COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Hosted Environment 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 the Enterprise Architecture (EA) Division. EA 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 EA considers interested in the change.

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

Version	Date	Purpose of Revision
01	03/22/2016	Base Document
02	08/11/2016	*The updates to the Hosted Environment Information Security Standard (SEC525-02) remove Section 1.8., which required hosting facilities be located within the Commonwealth of Virginia. However, section PE-18-COV remains and still requires all information system components and services remain within the continental United States unless the COV CISO has granted an exception. Furthermore, the updates amend SI-2-COV to apply security updates ASAP and NLT 30 days for patching (previously stated 60 days which was in conflict with SI-2 and FedRamp)*
03	*09/01/2018*	*General responsibilities were updated to reflect Code of Virginia requirements in the PREFACE.* *New requirements were added to the following controls: CA-8;PE-1-COV* *Clarifying language was added to the following controls: Section 1.5; IA-5; MP-1-COV* *Control inserted that was left out of prior publication: SA-19* *RA-5-COV was removed*

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

Review Process

Enterprise Architecture (EA) Division 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 SEC525-~~01~~03

Subject
Information Security

Effective Date
September 1, 2018

Compliance Date
December 31, 2018

Supersedes
August 11, 2016

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 2.7 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 (Section 9.4 of the standard*)* 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.

~~**Enterprise Solutions and Governance Directorate**~~
~~In accordance with the Code of Virginia § 2.2-2010 the CIO has assigned the Enterprise Solutions and Governance Directorate the following duties: "*Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."~~

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

Table of Contents

1. INTRODUCTION 1
1.1 Intent 1
1.2 Organization of this Standard 2
1.3 Roles and Responsibilities 2
1.4 Information Security Program 2
1.5 Exceptions to Security Requirements 2
1.6 Exemptions from Applicability 3
1.7 Determination of Liability 3
1.8 Restriction of Geographically Location of Commonwealth Data 3
1.9 Revocation of Hosted Computing Permissions 4
2. Information Security Roles and Responsibilities 4
2.1. Purpose 4
2.2. Chief Information Officer of the Commonwealth (CIO) 4
2.3. Chief Information Security Officer (CISO) 4
2.4. Agency Head 5
2.5. Information Security Officer (ISO) 7
2.6. Privacy Officer 7
2.7. System Owner 8
2.8. Data Owner 8
2.9. System Administrator 9
2.10. Data Custodian 9
2.11. IT System Users 9
3. Business Impact Analysis 9
3.1. Purpose 9
3.2. Requirements 10
4. IT System and Data Sensitivity Classification 10
4.1. Purpose 11
4.2. Requirements 11
5. Sensitive IT System Inventory and Definition 12
5.1. Purpose 12
5.2. Requirements 12
6. Risk Assessment 13
6.1. Purpose 13
6.2. Requirements 13
7. IT Security Audits 14
7.1. Purpose 14
7.2. Requirements 14
8. SECURITY CONTROL CATALOG 14
1.1. FAMILY: ACCESS CONTROL CLASS: TECHNICAL 15
1.2. FAMILY: AWARENESS AND TRAINING CLASS: OPERATIONAL 37
1.3. FAMILY: AUDIT AND ACCOUNTABILITY CLASS: TECHNICAL 41
1.4. FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION CLASS: MANAGEMENT 50
1.5. FAMILY: CONFIGURATION MANAGEMENT CLASS: OPERATIONAL 56
1.6. FAMILY: CONTINGENCY PLANNING CLASS: OPERATIONAL 68
1.7. FAMILY: IDENTIFICATION AND AUTHENTICATION CLASS: TECHNICAL ... 82

1.8. FAMILY: INCIDENT RESPONSE CLASS: OPERATIONAL 90
1.9. FAMILY: MAINTENANCE CLASS: OPERATIONAL..... 103
1.10. FAMILY: MEDIA PROTECTION CLASS: OPERATIONAL..... 110
1.11. FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION CLASS: OPERATIONAL 117
1.12. FAMILY: PLANNING CLASS: MANAGEMENT..... 128
1.13. FAMILY: PERSONNEL SECURITY CLASS: OPERATIONAL 135
1.14. FAMILY: RISK ASSESSMENT CLASS: MANAGEMENT 139
1.15. FAMILY: SYSTEM AND SERVICES ACQUISITION CLASS: MANAGEMENT .. 145
1.16. FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION CLASS: TECHNICAL .. 169
1.17. FAMILY: SYSTEM AND INFORMATION INTEGRITY CLASS: OPERATIONAL . 190
Glossary of Security Definitions..... 209
APPENDIX A – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM 211

1. INTRODUCTION

1.1 Intent

The intent of this information security standard is to establish a baseline for information security and risk management activities associated with commonwealth data stored in a data center not owned or leased by 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. 4, 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:

Control Family:	***Page:***
• *AC - Access Control*	*15*
• *AT - Awareness and Training*	*36*
• *AU - Audit and Accountability*	*37*
• *CA - Security Assessment and Authorization*	*40*
• *CM - Configuration Management*	*48*
• *CP - Contingency Planning*	*53*
• *IA - Identification and Authentication*	*67*
• *IR - Incident Response*	*78*
• *MA – Maintenance*	*85*
• *MP - Media Protection*	*99*
• *PE - Physical and Environmental Protection*	*113*
• *PL – Planning*	*123*
• *PS - Personnel Security*	*130*
• *RA - Risk Assessment*	*134*
• *SA - System and Services Acquisition*	*140*

- SC - System and Communications Protection 163
- SI - System and Information Integrity 184
- PM – Program Management 200

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
- Supplemental Guidance
- Control Enhancements for Sensitive Systems
- Previous SEC 501 Control References

1.3 Roles and Responsibilities

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. In addition, because resources that can reasonably be committed to protecting IT systems are limited, each agency must implement its information security program in a manner commensurate with sensitivity and risk.

