC-12, SC-13.

(19) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CONTINUOUS PROTECTION

Implement the security design principle of continuous protection in organization-defined systems or system components.

Discussion: The principle of continuous protection states that components and data used to enforce the security policy have uninterrupted protection that is consistent with the security policy and the security architecture assumptions. No assurances that the system can provide the confidentiality, integrity, availability, and privacy protections for its design capability can be made if there are gaps in the protection. Any assurances about the ability to secure a delivered capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unprotected while under control of the system (i.e., during the creation, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruption, and shutdown). Continuous protection requires adherence to the precepts of the reference monitor concept (i.e., every request is validated by the reference monitor; the reference monitor is able to protect itself from tampering; and sufficient assurance of the correctness and completeness of the mechanism can be ascertained from analysis and testing) and the principle of secure failure and recovery (i.e., preservation of a secure state during error, fault, failure, and successful attack; preservation of a secure state during recovery to normal, degraded, or alternative operational modes).

Continuous protection also applies to systems designed to operate in varying configurations, including those that deliver full operational capability and degraded-mode configurations that deliver partial operational capability. The continuous protection principle requires that changes to the system security policies be traceable to the operational need that drives the configuration and be verifiable (i.e., it is possible to verify that the proposed changes will not put the system into an insecure state). Insufficient traceability and verification may lead to inconsistent states or protection discontinuities due to the complex or undecidable nature of the problem. The use of pre-verified configuration definitions that reflect the new security policy enables analysis to determine that a transition from old to new policies is essentially atomic and that any residual effects from the old policy are guaranteed to not conflict with the new policy. The ability to demonstrate continuous protection is rooted in the clear articulation of life cycle protection needs as stakeholder security requirements.

Related Controls: AC-25.

(20) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE METADATA MANAGEMENT

Implement the security design principle of secure metadata management in organization-defined systems or system components.

Discussion: The principle of secure metadata management states that metadata are “first class” objects with respect to security policy when the policy requires either complete protection of information or that the security subsystem be self-protecting. The principle of secure metadata management is driven by the recognition that a system, subsystem, or component cannot achieve self-protection unless it protects the data it relies on for correct execution. Data is generally not interpreted by the system that stores it. It may have semantic value (i.e., it comprises information) to users and programs that process the data. In contrast, metadata is information about data, such as a file name or the date when the file was created. Metadata is bound to the target data that it describes in a way that the system can interpret, but it need not be stored inside of or proximate to its target data.

There may be metadata whose target is itself metadata (e.g., the classification level or impact level of a file name), including self-referential metadata.

The apparent secondary nature of metadata can lead to neglect of its legitimate need for protection, resulting in a violation of the security policy that includes the exfiltration of information. A particular concern associated with insufficient protections for metadata is associated with multilevel secure (MLS) systems. MLS systems mediate access by a subject to an object based on relative sensitivity levels. It follows that all subjects and objects in the scope of control of the MLS system are either directly labeled or indirectly attributed with sensitivity levels. The corollary of labeled metadata for MLS systems states that objects containing metadata are labeled. As with protection needs assessments for data, attention is given to ensure that the confidentiality and integrity protections are individually assessed, specified, and allocated to metadata, as would be done for mission, business, and system data.

Related Controls: None.

(21) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-ANALYSIS

Implement the security design principle of self-analysis in organization- defined systems or system components.

Discussion: The principle of self-analysis states that a system component is able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability is commensurate with the level of trustworthiness invested in the system. At the system level, self-analysis can be achieved through hierarchical assessments of trustworthiness established in a bottom-up fashion. In this approach, the lower-level components check for data integrity and correct functionality (to a limited extent) of higher- level components. For example, trusted boot sequences involve a trusted lower-level component that attests to the trustworthiness of the next higher-level components so that a transitive chain of trust can be established. At the root, a component attests to itself, which usually involves an axiomatic or environmentally enforced assumption about its integrity.

Results of the self-analyses can be used to guard against externally induced errors, internal malfunction, or transient errors. By following this principle, some simple malfunctions or errors can be detected without allowing the effects of the error or malfunction to propagate outside of the component. Further, the self-test can be used to attest to the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.

Related Controls: CA-7.

(22) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ACCOUNTABILITY AND TRACEABILITY

Implement the security design principle of accountability and traceability in organization-defined systems or system components.

Discussion: The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-object interactions) to the entity on whose behalf the action is being taken. The principle of accountability and traceability requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., an audit subsystem). To record the details about actions, the system is able to uniquely identify the entity on whose behalf the action is being carried out and also record the relevant sequence of actions that are carried out. The accountability policy also requires that audit trail itself be protected from unauthorized access and modification. The principle of least privilege assists in tracing the actions to particular entities, as it increases the granularity of accountability. Associating specific actions with system entities, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provide non-repudiation because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serves is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or

component that allowed the violation of the security policy and the actions of individuals associated with the violation of the security policy.

Related Controls: AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.

(23) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DEFAULTS

Implement the security design principle of secure defaults in organization- defined systems or system components.

Discussion: The principle of secure defaults states that the default configuration of a system (including its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults applies to the initial (i.e., default) configuration of a system as well as to the security engineering and design of access control and other security functions that follow a “deny unless explicitly authorized” strategy. The initial configuration aspect of this principle requires that any “as shipped” configuration of a system, subsystem, or system component does not aid in the violation of the security policy and can prevent the system from operating in the default configuration for those cases where the security policy itself requires configuration by the operational user.

Restrictive defaults mean that the system will operate “as-shipped” with adequate self-protection and be able to prevent security breaches before the intended security policy and system configuration is established. In cases where the protection provided by the “as-shipped” product is inadequate, stakeholders assess the risk of using it prior to establishing a secure initial state. Adherence to the principle of secure defaults guarantees that a system is established in a secure state upon successfully completing initialization. In situations where the system fails to complete initialization, either it will perform a requested operation using secure defaults or it will not perform the operation. Refer to the principles of continuous protection and secure failure and recovery that parallel this principle to provide the ability to detect and recover from failure.

The security engineering approach to this principle states that security mechanisms deny requests unless the request is found to be well-formed and consistent with the security policy. The insecure alternative is to allow a request unless it is shown to be inconsistent with the policy. In a large system, the conditions that are satisfied to grant a request that is denied by default are often far more compact and complete than those that would need to be checked in order to deny a request that is granted by default.

Related Controls: CM-2, CM-6, SA-4.

(24) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE FAILURE AND RECOVERY

Implement the security design principle of secure failure and recovery in organization-defined systems or system components.

Discussion: The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The principle of secure failure and recovery parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated. In addition, when specified, the system is capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operations while ensuring that a secure state is maintained such that security policies are not violated.

Failure is a condition in which the behavior of a component deviates from its specified or expected behavior for an explicitly documented input. Once a failed security function is detected, the system may reconfigure itself to circumvent the failed component while maintaining security and provide all or part of the functionality of the original system, or it

may completely shut itself down to prevent any further violation of security policies. For this to occur, the reconfiguration functions of the system are designed to ensure continuous enforcement of security policy during the various phases of reconfiguration.

Another technique that can be used to recover from failures is to perform a rollback to a secure state (which may be the initial state) and then either shutdown or replace the service or component that failed such that secure operations may resume. Failure of a component may or may not be detectable to the components using it. The principle of secure failure indicates that components fail in a state that denies rather than grants access. For example, a nominally “atomic” operation interrupted before completion does not violate security policy and is designed to handle interruption events by employing higher-level atomicity and rollback mechanisms (e.g., transactions). If a service is being used, its atomicity properties are well-documented and characterized so that the component availing itself of that service can detect and handle interruption events appropriately. For example, a system is designed to gracefully respond to disconnection and support resynchronization and data consistency after disconnection.

Failure protection strategies that employ replication of policy enforcement mechanisms, sometimes called defense in depth, can allow the system to continue in a secure state even when one mechanism has failed to protect the system. If the mechanisms are similar, however, the additional protection may be illusory, as the adversary can simply attack in series. Similarly, in a networked system, breaking the security on one system or service may enable an attacker to do the same on other similar replicated systems and services. By employing multiple protection mechanisms whose features are significantly different, the possibility of attack replication or repetition can be reduced. Analyses are conducted to weigh the costs and benefits of such redundancy techniques against increased resource usage and adverse effects on the overall system performance. Additional analyses are conducted as the complexity of these mechanisms increases, as could be the case for dynamic behaviors. Increased complexity generally reduces trustworthiness. When a resource cannot be continuously protected, it is critical to detect and repair any security breaches before the resource is once again used in a secure context.