1.5 Exceptions 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 Agency ISO. Denied exception requests may be appealed to the CIO of the Commonwealth. The form that agencies must use to document exception requests is included in the Appendix to this document.

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
2. Surplus and retired systems

1.7 Determination 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 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 Restriction of Geographically Location of Commonwealth Data~~

~~The Commonwealth of Virginia requires that all data classified as sensitive with respect to confidentiality, integrity, or availability remain within the geographical boundaries of the commonwealth. The policy further stipulates that data classified as sensitive be housed only within facilities owned or leased by the commonwealth. This policy ensures that all sensitive data owned by the commonwealth will be governed by a security architecture standard sufficient to protect the data at all times.~~

NOTE*: Section 1.8., which required hosting facilities be located within the Commonwealth of Virginia has been removed. However, section PE-18-COV remains and still requires all information system components and services remain within the continental United States unless the COV CISO has granted an exception.*

1.9 Revocation of Hosted Computing Permissions

The CIO of the Commonwealth of Virginia reserves the right to revoke an agency' 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

   Note: The ISO should report directly to the Agency Head where practical and should not report to the CIO. The ISO is responsible for developing and managing the agency's information security program. The Agency Head is strongly encouraged to designate at least one backup for the ISO. 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 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. Meet educational requirements necessary to maintain an information security program by meeting all of the following requirements:
   - attending Information Security Orientation training, biennially
   - successfully completing at least 3 course hours per year of security courses authorized by the CISO.
   - possessing a recognized professional IT Security Certification, i.e., CISSP, CISM, CISA, SANS, meeting all requirements of the certification body, may be substituted for two (2) courses.
   - attending one mandatory ISOAG meeting per year, and
   - obtaining an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each!)
     Note: Continuing Profession Education credits (CPE's) for professional IT Security Certifications may be applied to this requirement.

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 has an obligation under the Code of Virginia to 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, and/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.

4.2. Requirements

Each agency ISO shall:

1. Identify or require that the Data Owner identify the type(s) of data handled by each agency IT system.

2. 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.

3. Determine or require that the Data Owner determine the potential damages to the agency of a compromise of confidentiality, integrity or availability 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. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration of one way to accomplish this.

System ID: ABC123	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal	High	High	High

Records			

Table 1: Sample Sensitivity Analysis Results

4. 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.

   Note: Agencies should consider classifying IT systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability.

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

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

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

8. Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public website, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating controls, and all residual risks.

9. 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 is to be given to the ISO for review.

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 CONTROL ORGANIZATION AND STRUCTURE

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 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 supplemental guidance section; and (iii) a Control Enhancements for Sensitive Systems 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 supplemental guidance section provides additional information related to a specific security control, but contains no requirements. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. The supplemental guidance 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 for Sensitive Systems may also contain supplemental guidance. Enhancement supplemental guidance is used in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement.

The security Control Enhancements for Sensitive Systems for sensitive systems section provides statements of security capability to: (i) build in additional functionality to a control; and/or (ii) increase the strength of a control for sensitive systems. In both cases, the Control Enhancements for Sensitive Systems 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 for Sensitive Systems 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 for Sensitive Systems 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.

1.1. FAMILY: ACCESS CONTROL CLASS: TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to all organization personnel, contractors, and service providers with a responsibility to implement access controls:

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

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

b. Reviews and updates the current:

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

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

Supplemental Guidance: Withdrawn: Not applicable to COV

Control Enhancements for Sensitive Systems: None.

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, service, application, guest/anonymous, and temporary;

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

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

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with the agency-defined logical access control policy.

g. Monitors the use of information system accounts;

h. Notifies account managers:

   1. When accounts are no longer required;

   2. When users are terminated or transferred; and

   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information 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. Reviews accounts for compliance with account management requirements on an annual basis or more frequently if required to address an environmental change; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system

and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a 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 (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

The information system automatically terminates temporary and emergency accounts after a predetermined period which is not to exceed 30-days in accordance with sensitivity and risk.

Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

The information system automatically disables inactive accounts after 90 consecutive days of non-use.

(4) [Withdrawn: Not applicable to COV]

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

The organization requires that users log out when the session inactivity time has exceeded 30-minutes.

(6) [WITHDRAWN: NOT APPLICABLE TO COV]

(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES

The organization:

(a) [Withdrawn: Not applicable to COV]

(b) Monitors privileged role assignments; and

(c) Takes the appropriate actions to remove the role privileges when privileged role assignments are no longer appropriate.

Supplemental Guidance: 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. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

(8) [WITHDRAWN: NOT APPLICABLE TO COV]

(9) [WITHDRAWN: NOT APPLICABLE TO COV]

(10) [WITHDRAWN: NOT APPLICABLE TO COV]

(11) [WITHDRAWN: NOT APPLICABLE TO COV]

(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE

The organization:

(a) Monitors information system accounts for atypical or suspicious usage use; and

(b) Reports atypical usage of information system accounts to the agency ISO, agency head, or CISO.

Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.

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

The organization disables accounts of users posing a significant risk within an organizational defined time period of discovery of the risk.

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Commonwealth. Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement. Related control: PS-4.

AC-3 ACCESS ENFORCEMENT

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

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level

and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security

Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

Control Enhancements for Sensitive Systems:

(1) ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6].

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

(6) [Withdrawn: Not applicable to COV]

(7) [Withdrawn: Not applicable to COV]

(8) [Withdrawn: Not applicable to COV]

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

The information system does not release information outside of the established system boundary unless:

(a) The receiving organization authorized information system or system component provides the appropriate organization-defined security safeguards; and

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

Supplemental Guidance: Information systems can only protect organizational information within the confines of established system boundaries. Additional security safeguards may be needed to ensure that such information is adequately protected once it is passed beyond the established information system boundaries. Examples of information leaving the system boundary include transmitting information to an external information system or printing the information on one of its printers. In cases where the information system is unable to make a determination of the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external information systems are providing adequate security. The means used to determine the adequacy of the security provided by external information systems include, for example, conducting inspections or periodic testing, 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 policy to protect the information. This control enhancement requires information systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the information system passes information to another system controlled by another organization, technical means are employed to validate that the security attributes associated with the exported information are appropriate

for the receiving system. Alternatively, if the information system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only appropriately authorized individuals gain access to the printer. This control enhancement is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular information system or organization.

(10) [Withdrawn: Not applicable to COV]

AC-4 INFORMATION FLOW ENFORCEMENT

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

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.
Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control Enhancements for Sensitive Systems 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]
(2) [Withdrawn: Not applicable to COV]
(3) [Withdrawn: Not applicable to COV]
(4) [Withdrawn: Not applicable to COV]
(5) [Withdrawn: Not applicable to COV]
(6) [Withdrawn: Not applicable to COV]
(7) [Withdrawn: Not applicable to COV]
(8) [Withdrawn: Not applicable to COV]
(9) [Withdrawn: Not applicable to COV]
(10) [Withdrawn: Not applicable to COV]
(11) [Withdrawn: Not applicable to COV]
(12) [Withdrawn: Not applicable to COV]
(13) [Withdrawn: Not applicable to COV]
(14) [Withdrawn: Not applicable to COV]
(15) [Withdrawn: Not applicable to COV]
(16) [Withdrawn: Not applicable to COV]
(17) [Withdrawn: Not applicable to COV]
(18) [Withdrawn: Not applicable to COV]
(19) [Withdrawn: Not applicable to COV]
(20) [Withdrawn: Not applicable to COV]
(21) [Withdrawn: Not applicable to COV]
(22) [Withdrawn: Not applicable to COV]

AC-5 SEPARATION OF DUTIES

Control: The organization:

a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: 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, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements for Sensitive Systems: None.

AC-6 LEAST PRIVILEGE

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements for Sensitive Systems:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

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

The organization requires that users of information 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.

Supplemental Guidance: This control enhancement 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 both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges) setting events to be audited, and setting intrusion detection parameters, systems programming, system and security administration, other privileged functions. Related control: PL-4.

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

The organization restricts privileged accounts on the information system to administrative personnel

Supplemental Guidance: 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 having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

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

The organization prohibits privileged access to the information system by non-organizational users or individuals not under the contractual control of the Commonwealth.

Supplemental Guidance: Related control: IA-8.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

The organization:

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

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. 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 control: CA-7.

(8) [Withdrawn: Not applicable to COV]

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing 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 (APT). Related control: AU-2.

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

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

a. Enforces a limit of 3 consecutive invalid logon attempts by a user during a 15 minute period; and

b. Automatically locks the account/node for a minimum of a 30 minute period when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control 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 information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements for Sensitive Systems:

(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK

[Withdrawn: Incorporated into AC-7].

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

The information system purges/wipes information from mobile devices based on organization-defined purging/wiping requirements/techniques after 10 consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/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, SC-13.

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays to users organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices

consistent with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a Commonwealth information system;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
4. Use of the information 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 information system; and

c. For publicly accessible systems:

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

Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Attorney General for legal review and approval of warning banner content.

Control Enhancements for Sensitive Systems: 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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

[Withdrawn: Not applicable to COV]

AC-10 CONCURRENT SESSION CONTROL

[Withdrawn: Not applicable to COV]

AC-11 SESSION LOCK

Control: The information system:

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

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

Control Enhancements for Sensitive Systems:

(1) SESSION LOCK | PATTERN-HIDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a user session after 24 hours of inactivity.

Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are 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 information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.

Control Enhancements for Sensitive Systems:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to information resources; and

(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

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

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization:

a. Identifies restricted user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible Commonwealth information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), 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. This control 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 information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2.

Control Enhancements for Sensitive Systems: 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 ATTRIBUTES

[Withdrawn: Not applicable to COV]

AC-17 REMOTE ACCESS

Control: The organization:

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

b. Authorizes remote access to the information system prior to allowing such connections.

Supplemental Guidance: Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

Control Enhancements for Sensitive Systems:

(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL

The information system monitors and controls remote access methods.

Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers,

workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.

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

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

The information system routes all remote accesses through managed network access control points.

Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for organization-defined needs; and

(b) Documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Related control: AC-6.

(5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4].

(6) REMOTE ACCESS | PROTECTION OF INFORMATION

The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

Supplemental Guidance: 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 / DISABLE ACCESS

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within 15 minutes.

Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business

functions and the need to eliminate immediate or future remote access to organizational information systems.

AC-17-COV

Control: The organization shall:

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

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

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

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

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

6. Where supported by features of the system, session timeouts shall be implemented after a period of not longer than 15 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.

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

   Supplemental Guidance: 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.

Control Enhancements for Sensitive Systems: None

AC-18 WIRELESS ACCESS

Control: The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. Authorizes wireless access to the information system prior to allowing such connections.

Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection

and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

Control Enhancements for Sensitive Systems:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

The information system protects wireless access to the system using authentication and encryption.

Supplemental Guidance: Related controls: SC-8, SC-13.

(2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4].

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

Supplemental Guidance: Related control: AC-19.

(4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15.

(5) WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area. Related control: PE-19.

AC-18-COV

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

Wireless LAN (WLAN) Connectivity on the COV Network

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

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

    b. WLAN infrastructure must authenticate *each* client device prior to permitting access to the WLAN;

    c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;

    d. Only COV owned or leased equipment shall be granted access to an internal WLAN;

    e. 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);

    f. Physical or logical separation between WLAN and wired LAN segments must exist;

    g. All COV WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;

    h. WLAN clients will only permit infrastructure mode communication.