Related Controls: CP-10, CP-12, SC-7, SC-8, SC-24, SI-13.

(25) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ECONOMIC SECURITY

Implement the security design principle of economic security in organization- defined systems or system components.

Discussion: The principle of economic security states that security mechanisms are not costlier than the potential damage that could occur from a security breach. This is the security-relevant form of the cost-benefit analyses used in risk management. The cost assumptions of cost-benefit analysis prevent the system designer from incorporating security mechanisms of greater strength than necessary, where strength of mechanism is proportional to cost. The principle of economic security also requires analysis of the benefits of assurance relative to the cost of that assurance in terms of the effort expended to obtain relevant and credible evidence as well as the necessary analyses to assess and draw trustworthiness and risk conclusions from the evidence.

Related Controls: RA-3.

(26) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PERFORMANCE SECURITY

Implement the security design principle of performance security in organization-defined systems or system components.

Discussion: The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized. For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers

adhere to the specified constraints that capability performance needs place on protection needs. The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection. The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat.

The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory is granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode. Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.

Related Controls: SC-12, SC-13, SI-2, SI-7.

(27) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HUMAN FACTORED SECURITY

Implement the security design principle of human factored security in organization-defined systems or system components.

Discussion: The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions that affect such policy and its enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made. Particular attention is given to interfaces through which personnel responsible for system administration and operation configure and set up the security policies. Ideally, these personnel are able to understand the impact of their choices. Personnel with system administrative and operational responsibilities are able to configure systems before start-up and administer them during runtime with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impede or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the strictness necessary for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable them, avoid them, or use them in ways inconsistent with the security requirements and protection needs that the mechanisms were designed to satisfy.

Related Controls: None.

(28) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ACCEPTABLE SECURITY

Implement the security design principle of acceptable security in organization-defined systems or system components.

Discussion: The principle of acceptable security requires that the level of privacy and performance that the system provides is consistent with the users' expectations. The perception of personal privacy may affect user behavior, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces or meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.

Related Controls: None.

(29) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REPEATABLE AND DOCUMENTED PROCEDURES

Implement the security design principle of repeatable and documented procedures in organization-defined systems or system components.

Discussion: The principle of repeatable and documented procedures states that the techniques and methods employed to construct a system component permit the same component to be completely and correctly reconstructed at a later time. Repeatable and documented procedures support the development of a component that is identical to the component created earlier, which may be in widespread use. In the case of other system artifacts (e.g., documentation and testing results), repeatability supports consistency and the ability to inspect the artifacts. Repeatable and documented procedures can be introduced at various stages within the system development life cycle and contribute to the ability to evaluate assurance claims for the system. Examples include systematic procedures for code development and review, procedures for the configuration management of development tools and system artifacts, and procedures for system delivery.

Related Controls: CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.

(30) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PROCEDURAL RIGOR

Implement the security design principle of procedural rigor in organization- defined systems or system components.

Discussion: The principle of procedural rigor states that the rigor of a system life cycle process is commensurate with its intended trustworthiness. Procedural rigor defines the scope, depth, and detail of the system life cycle procedures. Rigorous system life cycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the life cycle process such that the introduction of unspecified functionality is prevented.

Second, rigorous procedures applied to systems security engineering activities that produce specifications and other system design documents contribute to the ability to understand the system as it has been built rather than trusting that the component, as implemented, is the authoritative (and potentially misleading) specification.

Finally, modifications to an existing system component are easier when there are detailed specifications that describe its current design instead of studying source code or schematics to try to understand how it works. Procedural rigor helps ensure that security functional and assurance requirements have been satisfied, and it contributes to a better-informed basis for the determination of trustworthiness and risk posture. Procedural rigor is commensurate with the degree of assurance desired for the system. If the required trustworthiness of the system is low, a high level of procedural rigor may add unnecessary cost, whereas when high trustworthiness is critical, the cost of high procedural rigor is merited.

Related Controls: None.

(31) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE SYSTEM MODIFICATION

Implement the security design principle of secure system modification in organization-defined systems or system components.

Discussion: The principle of secure system modification states that system modification maintains system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform secure systems into systems that are not secure. The procedures for system modification ensure that if the system is to maintain its trustworthiness, the same rigor that was applied to its initial development is applied to any system changes. Because modifications can affect the ability of the system to maintain its secure state, a careful security analysis of the modification is

needed prior to its implementation and deployment. This principle parallels the principle of secure evolvability.

Related Controls: CM-3, CM-4.

(32) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SUFFICIENT DOCUMENTATION

Implement the security design principle of sufficient documentation in organization-defined systems or system components.

Discussion: The principle of sufficient documentation states that organizational personnel with responsibilities to interact with the system are provided with adequate documentation and other information such that the personnel contribute to rather than detract from system security. Despite attempts to comply with principles such as human factored security and acceptable security, systems are inherently complex, and the design intent for the use of security mechanisms and the ramifications of the misuse or misconfiguration of security mechanisms are not always intuitively obvious. Uninformed and insufficiently trained users can introduce vulnerabilities due to errors of omission and commission. The availability of documentation and training can help to ensure a knowledgeable cadre of personnel, all of whom have a critical role in the achievement of principles such as continuous protection.

Documentation is written clearly and supported by training that provides security awareness and understanding of security-relevant responsibilities.

Related Controls: AT-2, AT-3, SA-5.

(33) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZATION

Implement the privacy principle of minimization using organization-defined processes.

Discussion: The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

Related Controls: PE-8, PM-25, SC-42, SI-12.

SA-9 EXTERNAL SYSTEM SERVICES

Control:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: Virginia Information Technologies Agency's specified controls;

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: Virginia Information Technologies Agency and organization-defined processes, methods, and techniques.

Discussion: External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the

relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements.

Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

Control Enhancements:

(1) EXTERNAL SYSTEM SERVICES | RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS

(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

(b) Verify that the acquisition or outsourcing of dedicated information security services is approved by the Chief Information Security Officer or designee.

Discussion: Information security services include the operation of security devices, such as firewalls or key management services as well as incident monitoring, analysis, and response. Risks assessed can include system, mission or business, security, privacy, or supply chain risks.

Related Controls: CA-6, RA-3, RA-8.

(2) EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: organization-defined external system services.

Discussion: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls: CM-6, CM-7.

(3) EXTERNAL SYSTEM SERVICES | ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: Commonwealth Security and Risk Management and organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships.

Discussion: Trust relationships between organizations and external service providers reflect the degree of confidence that the risk from using external services is at an acceptable level. Trust relationships can help organizations gain increased levels of confidence that service providers are providing adequate protection for the services rendered and can also be useful when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complicated due to the potentially large number of entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control that organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or individual privacy and the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements.

Related Controls: SR-2.

(4) EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

Take the following actions to verify that the interests of the organization-defined external service providers are consistent with and reflect organizational interests: organization-defined actions.

Discussion: As organizations increasingly use external service providers, it is possible that the interests of the service providers may diverge from organizational interests. In such situations, simply having the required technical, management, or operational controls in place may not be sufficient if the providers that implement and manage those controls are not operating in a manner consistent with the interests of the consuming organizations.

Actions that organizations take to address such concerns include requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, such as providers with which organizations have had successful trust relationships; and conducting routine, periodic, unscheduled visits to service provider facilities.

Related Controls: None.

(5) EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION

Restrict the location of information processing; information or data; system services to locations within the Unites States of America based on the location of storing or processing of COV data.

Discussion: The location of information processing, information and data storage, or system services can have a direct impact on the ability of organizations to successfully execute their mission and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria that organizations use. For example, organizations may desire that data or information storage locations be restricted to certain locations to help facilitate incident response activities in case of information security incidents or breaches. Incident response activities, including forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws, policies, or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

Related Controls: SA-5, SR-4.

(6) EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS

[Withdrawn: Not applicable to COV.]

(7) EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED INTEGRITY CHECKING

Provide the capability to check the integrity of information while it resides in the external system.

Discussion: Storage of organizational information in an external system could limit visibility into the security status of its data. The ability of the organization to verify and validate the integrity of its stored data without transferring it out of the external system provides such visibility.

Related Controls: SI-7.

(8) EXTERNAL SYSTEM SERVICES | PROCESSING AND STORAGE LOCATION – U.S. JURISDICTION

Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

Discussion: The geographic location of information processing and data storage can have a direct impact on the ability of organizations to successfully execute their mission and business functions. A compromise or breach of high impact information and systems can have severe or catastrophic adverse impacts on organizational assets and operations, individuals, other organizations, and the Nation. Restricting the processing and storage of

high-impact information to facilities within the legal jurisdictional boundary of the United States provides greater control over such processing and storage.

Related Controls: SA-5, SR-4.

SA-9-COV-1

Control:

a. Establish the exact geographically location of all data if not stored within the Commonwealth. The Commonwealth will define the parameters and costs for data location options prior to making any contractual commitments; and

b. Confirm the exact geographically location of the sensitive data on at least a monthly basis and report the location to the appropriate regulatory authority at least every 90 days.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SA-9-COV-2

Control:

a. Establish a Data Escrow policy to address the data recovery process in case of system failure or facility issues and ensure all copies of data are returned to the Commonwealth at the end of contract; and

b. Establish a validated copy of any data elements classified as sensitive with respect to integrity or availability or are considered components in a system of record for the Commonwealth. The validated copy must be stored within a secured environment maintained by the Commonwealth.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SA-9-COV-3

Control:

a. Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis;

b. Perform at least a monthly review of activity logs related to the operation of the service. At a minimum, the activity review must include the access time and action of each individual using the system during the review period;

c. Receive reports from the vendor on vulnerability scans of the operating system and supporting software at least once every 90 days;

d. Ensure that the vendor conduct an independent vulnerability scan of the service at least once every 90 days and provide the results to Agency within 10 business days;

e. Submit a summary of all findings from the monthly activity log review once every 90 days to the appropriate regulatory authority;

f. Submit the vulnerability scan information within 30 days of receipt from the vendor to the appropriate regulatory authority; and

g. Submit the results from the Data Owning Agency vulnerability scan of the service within 30 days of scan completion.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;

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 and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to the Information Security Officer.

Discussion: Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls.

Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

Related Controls: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6.

Control Enhancements:

(1) DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Discussion: Software and firmware integrity verification allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. The integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

Related Controls: SI-7, SR-11.

(2) DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESS

Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Discussion: Alternate configuration management processes may be required when organizations use commercial off-the-shelf information technology products. Alternate configuration management processes include organizational personnel who review and approve proposed changes to systems, system components, and system services and conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services.

Related Controls: None.

(3) DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION

Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

Discussion: Hardware integrity verification allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations may verify the integrity of hardware components with hard-to-copy labels, verifiable serial numbers provided by developers, and by requiring the use of anti-tamper technologies. Delivered hardware components also include hardware and firmware updates to such components.

Related Controls: SI-7.

(4) DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION

Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.

Discussion: The trusted generation of descriptions, source code, and object code addresses authorized changes to hardware, software, and firmware components between versions during development. The focus is on the efficacy of the configuration management process by the developer to ensure that newly generated versions of security-relevant hardware descriptions, source code, and object code continue to enforce the security policy for the system, system component, or system service. In contrast, SA-10(1) and SA-10(3) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, or mechanisms provided by developers.

Related Controls: None.

(5) DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL

Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Discussion: Mapping integrity for version control addresses changes to hardware, software, and firmware components during both initial development and system development life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs, hardware drawings, source code) and the equivalent data in master copies in operational environments is essential to ensuring the availability of organizational systems that support critical mission and business functions.

Related Controls: None.

(6) DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION

Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Discussion: The trusted distribution of security-relevant hardware, software, and firmware updates help to ensure that the updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.

Related Controls: None.

(7) DEVELOPER CONFIGURATION MANAGEMENT | SECURITY AND PRIVACY REPRESENTATIVES

Require the Information Security Officer or designee to be included in the configuration change management and control process.

Discussion: Information security and privacy representatives can include system security officers, senior agency information security officers, senior agency officials for privacy, and system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change management and control process in this control enhancement refers to the change management and control process defined by organizations in SA-10b.

Related Controls: None.

SA-11 DEVELOPER TESTING AND EVALUATION

Control: Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy control assessments;

b. Perform unit, integration, system, and regression testing/evaluation before moving the development content to production at the appropriate depth and coverage;

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

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

Discussion: Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include 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; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and 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 and privacy assessment plans, flaw remediation processes, and the evidence that the plans and 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 system. Contracts may specify protection requirements for documentation.

Related Controls: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

Control Enhancements:

(1) DEVELOPER TESTING AND EVALUATION | STATIC CODE ANALYSIS

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Discussion: Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

Related Controls: None.

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

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

(a) Uses the following contextual information: Business Impact Analysis, Risk Assessment, and organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels;

(b) Employs the following tools and methods: approved tools and methods;

(c) Conducts the modeling and analyses at the following level of rigor: organization-defined breadth and depth of modeling and analyses; and

(d) Produces evidence that meets the following acceptance criteria: Information Security Officer-defined acceptance criteria.

Discussion: Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the system development life cycle. Therefore, updates to threat modeling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this stage of the system development life cycle ensure that design and implementation changes have been accounted for and that vulnerabilities created because of those changes have been reviewed and mitigated.

Related controls: PM-15, RA-3, RA-5.

(3) DEVELOPER TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE

[Withdrawn: Not applicable to COV.]

(4) DEVELOPER TESTING AND EVALUATION | MANUAL CODE REVIEWS

Require the developer of the system, system component, or system service to perform a manual code review of organization-defined code using the following processes, procedures, and/or techniques: organization-defined processes, procedures, and/or techniques.

Discussion: Manual code reviews are usually reserved for the critical software and firmware components of systems. Manual code reviews are effective at identifying weaknesses that require knowledge of the application's requirements or context that, in most cases, is unavailable to automated analytic tools and techniques, such as static and dynamic analysis. The benefits of manual code review include the ability to verify access control matrices against application controls and review detailed aspects of cryptographic implementations and controls.

Related Controls: None.

(5) DEVELOPER TESTING AND EVALUATION | PENETRATION TESTING

Require the developer of the system, system component, or system service to perform penetration testing:

(a) At the following level of rigor: inputs; and

(b) Under the following constraints: constraints as approved by the Information Security Officer.

Discussion: Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent the implemented security and privacy features of information technology products and systems. Useful information for assessors who conduct penetration testing includes product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black-box testing with analyses performed by skilled professionals who simulate adversary actions. The objective of penetration testing is to discover vulnerabilities in systems, system components, and services that result from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible. When user session information and other personally identifiable information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.

Related Controls: CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6.

(6) DEVELOPER TESTING AND EVALUATION | ATTACK SURFACE REVIEWS

Require the developer of the system, system component, or system service to perform attack surface reviews.

Discussion: Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to attacks. Attack surfaces include any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of the changes. The correction of identified flaws includes deprecation of unsafe functions.

Related Controls: SA-15.

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

Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of required controls at the following level of rigor: appropriate depth of testing/evaluation as approved by the Information Security Officer.

Discussion: Verifying that testing and evaluation provides complete coverage of required 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 that corresponds to the degree of formality of the analysis. Rigorously demonstrating control coverage at the highest levels of assurance can be achieved using formal modeling and analysis techniques, including correlation between control implementation and corresponding test cases.

Related Controls: SA-15.

(8) DEVELOPER TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Discussion: Dynamic code analysis provides runtime verification of software programs using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs runtime tools to ensure that security functionality performs in the way it was designed. A type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and the assurance provided, organizations may also consider conducting code coverage analysis (i.e., checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (i.e., checking for words that are out of place in software code, such as non-English language words or derogatory terms).

Related Controls: None.

(9) DEVELOPER TESTING AND EVALUATION | INTERACTIVE APPLICATION SECURITY TESTING

Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.

Discussion: Interactive (also known as instrumentation-based) application security testing is a method of detecting vulnerabilities by observing applications as they run during testing. The use of instrumentation relies on direct measurements of the actual running applications and uses access to the code, user interaction, libraries, frameworks, backend connections, and configurations to directly measure control effectiveness. When combined with analysis techniques, interactive application security testing can identify a broad range of potential vulnerabilities and confirm control effectiveness. Instrumentation-based testing works in real time and can be used continuously throughout the system development life cycle.

Related Controls: None.

SA-12 SUPPLY CHAIN PROTECTION

[Withdrawn: Incorporated into SR Family.]

Control Enhancements:

(1) SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS

[Withdrawn: Moved to SR-5.]

(2) SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS

[Withdrawn: Moved to SR-6.]

(3) SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING

[Withdrawn: Incorporated into SR-3.]

(4) SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS

[Withdrawn: Moved to SR-3(1).]

(5) SUPPLY CHAIN PROTECTION | LIMITATION OF HARM

[Withdrawn: Moved to SR-3(2).]

(6) SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME

[Withdrawn: Incorporated into SR-5(1).]

(7) SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE

[Withdrawn: Moved to SR-5(2).]

(8) SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE

[Withdrawn: Incorporated into RA-3(2).]