    WLAN Hotspot (Wireless Internet)

2. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:

    a. WLAN Hotspots must have logical or physical separation from the agency's LAN;

    b. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;

    c. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and

    d. Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.

    Wireless Bridging

3. The following network configuration shall be used when bridging two wired LANs:

    a. 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);

    b. Wireless bridging devices will not have a default gateway configured;

    c. Wireless bridging devices must be physically or logically separated from other networks;

    d. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;

    e. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control: The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. Authorizes the connection of mobile devices to organizational information systems.

Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices 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, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation

guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), 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 (e.g., wireless, infrared).

Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

Control Enhancements for Sensitive Systems:

(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) [Withdrawn: Not applicable to COV]

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

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

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and

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

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary

established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by non-Commonwealth governmental organizations; and (iv) Commonwealth information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other Commonwealth agencies, including organizations subordinate to those agencies), 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. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between Commonwealth agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable Commonwealth laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems. Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

Control Enhancements for Sensitive Systems:

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

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

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

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

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

(2) USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES

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

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

(3) USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES

The organization prohibits the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

Supplemental Guidance: Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use.

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

The organization prohibits the use of network accessible storage devices in external information systems.

Supplemental Guidance: Network accessible storage devices in external information systems include, for example, online storage devices in public, hybrid, or community cloud-based systems.

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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

AC-21 INFORMATION SHARING

[Withdrawn: Not applicable to COV]

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;

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

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

d. Reviews the content on the publicly accessible information system for nonpublic information prior to initial posting and at least once a quarter and removes such information, if discovered.

Supplemental Guidance: In accordance with Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.

Control Enhancements for Sensitive Systems: 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]

1.2.*FAMILY:* *AWARENESS AND TRAINING* ***CLASS:*** *OPERATIONAL*

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to all information system users (including managers, senior executives, and contractors):

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;

b. When required by information system changes; and

c. Annually or more often as necessary thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen

messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.

Control Enhancements for Sensitive Systems:

(1) SECURITY AWARENESS | PRACTICAL EXERCISES

The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Supplemental Guidance: Practical exercises may include, for example, 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) SECURITY AWARENESS | INSIDER THREAT

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance: 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 sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.

AT-2-COV

Control:

1. Develop an information security training program so that each IT system user is aware of and understands the following concepts:

   a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;

   b. The concept of separation of duties;

   c. Prevention and detection of information security incidents, including those caused by malicious code;

   d. Proper disposal of data storage media;

   e. Proper use of encryption;

   f. Access controls, including creating and changing passwords and the need to keep them confidential;

   g. Agency acceptable use policies;

h. Agency Remote Access policies;

i. Intellectual property rights, including software licensing and copyright issues;

j. Responsibility for the security of COV data;

k. Phishing;

l. Social engineering; and

m. Least privilege.

2. Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

AT-3 ROLE-BASED SECURITY TRAINING

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;

b. When required by information system changes; and

c. As practical and necessary thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide system owners, data owners, account managers, enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services

to Commonwealth agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for period as defined by the organization's records retention policy.

Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

Control Enhancements for Sensitive Systems: None.

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15].

1.3.*FAMILY:* *AUDIT AND ACCOUNTABILITY* ***CLASS:*** *TECHNICAL*

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization:

(a) Develops, documents, and disseminates to the appropriate organization-defined personnel and roles:

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

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

(b) Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

AU-2 AUDIT EVENTS

Control: The organization:

a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Withdrawn: Not applicable to COV

Supplemental Guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and Control Enhancements for Sensitive Systems. Organizations also include auditable events that are required by applicable Commonwealth laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as

information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

Control Enhancements for Sensitive Systems:

(1) AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

[Withdrawn: Incorporated into AU-12].

(2) AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT

[Withdrawn: Incorporated into AU-12].

(3) AUDIT EVENTS | REVIEWS AND UPDATES

The organization reviews and updates the audited events on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

(4) AUDIT EVENTS | PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6].

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements for Sensitive Systems:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

The information system generates audit records containing the following additional information: time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, event success or failure, and access control or flow control rules invoked**.**

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or

the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

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

The information system provides centralized management and configuration of the content to be captured in audit records generated by all web servers, database servers, messaging servers, file servers, print servers, middleware servers, DNS servers, routers, firewalls, IDS/IPS, and VoIP servers**.**

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity in accordance with the organization-defined audit record storage requirements.

Supplemental Guidance: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Control Enhancements for Sensitive Systems:

(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

The information system off-loads audit records at least once every 30-days onto a different system or media than the system being audited.

Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Withdrawn: Not applicable to COV

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

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

The information system provides an alert in real time to appropriate personnel, to include system owner and business owner when the following audit failure events occur: recording of authentication attempts or escalation of privilege.

Supplemental Guidance: 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).

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

a. Reviews and analyzes information system audit records at least once a week for indications of inappropriate or unusual activity; and

b. Reports findings to designated organizational officials.

Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

Control Enhancements for Sensitive Systems:

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

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.

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

[Withdrawn: Incorporated into SI-4].

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

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4.

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

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. Related controls: AU-2, AU-12.

(5) AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES

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

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information 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 and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber attacks resulting in 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, RA-5.

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

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

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

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

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

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

(8) [Withdrawn: Not applicable to COV]

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

The organization correlates information from nontechnical sources with audit information to enhance organization-wide situational awareness.

Supplemental Guidance: Nontechnical sources include, for example, human resources records documenting organizational policy violations (e.g., sexual harassment incidents, improper use of organizational information assets). Such information can lead organizations to a more directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions. Related control: AT-2.

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

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

Supplemental Guidance: The frequency, scope, and/or depth of the audit review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

[Withdrawn: Not applicable to COV]

AU-8 TIME STAMPS

Control: The information system:

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

b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets the organization-defined granularity of time measurement based on the sensitivity of the system.