(9) SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY

[Withdrawn: Moved to SR-7.]

(10) SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED

[Withdrawn: Moved to SR-4(3).]

(11) SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS

[Withdrawn: Moved to SR-6(1).]

(12) SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS

[Withdrawn: Moved to SR-8.]

(13) SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS

[Withdrawn: Incorporated into MA-6 and RA-9.]

(14) SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY

[Withdrawn: Moved to SR-4(1) and SR-4(2).]

(15) SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

[Withdrawn: Incorporated into SR-3.]

SA-13 TRUSTWORTHINESS

[Withdrawn: Incorporated into SA-8.]

SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS

[Withdrawn: Incorporated into RA-9.]

Control Enhancements:

(1) CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING

[Withdrawn: Incorporated into SA-20.]

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control:

a. Require the developer of the system, system component, or system service to follow a documented development process that:

   1. Explicitly addresses security and privacy 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, tool options, and tool configurations on at least an annual basis and following an environmental change to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy the following security and privacy requirements: organization-defined security and privacy requirements.

Discussion: Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Related Controls: MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9.

Control Enhancements:

(1) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS

[Withdrawn: Not applicable to COV.]

(2) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY AND PRIVACY TRACKING TOOLS

[Withdrawn: Not applicable to COV.]

(3) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS

[Withdrawn: Not applicable to COV.]

(4) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING AND VULNERABILITY ANALYSIS

[Withdrawn: Incorporated into SA-11(2).]

(5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION

Require the developer of the system, system component, or system service to reduce attack surfaces to the requirements set forth by the Enterprise Architecture Standard.

Discussion: Attack surface reduction is closely aligned with threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services. Attack surface reduction includes implementing the concept of layered defenses, applying the principles of least privilege and least functionality, applying secure software development practices, deprecating unsafe functions, reducing entry points available to unauthorized users, reducing the amount of code that executes, and eliminating application programming interfaces (APIs) that are vulnerable to attacks.

Related Controls: AC-6, CM-7, RA-3, SA-11.

(6) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT

[Withdrawn: Not applicable to COV.]

(7) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS

[Withdrawn: Not applicable to COV.]

(8) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT AND VULNERABILITY INFORMATION

Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Discussion: Analysis of vulnerabilities found in similar software applications can inform potential design and implementation issues for systems under development. Similar systems or system components may exist within developer organizations. Vulnerability information is available from a variety of public and private sector sources, including the NIST National Vulnerability Database.

Related Controls: None.

(9) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA

[Withdrawn: Incorporated into SA-3(2).]

(10) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN

[Withdrawn: Not applicable to COV.]

(11) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE SYSTEM OR COMPONENT

Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.

Discussion: Archiving system or system components requires the developer to retain key development artifacts, including hardware specifications, source code, object code, and relevant documentation from the development process that can provide a readily available configuration baseline for system and component upgrades or modifications.

Related Controls: CM-2.

(12) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION

Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.

Discussion: Organizations can minimize the risk to an individual's privacy by using techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information in development and test environments helps reduce the level of privacy risk created by a system.

Related Controls: PM-25, SA-3, SA-8.

SA-16 DEVELOPER-PROVIDED TRAINING

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

Discussion: Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Organizations can also request 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 and privacy functions, controls, and mechanisms.

Related Controls: AT-2, AT-3, PE-3, SA-4, SA-5.

Control Enhancements: None.

SA-17 DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN

Control: Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

a. Is consistent with the organization's security and privacy architecture that is an integrated part of the organization's enterprise architecture;

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

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

Discussion: Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-8 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA-17 and PL-8 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization. [ISO 15408-2], [ISO 15408-3], and [SP 800-160-1] provide information on security architecture and design, including formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

Related Controls: PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.

Control Enhancements:

(1) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL

[Withdrawn: Not applicable to COV.]

(2) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS

Require the developer of the system, system component, or system service to:

(a) Define security-relevant hardware, software, and firmware; and

(b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

Discussion: The security-relevant hardware, software, and firmware represent the portion of the system, component, or service that is trusted to perform correctly to maintain required security properties.

Related Controls: AC-25, SA-5.

(3) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE

[Withdrawn: Not applicable to COV.]

(4) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE

[Withdrawn: Not applicable to COV.]

(5) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN

[Withdrawn: Not applicable to COV.]

(6) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Discussion: Applying the security design principles in [SP 800-160-1] promotes complete, consistent, and comprehensive testing and evaluation of systems, system components, and services. The thoroughness of such testing contributes to the evidence produced to generate an effective assurance case or argument as to the trustworthiness of the system, system component, or service.

Related Controls: SA-5, SA-11.

(7) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Discussion: The principle of least privilege states that each component is allocated sufficient privileges to accomplish its specified functions but no more (see SA-8(14)). Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects. First, the security impact of a failure, corruption, or misuse of the system component results in a minimized security impact. Second, the security analysis of the component is simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has a need to view the audit data that has been collected but no need to perform operations on that data.

In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated upon by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality, and the access modes to the elements (e.g., read, write) are minimal.

Related Controls: AC-5, AC-6, SA-8.

(8) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | ORCHESTRATION

[Withdrawn: Not applicable to COV.]

(9) DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | DESIGN DIVERSITY

[Withdrawn: Not applicable to COV.]

SA-18 TAMPER RESISTANCE AND DETECTION

[Withdrawn: Moved to SR-9.]

Control Enhancements:

(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE

[Withdrawn: Moved to SR-9(1).]

(2) TAMPER RESISTANCE AND DETECTION | INSPECTION OF SYSTEMS OR COMPONENTS

[Withdrawn: Moved to SR-10.]

SA-19 COMPONENT AUTHENTICITY

[Withdrawn: Moved to SR-11.]

Control Enhancements:

(1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING

[Withdrawn: Moved to SR-11(1).]

(2) COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR

[Withdrawn: Moved to SR-11(2).]

(3) COMPONENT AUTHENTICITY | COMPONENT DISPOSAL

[Withdrawn: Moved to SR-12.]

(4) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING

[Withdrawn: Moved to SR-11(3).]

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:

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

b. Provide the following options for alternative sources for continued support for unsupported system components: an approved contract with an external provider.

Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks, or implementing other forms of isolation.

Related Controls: PL-2, SA-3.

Control Enhancements:

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

[Withdrawn: Incorporated into SA-22.]

SA-23 SPECIALIZATION

[Withdrawn: Not applicable to COV.]

8.18 SYSTEM AND COMMUNICATIONS PROTECTION

SC-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level system and communications protection policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;
b. Designate an Information Security Officer to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and
c. Review and update the current system and communications protection:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SA-8, SI-12.

Control Enhancements: None.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Control: Separate user functionality, including user interface services, from system management functionality.

Discussion: System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating

administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

Related Controls: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

Control Enhancements:

(1) SEPARATION OF SYSTEM AND USER FUNCTIONALITY | INTERFACES FOR NON-PRIVILEGED USERS

[Withdrawn: Not applicable to COV.]

(2) SEPARATION OF SYSTEM AND USER FUNCTIONALITY | DISASSOCIABILITY

Store state information from applications and software separately.

Discussion: If a system is compromised, storing applications and software separately from state information about users' interactions with an application may better protect individuals' privacy.

Related Controls: None.

SC-3 SECURITY FUNCTION ISOLATION

Control: Isolate security functions from nonsecurity functions.

Discussion: Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

Related Controls: AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.

Control Enhancements:

(1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION

[Withdrawn: Not applicable to COV.]

(2) SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS

[Withdrawn: Not applicable to COV.]

(3) SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY

[Withdrawn: Not applicable to COV.]

(4) SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS

[Withdrawn: Not applicable to COV.]

(5) SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES

[Withdrawn: Not applicable to COV.]

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

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

Discussion: Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related Controls: AC-3, AC-4, SA-8.

Control Enhancements:

(1) INFORMATION IN SHARED *SYSTEM* RESOURCES | SECURITY LEVELS

[Withdrawn: Incorporated into SC-4.]

(2) INFORMATION IN SHARED *SYSTEM* RESOURCES | MULTILEVEL OR PERIODS PROCESSING

[Withdrawn: Not applicable to COV.]

SC-5 DENIAL-OF-SERVICE PROTECTION

Control:

a. Protect against or limit the effects of the following types of denial-of-service events: resource exhaustion, amplification attack, and organization-defined types of denial-of-service events; and

b. Employ the following controls to achieve the denial-of-service objective: application firewall and additional organization-defined controls by type of denial-of-service events.

Discussion: Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

Related Controls: CP-2, IR-4, SC-6, SC-7, SC-40.