Supplemental Guidance: Time stamps generated by the information 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 information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also 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.

Control Enhancements for Sensitive Systems:

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

The information system:

(a) Compares the internal information system clocks every 5-minutes with a Stratum two clock source or better; and

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than 2-seconds.

Supplemental Guidance: This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

(2) [Withdrawn: Not applicable to COV]

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.

Control Enhancements for Sensitive Systems:

(1) Withdrawn: Not applicable to COV

(2) PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS

The information system backs up audit records at least once every 24-hours onto a physically different system or system component than the system or component being audited.

Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.

(3) Withdrawn: Not applicable to COV

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

The organization authorizes access to management of audit functionality to only a limited subset of authorized users .

Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.

(5) Withdrawn: Not applicable to COV

(6) Withdrawn: Not applicable to COV

AU-10 NON-REPUDIATION

Withdrawn: Not applicable to COV

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for consistent with the agency's records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, 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-4, AU-5, AU-9, MP-6.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

AU-12 AUDIT GENERATION

Control: The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2 a. at the operating system, services, applications, and network components;

b. Allows authorized organization personnel to select which auditable events are to be audited by specific components of the information system; and

c. Generates audit records for the events and content defined in AU-3.

Supplemental Guidance: Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control: The organization monitors organization-defined open source information and/or information sites at the appropriate organization-defined frequency for evidence of unauthorized disclosure of organizational information.

Supplemental Guidance: Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.

Control Enhancements for Sensitive Systems:

Withdrawn: Not applicable to COV

AU-14 SESSION AUDIT

[Withdrawn: Not applicable to COV]

AU-15 ALTERNATE AUDIT CAPABILITY
Withdrawn: Not applicable to COV

AU-16 CROSS-ORGANIZATIONAL AUDITING
Withdrawn: Not applicable to COV

1.4.*FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION* ***CLASS:*** *MANAGEMENT*

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

CA-2 SECURITY ASSESSMENTS

[Withdrawn: Not applicable to COV]

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Reviews and updates Interconnection Security Agreements an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those

interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between Commonwealth agencies and non-Commonwealth (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Control Enhancements for Sensitive Systems:

[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:

1. The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:

   a. The types of shared data;

   b. The direction(s) of data flow; and

   c. 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.

2. The System Owners of interconnected systems must inform one another of connections with other systems.

3. The System Owners of interconnected systems must notify each other prior to establishing connections to other systems.

4. The written agreement shall specify if and how the shared data will be stored on each IT system.

5. 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.

6. The written agreement shall specify each Data Owner's authority to approve access to the shared data.

7. The System Owners shall approve and enforce the agreement.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 PLAN OF ACTION AND MILESTONES

[Withdrawn: Not applicable to COV]

CA-6 SECURITY AUTHORIZATION

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently Commonwealth responsibility and therefore, authorizing officials must be Commonwealth employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the

maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements for Sensitive Systems: None.

CA-7 CONTINUOUS MONITORING

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of organization-defined metrics to be monitored;

b. Establishment of organization-defined frequencies for monitoring and organization-defined frequencies for assessments supporting such monitoring;

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

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational 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 security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

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

Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, 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 information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into CA-2.]

(3) CONTINUOUS MONITORING | TREND ANALYSES

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the Commonwealth, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.

CA-8 PENETRATION TESTING

Control: The organization conducts penetration testing on an annual basis or more frequently if required to address an environmental change on any system housing commonwealth data.

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

Control Enhancements for Sensitive Systems [Withdrawn]

CA-9 INTERNAL SYSTEM CONNECTIONS

[Withdrawn: Not applicable to COV]

1.5.*FAMILY:* *CONFIGURATION MANAGEMENT* ***CLASS:*** *OPERATIONAL*

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to all individuals providing system support and all system owners:

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

   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

   1. Configuration management policy on an annual basis or more frequently if required to address an environmental change and

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

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

Control Enhancements for Sensitive Systems: None.

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those

components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

Control Enhancements for Sensitive Systems:

(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

The organization reviews and updates the baseline configuration of the information system:

(a) on an annual basis ;

(b) When required due to an environmental change and

(c) As an integral part of information system component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

(2) [Withdrawn: Not applicable to COV]
(3) [Withdrawn: Not applicable to COV]
(4) [Withdrawn: Incorporated into CM-7].
(5) [Withdrawn: Incorporated into CM-7].

(6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS

The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/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, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the 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. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4, SC-3, SC-7.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

The organization:

(a) Issues 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) Applies a default system sanitation process to the devices when the individuals return.

Supplemental Guidance: When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be

located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

CM-2-COV

Control:

1. The organization:

   a. Identifies, documents, and applies more restrictive security configurations for sensitive agency IT systems, as necessary.

   b. Maintains records that document the application of baseline security configurations.

   c. Monitors systems for security baselines and policy compliance.

   d. Reviews and revises all security configuration standards annually, or more frequently, as needed.

   e. Reapplies all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.

   f. Modifies individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

2. Requires creation and periodic review of a list of agency hardware and software assets.

3. The organization reviews and updates the baseline configuration of all information system:

   (a) Once a year at a minimum;

   (b) When required due to a significant configuration change or a demonstrated vulnerability; and

(c) As an integral part of information system component installations and upgrades.

4. Requires additional configuration changes to devices to be used for international travel:

(a) Install all operating system security updates.
(b) Install all anti-virus, firewall, and anti-spyware security application software updates.
(c) Encrypt the computer hard disk or at least all sensitive information on the device.
(d) Update the web browser software and implement strict security settings.
(e) Update all application software to be used during the trip.
(f) Disable infrared ports, Bluetooth ports, web cameras, and any hardware features not needed for the trip.
(g) Configure the device to use a VPN connection to create a more secure connection.
(h) Configure the device to disable sharing of all file and print services.
(i) Configure the device to disable ad-hoc wireless connections.
(j)Ensure that all required cables and power adapters are packed with the computing asset.

Supplemental Guidance: http://www.fbi.gov/about-us/investigate/counterintelligence/business-travel-brochure

Control Enhancements for Sensitive Systems: None

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:

a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

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

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

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

Supplemental Guidance: Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

(3) [Withdrawn: Not applicable to COV]

(4) CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE

The organization requires an information security representative to be a member of the organization-defined configuration change control element

Supplemental Guidance: Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.

(5) [Withdrawn: Not applicable to COV]

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

The organization ensures that cryptographic mechanisms used to provide system security safeguards are under configuration management.

Supplemental Guidance: Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13.

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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Control Enhancements for Sensitive Systems:

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

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.

Control Enhancements for Sensitive Systems:

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING

The information system enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

(2) [Withdrawn: Not applicable to COV]
(3) [Withdrawn: Not applicable to COV]
(4) [Withdrawn: Not applicable to COV]

(5) ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES

The organization:

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

(b) Reviews and reevaluates privileges on a quarterly basis or more frequently if required to address an environmental change.

Supplemental Guidance: In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers. Related control: AC-2.

(6) [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: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using system using the

Commonwealth of Virginia System Hardening Standards that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for information system components based on operational requirements; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, commonwealth or federal agencies, and other organizations in the public and private sectors. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

Control Enhancements for Sensitive Systems:

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

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.

Supplemental Guidance: Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.

Control Enhancements for Sensitive Systems:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

The organization:

(a) Reviews the information system on a monthly basis or more frequently if required to address an environmental change to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

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

Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.

(2) [Withdrawn: Not applicable to COV]
(3) [Withdrawn: Not applicable to COV]
(4) [Withdrawn: Not applicable to COV]
(5) [Withdrawn: Not applicable to COV]

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes organization-defined information deemed necessary to achieve effective information system component accountability; and

b. Reviews and updates the information system component inventory on a monthly basis or more frequently if required to address an environmental change.

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.

Control Enhancements for Sensitive Systems:

(1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

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

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

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

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

(6) INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS

The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Supplemental Guidance: This control enhancement focuses on configuration settings established by organizations for information 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: CM-2, CM-6.

(7) [Withdrawn: Not applicable to COV]
(8) [Withdrawn: Not applicable to COV]
(9) [Withdrawn: Not applicable to COV]

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops, documents, and implements a configuration management plan for the information 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 information system and places the configuration items under configuration management; and

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

Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information 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, SA-10.

Control Enhancements for Sensitive Systems:

(1) CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.

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

CM-10 SOFTWARE USAGE RESTRICTIONS

Control: The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents 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.

Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.

Control Enhancements for Sensitive Systems:
(1) SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE
The organization establishes 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.

Supplemental Guidance: 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. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

CM-11 USER-INSTALLED SOFTWARE

Control: The organization:

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

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

c. Monitors policy compliance at organization-defined frequency.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Control Enhancements for Sensitive Systems:

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

The information system alerts the appropriate organization-defined personnel or roles when the unauthorized installation of software is detected.

Supplemental Guidance: Related controls: CA-7, SI-4.

(2) USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS

The information system prohibits user installation of software without explicit privileged status.

Supplemental Guidance: Privileged status can be obtained, for example, by serving in the role of system administrator. Related control: AC-6.

1.6.*FAMILY:* *CONTINGENCY PLANNING* *CLASS:* *OPERATIONAL*

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization:

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

1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:

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

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

Control Enhancements for Sensitive Systems: None.

CP-1-COV-1

Control: Each agency shall:

1. 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.

2. Based on BIA and RA results, develop IT disaster components of the agency CONTINUITY PLAN which identifies:

   a. 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

   b. 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.

3. Require an annual exercise (or more often as necessary) of IT DR components to assess their adequacy and effectiveness.

4. Require review and revision of IT DR components following the exercise (and at other times as necessary).

Supplemental Guidance: None.

Controls Enhancement for Sensitive Systems: None

CP-1-COV-2

Control: Each agency shall:

1. Based on the CONTINUITY PLAN, develop and maintain an IT DRP, which supports the restoration of mission essential functions and dependent business functions.

2. Require approval of the IT DRP by the Agency Head.

3. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in mission essential functions, services, IT system hardware and software, and personnel.

4. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.

Supplemental Guidance: None.

Controls Enhancement for Sensitive Systems: None

CP-2 CONTINGENCY PLAN

Control: The organization:

a. Develops a contingency plan for the information system that:

1. Identifies essential missions 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 missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by appropriate organization-defined personnel or roles;

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

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system on an annual basis or more frequently if required to address an environmental change;

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

Control Enhancements for Sensitive Systems:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: 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

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

(3) CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of essential missions and business functions within the organization-defined time period of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(4) CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of all missions and business functions within the organization-defined time period of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(5) [Withdrawn: Not applicable to COV]

(6) [Withdrawn: Not applicable to COV]

(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

The organization identifies critical information system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.

CP-3 CONTINGENCY TRAINING

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

a. Within 10-days of assuming a contingency role or responsibility;

b. When required by information system changes; and

c. Annually thereafter.

Supplemental Guidance: 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, regular users 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 set up information systems at alternate processing and storage sites; and managers/senior leaders 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/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2.

Control Enhancements for Sensitive Systems:

(1) CONTINGENCY TRAINING | SIMULATED EVENTS

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

(2) Withdrawn: Not applicable to COV

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:

a. Tests the contingency plan for the information system on an annual basis or more frequently if required to address an environmental change using approved tests to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Reviews the contingency plan test results; and

c. Initiates corrective actions, if needed.

Supplemental Guidance: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.