Control Enhancements:

(1) DENIAL-OF-SERVICE PROTECTION | RESTRICT ABILITY TO ATTACK OTHER SYSTEMS

Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: all denial-of-service attacks except for system testing purposes.

Discussion: Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against

individuals having the ability to launch denial-of-service attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.

Related Controls: None.

(2) DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.

Discussion: Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.

Related Controls: None.

(3) DENIAL-OF-SERVICE PROTECTION | DETECTION AND MONITORING

(a) Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: intrusion detection and application firewall; and

(b) Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: organization-defined system resources.

Discussion: Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles. Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

Related Controls: CA-7, SI-4.

SC-6 RESOURCE AVAILABILITY

Control: Protect the availability of resources by allocating organization-defined resources by priority.

Discussion: Priority protection prevents lower-priority processes from delaying or interfering with the system that services higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources.

Related Controls: SC-5.

Control Enhancements: None.

SC-7 BOUNDARY PROTECTION

Control:

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

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

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

Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal

networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. [SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Related Controls: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP- 8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.

Control Enhancements:

(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS

[Withdrawn: Incorporated into SC-7.]

(2) BOUNDARY PROTECTION | PUBLIC ACCESS

[Withdrawn: Incorporated into SC-7.]

(3) BOUNDARY PROTECTION | ACCESS POINTS

Limit the number of external network connections to the system.

Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection [DHS TIC] initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

Related Controls: None.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

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

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

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

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

(e) Review exceptions to the traffic flow policy at least on an annual basis and following an environmental change and remove exceptions that are no longer supported by an explicit mission or business need;

(f) Prevent unauthorized exchange of control plane traffic with external networks;

(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

(h) Filter unauthorized control plane traffic from external networks.

Discussion: External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol

(BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Related Controls: AC-3, SC-8, SC-20, SC-21, SC-22.

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

Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

Discussion: Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Related Controls: None.

(6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES

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

(7) BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using a Commonwealth Security and Risk Management approved solution.

Discussion: Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

Related Controls: None.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Route organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.

Discussion: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for “man-in-the-middle” attacks (depending on the implementation).

Related Controls: AC-3.

(9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

(a) Detect and deny outgoing communications traffic posing a threat to external systems; and
(b) Audit the identity of internal users associated with denied communications.

Discussion: Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out within the system at managed interfaces. Extrusion detection includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code. Organizations have criteria to determine, update, and manage identified threats related to extrusion detection.

Related Controls: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.

(10) BOUNDARY PROTECTION | PREVENT EXFILTRATION

[Withdrawn: Not applicable to COV.]

(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Only allows incoming communications from organization-defined authorized sources to be routed to organization-defined authorized destinations.

Discussion: General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs. Strong authentication of network addresses is not possible without the use of explicit security protocols, and thus, addresses can often be spoofed. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.

Related Controls: AC-3.

(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

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

Discussion: Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

Related Controls: None.

(13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

Isolate organization-defined information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Discussion: Physically separate subnetworks with managed interfaces are useful in isolating computer network defenses from critical operational processing networks to prevent

adversaries from discovering the analysis and forensics techniques employed by organizations.

Related Controls: SC-2, SC-3.

(14) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

[Withdrawn: Not applicable to COV.]

(15) BOUNDARY PROTECTION | NETWORKED PRIVILEGED ACCESSES

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Discussion: Privileged access provides greater accessibility to system functions, including security functions. Adversaries attempt to gain privileged access to systems through remote access to cause adverse mission or business impacts, such as by exfiltrating information or bringing down a critical system capability. Routing networked, privileged access requests through a dedicated, managed interface further restricts privileged access for increased access control and auditing.

Related Controls: AC-2, AC-3, AU-2, SI-4.

(16) BOUNDARY PROTECTION | PREVENT DISCOVERY OF SYSTEM COMPONENTS

[Withdrawn: Not applicable to COV.]

(17) BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

[Withdrawn: Not applicable to COV.]

(18) BOUNDARY PROTECTION | FAIL SECURE

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Discussion: Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.

Related Controls: CP-2, CP-12, SC-24.

(19) BOUNDARY PROTECTION | BLOCK COMMUNICATIONS FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS

Block inbound and outbound communications traffic between organization- defined communication clients that are independently configured by end users and external service providers.

Discussion: Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

Related Controls: None.

(20) BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION

[Withdrawn: Not applicable to COV.]

(21) BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS

[Withdrawn: Not applicable to COV.]

(22) BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS

[Withdrawn: Not applicable to COV.]

(23) BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE

[Withdrawn: Not applicable to COV.]

(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION

[Withdrawn: Not applicable to COV.]

(25) BOUNDARY PROTECTION | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Not applicable to COV.]

(26) BOUNDARY PROTECTION | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Not applicable to COV.]

(27) BOUNDARY PROTECTION | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Not applicable to COV.]

(28) BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS

Prohibit the direct connection of organization-defined system to a public network.

Discussion: A direct connection is a dedicated physical or virtual connection between two or more systems. A public network is a network accessible to the public, including the Internet and organizational extranets with public access.

Related Controls: None.

(29) BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS

Implement logically separate subnetworks to isolate the following critical system components and functions: organization-defined critical system components and functions.

Discussion: Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command and control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in the trustworthiness of critical system functions.

Related Controls: None.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: Protect the confidentiality and integrity of transmitted information.

Discussion: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through

appropriate contracting vehicles, organizations can implement appropriate compensating controls.

Related Controls: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC- 20, SC-23, SC-28.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

Discussion: Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related Controls: SC-12, SC-13.

(2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE- AND POST-TRANSMISSION HANDLING

[Withdrawn: Not applicable to COV.]

(3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS

[Withdrawn: Not applicable to COV.]

(4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS

[Withdrawn: Not applicable to COV.]

(5) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PROTECTED DISTRIBUTION SYSTEM

[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.

a. Require the use of encryption or digital signatures for the transmission of email and attached data that is sensitive relative to integrity; and

b. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8.]

SC-10 NETWORK DISCONNECT

Control: Terminate the network connection associated with a communications session at the end of the session or after 15 minutes of inactivity.

Discussion: Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level

network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Related Controls: AC-17, SC-23.

Control Enhancements: None.

SC-11 TRUSTED PATH

[Withdrawn: Not applicable to COV.]

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: Commonwealth Security and Risk Management approved key management services, generation, distribution, storage, access, and destruction.

Discussion: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. [NIST CMVP] and [NIST CAVP] provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

Related Controls: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.

Control Enhancements:

(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

Maintain availability of information in the event of the loss of cryptographic keys by users.

Discussion: Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

Related Controls: None.

(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

Produce, control, and distribute symmetric cryptographic keys using NIST FIPS 140-3 validated key management technology and processes.

Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and [SP 800-57-3] provide guidance on cryptographic key management.

Related Controls: None.

(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS

Produce, control, and distribute asymmetric cryptographic keys using certificates issued in accordance with organization-defined requirements.

Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and [SP 800-57-3] provide guidance on cryptographic key management.

Related Controls: None.

(4) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES

[Withdrawn: Incorporated into SC-12(3).]

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

[Withdrawn: Incorporated into SC-12(3).]

(6) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PHYSICAL CONTROL OF KEYS

[Withdrawn: Not applicable to COV.]

SC-12-COV

Control:

a. ~~1.~~ Define the process for the creation and storage of any cryptographic keying material used to protect organization-defined information rated sensitive for confidential or integrity Agency practices for selecting and deploying encryption technologies and for the encryption of data; *and*

b. ~~2.~~ Document the procedure for the creation and storage of any cryptographic keying material used to protect organization-defined information rated sensitive for confidential or integrity.~~; and~~

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SC-13 ~~USE OF CRYPTOGRAPHY~~ CRYPTOGRAPHIC PROTECTION

Control:

a. Determine the cryptographic uses to protect sensitive data; and

b. Implement the following types of cryptography required for each specified cryptographic use: FIPS-validated cryptography for the uses prescribed in SC-13-a.

Discussion: Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation.

Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI- 7.

Control Enhancements:

(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:

a. Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data;

b. Document appropriate processes before implementing encryption. These processes must include the following components:

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

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

   3. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances; and

c. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, and SI-10.]

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

Control:

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: computer support that a user explicitly approves; and
b. Provide an explicit indication of use to users physically present at the devices.

Discussion: Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Related Controls: AC-21, SC-42.

Control Enhancements:

(1) COLLABORATIVE COMPUTING DEVICES | PHYSICAL OR LOGICAL DISCONNECT

Provide physical or logical disconnect of collaborative computing devices in a manner that supports ease of use.

Discussion: Failing to disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures. Disconnect from collaborative computing devices can be manual or automatic.

Related Controls: None.

(2) COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND AND OUTBOUND COMMUNICATION TRAFFIC

[Withdrawn: Incorporated into SC-7.]

(3) COLLABORATIVE COMPUTING DEVICES | DISABLING AND REMOVAL IN SECURE WORK AREAS

[Withdrawn: Not applicable to COV.]

(4) COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS

Provide an explicit indication of current participants in all online meetings and teleconferences.

Discussion: Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

Related Controls: None.

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

[Withdrawn: Not applicable to COV.]

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control:

a. Issue public key certificates under an approved organization-defined certificate policy or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Discussion: Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Related Controls: AU-10, IA-5, SC-12.

Control Enhancements: None.

SC-18 MOBILE CODE

Control:

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

b. Authorize, monitor, and control the use of mobile code within the system.

Discussion: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Related Controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements:

(1) MOBILE CODE | IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS

[Withdrawn: Not applicable to COV.]

(2) MOBILE CODE | ACQUISITION, DEVELOPMENT, AND USE

[Withdrawn: Not applicable to COV.]

(3) MOBILE CODE | PREVENT DOWNLOADING AND EXECUTION

[Withdrawn: Not applicable to COV.]

(4) MOBILE CODE | PREVENT AUTOMATIC EXECUTION

[Withdrawn: Not applicable to COV.]

(5) MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS

[Withdrawn: Not applicable to COV.]

SC-19 VOICE OVER INTERNET PROTOCOL

[Withdrawn: Technology-specific; addressed as any other technology or protocol.]

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

Control:

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

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Discussion: Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related Controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements:

(1) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES

[Withdrawn: Incorporated into SC-20.]

(2) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN AND INTEGRITY

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

Discussion: None.

Related Controls: None.

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

Control: Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Discussion: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Related Controls: SC-20, SC-22.

Control Enhancements: ~~None.~~

(1) SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN AND INTEGRITY

[Withdrawn: Incorporated into SC-21.]

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

Control: Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Discussion: Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

Related Controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

SC-23 SESSION AUTHENTICITY

Control: Protect the authenticity of communications sessions.

Discussion: Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions.

Related Controls: AU-10, SC-8, SC-10, SC-11.

Control Enhancements:

(1) SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT

[Withdrawn: Not applicable to COV.]

(2) SESSION AUTHENTICITY | USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS

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

(3) SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS

Generate a unique session identifier for each session with randomness and recognize only session identifiers that are system-generated.

Discussion: Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Related Controls: AC-10, SC-12, SC-13.

(4) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

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

(5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

Only allow the use of approved certificate authorities for verification of the establishment of protected sessions.

Discussion: Reliance on certificate authorities for the establishment of secure sessions includes the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

Related Controls: SC-12, SC-13.

SC-24 FAIL IN KNOWN STATE

[Withdrawn: Not applicable to COV.]

SC-25 THIN NODES

[Withdrawn: Not applicable to COV.]

SC-26 DECOYS

[Withdrawn: Not applicable to COV.]

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

[Withdrawn: Not applicable to COV.]

SC-28 PROTECTION OF INFORMATION AT REST

Control: Protect the confidentiality and integrity of the following information at rest: sensitive information.

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

Related Controls: AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC- 8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on any system or system components: sensitive information based on confidentiality or integrity.

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Related Controls: AC-19, SC-12, SC-13.

(2) PROTECTION OF INFORMATION AT REST | OFFLINE STORAGE

[Withdrawn: Not applicable to COV.]

(3) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC KEYS

[Withdrawn: Not applicable to COV.]

SC-29 HETEROGENEITY

[Withdrawn: Not applicable to COV.]

SC-30 CONCEALMENT AND MISDIRECTION

[Withdrawn: Not applicable to COV.]

SC-31 COVERT CHANNEL ANALYSIS

[Withdrawn: Not applicable to COV.]

SC-32 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 EXTERNAL MALICIOUS CODE IDENTIFICATION

[Withdrawn: Not applicable to COV.]

SC-36 DISTRIBUTED PROCESSING AND STORAGE

[Withdrawn: Not applicable to COV.]

SC-37 OUT-OF-BAND CHANNELS

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

Discussion: Out-of-band channels include local, non-network accesses to systems; network paths physically separate from network paths used for operational traffic; or non-electronic paths, such as the U.S. Postal Service. The use of out-of-band channels is contrasted with the use of in-band channels (i.e., the same channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability or exposure as in-band channels. Therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of organizational items, including authenticators and credentials; cryptographic key management information; system and data backups; configuration management changes for

hardware, firmware, or software; security updates; maintenance information; and malicious code protection updates.

Related Controls: AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements:

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

Employ organization-defined controls to ensure that only organization-defined individuals or systems receive the following information, system components, or devices: organization-defined information, system components, or devices.

Discussion: Techniques employed by organizations to ensure that only designated systems or individuals receive certain information, system components, or devices include sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

Related Controls: None.

SC-38 OPERATIONS SECURITY

[Withdrawn: Not applicable to COV.]

SC-39 PROCESS ISOLATION

Control: Maintain a separate execution domain for each executing system process.

Discussion: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

Related Controls: AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.

Control Enhancements:

(1) PROCESS ISOLATION | HARDWARE SEPARATION

[Withdrawn: Not applicable to COV.]

(2) PROCESS ISOLATION | SEPARATE EXECUTION DOMAIN PER THREAD

[Withdrawn: Not applicable to COV.]

SC-40 WIRELESS LINK PROTECTION

[Withdrawn: Not applicable to COV.]

SC-41 PORT AND I/O DEVICE ACCESS

[Withdrawn: Not applicable to COV.]

SC-42 SENSOR CAPABILITY AND DATA

Control:

a. Prohibit the remote activation of environmental sensing capabilities on organizational systems or system components with the following exception: Agency Head approved policy, indicating business functions that cannot be accomplished without the use of the capability; and

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

Discussion: Sensor capability and data applies to types of systems or system components characterized as mobile devices, such as cellular telephones, smart phones, and tablets. Mobile devices often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include microphones, cameras, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the movements of an individual. Organizations may prohibit individuals from bringing cellular telephones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

Related Controls: SC-15.

Control Enhancements:

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

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

Discussion: In situations where sensors are activated by authorized individuals, it is still possible that the data or information collected by the sensors will be sent to unauthorized entities.

Related Controls: None.

(2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

Employ the following measures so that data or information collected by organization-defined sensors is only used for authorized purposes: organization-defined measures.

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

Related Controls: PT-2.

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

[Withdrawn: Incorporated into SC-42.]

(4) SENSOR CAPABILITY AND DATA | NOTICE OF COLLECTION

[Withdrawn: Not applicable to COV.]

(5) SENSOR CAPABILITY AND DATA | COLLECTION MINIMIZATION

[Withdrawn: Not applicable to COV.]

SC-42-COV

Control:

a. ~~1)~~ Permits the remote activation of environmental sensing capabilities if required as part of an authorized incident response activity; and

b. ~~2)~~ Only provides an explicit indication of the sensor use if authorized by the incident response team.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SC-43 USAGE RESTRICTIONS

Control:

a. Establish usage restrictions and implementation guidance for the following system components: as defined in SEC528; and

b. Authorize, monitor, and control the use of such components within the system.

Discussion: Usage restrictions apply to all system components including but not limited to mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.

Related Controls: AC-18, AC-19, CM-6, SC-7, SC-18.

Control Enhancements: None.

SC-44 DETONATION CHAMBERS

Control: Employ a detonation chamber capability within systems supporting incident response activities.

Discussion: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

Related Controls: SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7.

Control Enhancements: None.

SC-45 SYSTEM TIME SYNCHRONIZATION

Control: Synchronize system clocks within and between systems and system components.

Discussion: Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities—such as access control and identification and authentication—depending on the nature of the mechanisms used to support the capabilities.

Related Controls: AC-3, AU-8, IA-2, IA-8.

Control Enhancements:

(1) SYSTEM TIME SYNCHRONIZATION | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

(a) Compare the internal system clocks at least every 1024 seconds with Commonwealth approved time servers; and

(b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 100 milliseconds.

Discussion: Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

Related Controls: None.

(2) SYSTEM TIME SYNCHRONIZATION | SECONDARY AUTHORITATIVE TIME SOURCE

(a) Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and

(b) Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

Discussion: It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.

Related Controls: None.

SC-46 CROSS DOMAIN POLICY ENFORCEMENT

Control: Implement a policy enforcement mechanism logically between the physical and/or network interfaces for the connecting security domains.