Control Enhancements for Sensitive Systems:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: 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, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.

(2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE

The organization tests 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.

Supplemental Guidance: Related control: CP-7.

(3) Withdrawn: Not applicable to COV

(4) CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Supplemental Guidance: Related controls: CP-10, SC-24.

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

Control Enhancements for Sensitive Systems:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/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 one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

Control Enhancements for Sensitive Systems:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/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 one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Supplemental Guidance: 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 at the alternate processing site.

(4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6.

(5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS

[Withdrawn: Incorporated into CP-7].

(6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

The organization plans and prepares for circumstances that preclude returning to the primary processing site.

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. 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.

Control Enhancements for Sensitive Systems:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, 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 meeting the separation needs addressed in the risk assessment.

(4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN

The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Withdrawn: Not applicable to COV

(5) [Withdrawn: Not applicable to COV]

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system within the organization-defined frequency consistent with recovery time and recovery point objectives;

b. Conducts backups of system-level information contained in the information system in accordance with organization-defined frequency consistent with recovery time and recovery point objectives;

c. Conducts backups of information system documentation including security-related documentation in accordance with organization-defined frequency consistent with recovery time and recovery point objectives; and

d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.

Control Enhancements for Sensitive Systems:

(1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY

The organization tests backup information at least every 30-days to verify media reliability and information integrity.

Supplemental Guidance: Related control: CP-4.

(2) INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Supplemental Guidance: Related control: CP-4.

(3) INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

The organization stores backup copies of critical information 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.

Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.

(4) INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION

[Withdrawn: Incorporated into CP-9].

(5) [Withdrawn: Not applicable to COV]
(6) [Withdrawn: Not applicable to COV]
(7) [Withdrawn: Not applicable to COV]

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:

1. Secure off-site storage for backup media.

2. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.

3. Performance of backups only by authorized personnel.

4. Review of backup logs after the completion of each backup job to verify successful completion.

5. Approval of backup schedules of a system by the System Owner.

6. Approval of emergency backup and operations restoration plans by the System Owner.

7. 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.

8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.

9. Retention of the data handled by an IT system in accordance with the agency's records retention policy.

10. 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.

11. 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.

12. 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 of Operations Plan.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any

interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

Control Enhancements for Sensitive Systems:

(1) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING

[Withdrawn: Incorporated into CP-4].

(2) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

The information system implements transaction recovery for systems that are transaction-based.

Supplemental Guidance: Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

(3) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS

[Withdrawn: Addressed through tailoring procedures].

(4) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD

The organization provides the capability to restore information system components within the organization-defined restoration time-periods from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance: Restoration of information system components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2.

(5) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY

[Withdrawn: Incorporated into SI-13].

(6) [Withdrawn: Not applicable to COV]

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

[Withdrawn: Not applicable to COV]

CP-12 SAFE MODE

[Withdrawn: Not applicable to COV]

CP-13 ALTERNATIVE SECURITY MECHANISMS

[Withdrawn: Not applicable to COV]

1.7. *FAMILY: IDENTIFICATION AND AUTHENTICATION* *CLASS: TECHNICAL*

IA-1

Control: The organization:

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

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

   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

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

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or

network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks.

Control Enhancements for Sensitive Systems:

(1) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

Supplemental Guidance: Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.

(6) [Withdrawn: Not applicable to COV]

(7) [Withdrawn: Not applicable to COV]

(8) [Withdrawn: Not applicable to COV]

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) [Withdrawn: Not applicable to COV]

(12) [Withdrawn: Not applicable to COV]

(13) [Withdrawn: Not applicable to COV]

IA-2-COV

Control:

a. The organization ensures that network connections for accessing development environments or performing administrative functions on servers or multi-user systems employ two-factor authentication and are audited. Two-Factor authentication is required for all network-based administrative access to servers and multi-use systems.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: The organization ensures that remote (Internet, dial-up) network connections for accessing sensitive systems employ two-factor authentication and are audited.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV]

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers by:

a. Receiving authorization from a designated organizational official to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device;

d. Preventing reuse of identifiers for at least 24 changes of the identifier and at least 24 days from the initial use of the identifier; and

e. Disabling the identifier after 90-days of inactivity.

Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

(6) [Withdrawn: Not applicable to COV]

(7) [Withdrawn: Not applicable to COV]

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined 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/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing user-account authenticators at least every 60-days;

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

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

h. Protecting authenticator content from unauthorized disclosure and modification;

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

j. Withdrawn: Not applicable to COV

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

Control Enhancements ~~for Sensitive Systems~~:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

(a) Enforces minimum password complexity of

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

(b) [Withdrawn: Not applicable to COV]

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

(d) Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum *or dual factor authentication*;

(e) Prohibits password reuse for 24 generations; and

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

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group

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

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY

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

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

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

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

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

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

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

Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

(8) [Withdrawn: Not applicable to COV]

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) [Withdrawn: Not applicable to COV]

(12) [Withdrawn: Not applicable to COV]

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

IA-5-COV-1

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

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

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

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

d. documenting and storing hardware passwords securely.

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

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

g. requiring that any authentication trust relation be structured such that the commonwealth's authentication mechanism is the only trusted source of information.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IA-5-COV-2

Control: An organization sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may:

- determine the appropriate validity period of the password, commensurate with sensitivity and risk.
- determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk.
- allow the citizen to continue to use the initial password so long as the Agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.

The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IA-6 AUTHENTICATOR FEEDBACK

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

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

Control Enhancements for Sensitive Systems: None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

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

Supplemental Guidance: [Withdrawn: Not applicable to COV]

Control Enhancements for Sensitive Systems: None.