Discussion: For logical policy enforcement mechanisms, organizations avoid creating a logical path between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation afforded by the physical implementation of policy enforcement to preclude the presence of logical covert channels penetrating the security domain may be needed.

Related Controls: AC-4, SC-7.

Control Enhancements: None.

SC-47 ALTERNATE COMMUNICATIONS PATHS

Control: Establish organization-defined alternate communications paths for system operations organizational command and control.

Discussion: An incident, whether adversarial- or nonadversarial-based, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. To compound the problem, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communications path incident, can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communications paths for command and control purposes, including designating alternative decision makers if primary decision makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization's ability to continue to operate and take appropriate actions during an incident.

Related Controls: CP-2, CP-8.

Control Enhancements: None.

SC-48 SENSOR RELOCATION

[Withdrawn: Not applicable to COV.]

SC-49 HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

[Withdrawn: Not applicable to COV.]

SC-50 SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

Control: Implement software-enforced separation and policy enforcement mechanisms between organization-defined security domains.

Discussion: System owners may require additional strength of mechanism to ensure domain separation and policy enforcement for specific types of threats and environments of operation.

Related Controls: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49.

Control Enhancements: None.

SC-51 HARDWARE-BASED PROTECTION

[Withdrawn: Not applicable to COV.]

8.19 SYSTEM AND INFORMATION INTEGRITY

SI-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to the appropriate organization-defined personnel:
    1. Organization-level system and information integrity policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;
b. Designate an Information Security Officer to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and
c. Review and update the current system and information integrity:
    1. Policy on an annual basis and following an environmental change; and
    2. Procedures on an annual basis and following an environmental change.

Discussion: System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SA-8, SI-12.

Control Enhancements: None.

SI-2 FLAW REMEDIATION

Control:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within ~~at least~~ 30 days or within a timeframe approved by Commonwealth Security and Risk Management of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

Discussion: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI- 5, SI-7, SI-11.

Control Enhancements:

(1) FLAW REMEDIATION | CENTRAL MANAGEMENT

[Withdrawn: Incorporated into PL-9.]

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Determine if system components have applicable security-relevant software and firmware updates installed using Commonwealth Security and Risk Management approved automated mechanisms within ~~at least~~ 30 days.

Discussion: Automated mechanisms can track and determine the status of known flaws for system components.

Related Controls: CA-7, SI-4.

(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions: within ~~at least~~ 30 days.

Discussion: Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

Related Controls: None.

(4) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS

Employ automated patch management tools to facilitate flaw remediation to the following system components: organization-defined system components.

Discussion: Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.

Related Controls: None.

(5) FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES

Install security-relevant software and firmware updates automatically to system components.

Discussion: Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose.

Related Controls: None.

(6) FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE

Remove previous versions of software and firmware components after updated versions have been installed.

Discussion: Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.

Related Controls: None.

SI-2-COV

Control: ~~The organization:~~

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

b. 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).

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SI-3 MALICIOUS CODE PROTECTION

Control:

a. Implement signature or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as 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 system on an organization-defined frequency and real-time scans of files from external sources at endpoint, network entry, and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and

   2. Block malicious code and send alert to administrator and Information Security Officer 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 system.

Discussion: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious

code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

Control Enhancements:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

[Withdrawn: Incorporated into PL-9.]

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

[Withdrawn: Incorporated into SI-3.]

(3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS

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

(4) MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS

[Withdrawn: Not applicable to COV.]

(5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7.]

(6) MALICIOUS CODE PROTECTION | TESTING AND VERIFICATION

(a) Test malicious code protection mechanisms at least on an annual basis by introducing known benign code into the system; and

(b) Verify that the detection of the code and the associated incident reporting occur.

Discussion: None.

Related Controls: CA-2, CA-7, RA-5.

(7) MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION

[Withdrawn: Incorporated into SI-3.]

(8) MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS

[Withdrawn: Not applicable to COV.]

(9) MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS

[Withdrawn: Moved to AC-17(10).]

(10) MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS

(a) Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: Commonwealth Security and Risk Management approved tools and techniques; and

(b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

Discussion: The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by employing reverse engineering techniques or by monitoring the behavior of executing code.

Related Controls: None.

SI-3-COV

Control:

a. 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.);

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

c. 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;

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

1. Eliminates, blocks, or quarantines malicious programs that it detects;

2. Provides an alert notification;

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

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

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

6. Maintains a log of protection activities;

e. 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;

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

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

h. 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;

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

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

k. 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; and

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

Discussion: None.

Related Controls: None.

Control Enhancements: None.

SI-4 SYSTEM MONITORING

Control:

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: organization-defined monitoring objectives; and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: organization-defined techniques and methods;

c. [Withdrawn: Not applicable to COV.];

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide organization-defined system monitoring information to information security personnel as needed.

Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP

proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.

Control Enhancements:

(1) SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system.

Discussion: Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

Related Controls: None.

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: PM-23, PM-25.

(3) SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION

[Withdrawn: Not applicable to COV.]

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic in real time for organization-defined unusual or unauthorized activities or conditions.

Discussion: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Related Controls: None.

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Alert information security personnel when the following system-generated indicators of compromise or potential compromise occur: organization-defined compromise indicators.

Discussion: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related Controls: AU-4, AU-5, PE-6.

(6) SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS

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

(7) SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

[Withdrawn: Not applicable to COV.]

(8) ~~INFORMATION~~ SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION

[Withdrawn: Incorporated into SI-4.]

(9) SYSTEM MONITORING | TESTING OF MONITORING TOOLS AND MECHANISMS

Test intrusion-monitoring tools and mechanisms at least on an annual basis.

Discussion: Testing intrusion-monitoring tools and mechanisms is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency and depth of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

Related Controls: None.

(10) SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS

[Withdrawn: Not applicable to COV.]

(11) SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Analyze outbound communications traffic at the external interfaces to the system and selected organization-defined interior points within the system to discover anomalies.

Discussion: Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

Related Controls: None.

(12) SYSTEM MONITORING | AUTOMATED ORGANIZATION-GENERATED ALERTS

[Withdrawn: Not applicable to COV.]

(13) SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS

(a) Analyze communications traffic and event patterns for the system;

(b) Develop profiles representing common traffic and event patterns; and

(c) Use the traffic and event profiles in tuning system-monitoring devices.

Discussion: Identifying and understanding common communications traffic and event patterns help organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.

Related Controls: None.

(14) SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Discussion: Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

Related Controls: AC-18, IA-3.

(15) SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

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

Discussion: Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given the greater facility of unauthorized network access via wireless access points compared to unauthorized wired network access from within the physical boundaries of the system, additional monitoring of transitioning traffic between wireless and wired networks may be necessary to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps to ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.

Related Controls: AC-18.

(16) SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

Correlate information from monitoring tools and mechanisms employed throughout the system.

Discussion: Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation—including malicious code protection software, host monitoring, and network monitoring—can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Related Controls: AU-6.

(17) SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS

[Withdrawn: Not applicable to COV.]

(18) SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION

[Withdrawn: Not applicable to COV.]

(19) SYSTEM MONITORING | RISK FOR INDIVIDUALS

[Withdrawn: Not applicable to COV.]

(20) SYSTEM MONITORING | PRIVILEGED USERS

[Withdrawn: Not applicable to COV.]

(21) SYSTEM MONITORING | PROBATIONARY PERIODS

[Withdrawn: Not applicable to COV.]

(22) SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

(a) Detect network services that have not been authorized or approved by information security personnel; and

(b) Alert information security personnel when detected.

Discussion: Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

Related Controls: CM-7.

(23) SYSTEM MONITORING | HOST-BASED DEVICES

Implement the following host-based monitoring mechanisms at organization-defined system components: organization-defined host-based monitoring mechanisms.

Discussion: Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

Related Controls: AC-18, AC-19.

(24) SYSTEM MONITORING | INDICATORS OF COMPROMISE

Discover, collect, and distribute to information security personnel, indicators of compromise provided by Commonwealth Security and Risk Management approved sources.

Discussion: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffic include Universal Resource Locator or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Threat indicators, signatures, tactics, techniques, procedures, and other indicators of compromise may be available via government and non-government cooperatives, including the Forum of Incident Response and Security Teams, the United States Computer Emergency Readiness Team, the Defense Industrial Base Cybersecurity Information Sharing Program, and the CERT Coordination Center.

Related Controls: AC-18.

(25) SYSTEM MONITORING | OPTIMIZE NETWORK TRAFFIC ANALYSIS

[Withdrawn: Not applicable to COV.]

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control:

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

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

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

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

Discussion: The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Related Controls: PM-15, RA-5, SI-2.

Control Enhancements:

(1) SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES

[Withdrawn: Not applicable to COV.]

SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION

Control:

a. Verify the correct operation of organization-defined security and privacy functions;

b. Perform this verification of the functions specified in SI-6a at organization-defined system transitional states, upon command by user with appropriate privilege, or at least once every 90 days;

c. Alert organization-defined personnel to failed security and privacy verification tests; and

d. Shut the system down when anomalies are discovered.

Discussion: Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

Related Controls: CA-7, CM-4, CM-6, SI-7.

Control Enhancements:

(1) SECURITY AND PRIVACY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS

[Withdrawn: Incorporated into SI-6.]

(2) SECURITY AND PRIVACY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING

Implement automated mechanisms to support the management of distributed security and privacy function testing.

Discussion: The use of automated mechanisms to support the management of distributed function testing helps to ensure the integrity, timeliness, completeness, and efficacy of such testing.

Related Controls: SI-2.

(3) SECURITY AND PRIVACY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS

Report the results of security and privacy function verification to the Information Security Officer

Discussion: Organizational personnel with potential interest in the results of the verification of security and privacy functions include systems security officers, senior agency information security officers, and senior agency officials for privacy.

Related Controls: SI-4, SR-4, SR-5.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: organization-defined software, firmware, and information.

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify the Information Security Officer.

Discussion: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

Control Enhancements:

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

Perform an integrity check of organization-defined software, firmware, and information at startup; at organization-defined transitional states or security-relevant events, and at least once every 7 days.

Discussion: Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Related Controls: None.

(2) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

Employ automated tools that provide notification to the Information Security Officer upon discovering discrepancies during integrity verification.

Discussion: The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.

Related Controls: None.

(3) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS

Employ centrally managed integrity verification tools.

Discussion: Centrally managed integrity verification tools provides greater consistency in the application of such tools and can facilitate more comprehensive coverage of integrity verification actions.

Related Controls: AU-3, SI-2, SI-8.

(4) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING

[Withdrawn: Incorporated into SA-12.]

(5) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS

Automatically implement organization-defined controls when integrity violations are discovered.

Discussion: Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Related Controls: None.

(6) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Discussion: Cryptographic mechanisms used to protect integrity include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: organization-defined security-relevant changes to the system.

Discussion: Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related Controls: AU-2, AU-6, IR-4, IR-5, SI-4.

(8) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS

Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: generates an audit record and alert the Information Security Officer.

Discussion: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

Related Controls: AU-2, AU-6, AU-12.

(9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS

Verify the integrity of the boot process of the following system components: organization-defined system components.

Discussion: Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.

Related Controls: SI-6.

(10) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE

Implement the following mechanisms to protect the integrity of boot firmware in organization-defined system components: organization-defined mechanisms.

Discussion: Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.

Related Controls: SI-6.

(11) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

[Withdrawn: Moved to CM-7(6).]

(12) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION

Require that the integrity of the following user-installed software be verified prior to execution: organization-defined user-installed software.

Discussion: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or programs that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity, including the availability of trustworthy checksums from software developers and vendors.

Related Controls: CM-11.

(13) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

[Withdrawn: Moved to CM-7(7).]

(14) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE

[Withdrawn: Moved to CM-7(8).]

(15) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: organization-defined software or firmware components.

Discussion: Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls: CM-5, SC-12, SC-13.

(16) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

Prohibit processes from executing without supervision for more than 24 hours.

Discussion: Placing a time limit on process execution without supervision is intended to apply to processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes timers on

operating systems, automated responses, and manual oversight and response when system process anomalies occur.

Related Controls: None.

(17) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | RUNTIME APPLICATION SELF-PROTECTION

Implement organization-defined controls for application self-protection at runtime.

Discussion: Runtime application self-protection employs runtime instrumentation to detect and block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections such as guards and firewalls which can only detect and block attacks by using network information without contextual awareness. Runtime application self-protection technology can reduce the susceptibility of software to attacks by monitoring its inputs and blocking those inputs that could allow attacks. It can also help protect the runtime environment from unwanted changes and tampering. When a threat is detected, runtime application self-protection technology can prevent exploitation and take other actions (e.g., sending a warning message to the user, terminating the user's session, terminating the application, or sending an alert to organizational personnel). Runtime application self-protection solutions can be deployed in either a monitor or protection mode.

Related Controls: SI-16.

SI-8 SPAM PROTECTION

Control:

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

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

Discussion: System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices.

Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Related Controls: PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

Control Enhancements:

(1) SPAM PROTECTION | CENTRAL MANAGEMENT

[Withdrawn: Incorporated into PL-9.]

(2) SPAM PROTECTION | AUTOMATIC UPDATES

Automatically update spam protection mechanisms at least on a daily basis.

Discussion: Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Related Controls: None.

(3) SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY

Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Discussion: Learning mechanisms include Bayesian filters that respond to user inputs that identify specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

Related Controls: None.

SI-9 INFORMATION INPUT RESTRICTIONS

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

SI-10 INFORMATION INPUT VALIDATION

Control: Check the validity of the following information inputs: organization-defined information inputs to the system.

Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Related Controls: None.

Control Enhancements:

(1) INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY

[Withdrawn: Not applicable to COV.]

(2) INFORMATION INPUT VALIDATION | REVIEW AND RESOLVE ERRORS

Review and resolve input validation errors ~~at least~~ within 30 days of discovery.

Discussion: Resolution of input validation errors includes correcting systemic causes of errors and resubmitting transactions with corrected input. Input validation errors are those related to the information inputs defined by the organization in the base control (SI-10).

Related Controls: None.

(3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR

Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

Discussion: A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. Verification of system predictability helps ensure that the system behaves as expected when invalid inputs are received. This occurs by specifying system responses that allow the system to transition to known states without adverse, unintended side effects. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Related Controls: None.

(4) INFORMATION INPUT VALIDATION | TIMING INTERACTIONS

[Withdrawn: Not applicable to COV.]

(5) INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS

[Withdrawn: Not applicable to COV.]

(6) INFORMATION INPUT VALIDATION | INJECTION PREVENTION

Prevent untrusted data injections.

Discussion: Untrusted data injections may be prevented using a parameterized interface or output escaping (output encoding). Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter's parser whether data is trusted. Prevention of untrusted data injections are with respect to the information inputs defined by the organization in the base control (SI-10).

Related Controls: AC-3, AC-6.

SI-11 ERROR HANDLING

Control:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to the Information Security Officer and appropriate organization-defined personnel.

Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related Controls: AU-2, AU-3, SC-31, SI-2, SI-15.

Control Enhancements: None.

SI-12 INFORMATION MANAGEMENT AND RETENTION

Control: Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

Discussion: Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-1, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.

Related Controls: All XX-1 Controls, AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM- 5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.

Control Enhancements:

(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Withdrawn: Not applicable to COV.]

(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: obfuscation hashing or organization-defined techniques.

Discussion: Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

Related Controls: PM-22, PM-25, SI-19.

(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL

Use the following techniques to dispose of, destroy, or erase information following the retention period: in accordance with SEC514.

Discussion: Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Related Controls: None.

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

Control: Implement the following controls to protect the system memory from unauthorized code execution: malicious code protection and other organization-defined controls.

Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls: AC-25, SC-3, SI-7.

Control Enhancements: None.

SI-17 FAIL-SAFE PROCEDURES

[Withdrawn: Not applicable to COV.]

SI-18 PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS

[Withdrawn: Not applicable to COV.]

SI-19 DE-IDENTIFICATION

[Withdrawn: Not applicable to COV.]

SI-20 TAINTING

Control: Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: organization-defined systems or system components.

Discussion: Many cyber-attacks target organizational information, or information that the organization holds on behalf of other entities (e.g., personally identifiable information), and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system that is in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any packets it includes potentially contain malicious code, and that the unauthorized entity may have potentially obtained a copy of the database. Another tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open-source analysis. Finally, an active tainting approach can include embedding software in the data that is able to "call home," thereby alerting the organization to its "capture," and possibly its location, and the path by which it was exfiltrated or removed.

Related Controls: AU-13.

Control Enhancements: None.

SI-21 INFORMATION REFRESH

[Withdrawn: Not applicable to COV.]

SI-22 INFORMATION DIVERSITY

[Withdrawn: Not applicable to COV.]

SI-23 INFORMATION FRAGMENTATION

[Withdrawn: Not applicable to COV.]

8.20 SUPPLY CHAIN RISK 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 **https://www.vita.virginia.gov/policy--governance/glossary/cov-itrm-glossary/**

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: System Security Plan

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX A – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

COV Hosted Environment Information Security 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 Approved_____ Appeal Denied_____ Comments:

_____ _____

CIO Date