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

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

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

Supplemental Guidance: [Withdrawn: Not applicable to COV]

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV]

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

[Withdrawn: Not applicable to COV]

IA-11 RE-AUTHENTICATION

[Withdrawn: Not applicable to COV]

1.8.*FAMILY:* *INCIDENT RESPONSE* ***CLASS:*** *OPERATIONAL*

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Reviews and updates the current:
   1. Incident response policy on an annual basis or more frequently if required to address an environmental change; and
   2. Incident response procedures on an annual basis or more frequently if required to address an environmental change.

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

Control Enhancements for Sensitive Systems: None.

IR-1-COV

Control: The organization:

1. Shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following:

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

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

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

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

2. Shall or shall require that its service provider, document and implement information security monitoring and logging practices that include the following components, at a minimum:

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

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

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

    d. Prohibit the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head.

3. Shall document information security incident handling practices and where appropriate the agency shall incorporate its service provider's procedures for incident handling practices that include the following at a minimum:

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

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

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

    d. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-2 INCIDENT RESPONSE TRAINING

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

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

b. When required by information system changes; and

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

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

Control Enhancements for Sensitive Systems:

(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

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

(2) [Withdrawn: Not applicable to COV]

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

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

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

IR-4 INCIDENT HANDLING

Control: The organization:

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

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

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

d. Must document incidents and investigations in the commonwealth's incident handling system.

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

Control Enhancements for Sensitive Systems:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) INCIDENT HANDLING | INFORMATION CORRELATION

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

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

(5) [Withdrawn: Not applicable to COV]

(6) INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES

The organization implements incident handling capability for insider threats.

Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

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

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

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

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

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

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

(9) Withdrawn: Not applicable to COV

(10) Withdrawn: Not applicable to COV

IR-4-COV-1

Control:

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

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-4-COV-2

Control:

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

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

Each agency shall:

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

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

      1) Social security number;

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

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

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

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

      2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the

individual, or any information in an individual's application and claims history, including any appeals records.

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

   a. Five digits of a social security number; or

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

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

   a. An individual's medical history; or

   b. Mental or physical condition; or

   c. Medical treatment or diagnosis; or

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

   e. Other unique identifier.

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

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

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

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

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

   b. Theft or loss of physical hardcopy; and

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

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

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

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

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

10. Provide notification that consists of:

    a. A general description of what occurred and when;

    b. The type of Personal Information that was involved;

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

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

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

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

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

    b. Telephone Notice;

    c. Electronic notice; or

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

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

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

3) Notice to major statewide media.

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-5 INCIDENT MONITORING

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

IR-5-COV

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-6 INCIDENT REPORTING

Control: The organization:

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

b. Reports security incident information to designated authorities.

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

Control Enhancements for Sensitive Systems:

(1) INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance: Related control: IR-7.

(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS

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

(3) [Withdrawn: Not applicable to COV]

IR-6-COV

Control: Organization shall:

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

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

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

IR-7 INCIDENT RESPONSE ASSISTANCE

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

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

Control Enhancements for Sensitive Systems:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response related information and support. Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

(2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS

The organization:

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

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

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

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

a. Develops an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by designated officials within the organization.

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

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

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

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

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

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

Control Enhancements for Sensitive Systems: None.

IR-9 INFORMATION SPILLAGE RESPONSE

Control: The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting organization-defined personnel of the information spill using a method of communication not associated with the spill;

c. Isolating the contaminated information system or system component;

d. Eradicating the information from the contaminated information system or component;

e. Identifying other information systems or system components that may have been subsequently contaminated;

f. Performing other organization-defined actions. Supplemental Guidance: Information spillage refers to instances where either classified or sensitive

information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Control Enhancements:

(1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL The organization assigns organization-defined personnel or roles with responsibility for responding to information spills.

(2) INFORMATION SPILLAGE RESPONSE | TRAINING The organization provides information spillage response training on an annual basis or more frequently if required to address an environmental change.

(3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS The organization implements organization-defined procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Supplemental Guidance: Correction actions for information systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.

(4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL The organization employs organization-defined security safeguards for personnel exposed to information not within assigned access authorizations.

Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the commonwealth laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

[Withdrawn: Not applicable to COV]

1.9. *FAMILY:* *MAINTENANCE* *CLASS:* *OPERATIONAL*

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

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

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

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

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

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

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

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

Control Enhancements for Sensitive Systems:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2].

(2) [Withdrawn: Not applicable to COV]

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

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors information system maintenance tools.

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS
The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related control: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA
The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system. Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related control: SI-3.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL
The organization prevents the unauthorized 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 organization-defined personnel explicitly authorizing removal of the equipment from the facility. Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

(4) MAINTENANCE TOOLS | RESTRICTED TOOL USE
The information system restricts the use of maintenance tools to authorized personnel only. Supplemental Guidance: This control enhancement applies to information systems that are used to carry out maintenance functions.

Related controls: AC-2, AC-3, AC-5, AC-6. References: NIST Special Publication 800-88.

MA-4 NON-LOCAL MAINTENANCE

Control: The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;

b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, 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. 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, MP-6, PL-2, SC-7, SC-10, SC-17.

Control Enhancements:

(1) NONLOCAL MAINTENANCE | AUDITING AND REVIEW

The organization:

(a) Audits nonlocal maintenance and diagnostic sessions for organization-defined audit events; and

(b) Reviews the records of the maintenance and diagnostic sessions.

Supplemental Guidance: Related controls: AU-2, AU-6, AU-12.

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(3) NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION

The organization:

(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the

component (with regard to potentially malicious software) before reconnecting the component to the information system.

Supplemental Guidance: Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7.

(4) NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS

The organization protects 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 information system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths based upon encryption.

Supplemental Guidance: Related control: SC-13.

(5) NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS

The organization:

(a) Requires the approval of each nonlocal maintenance session by organization-defined personnel; and

(b) Notifies organization-defined personnel of the date and time of planned nonlocal maintenance.

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and information system knowledge to determine the appropriateness of the proposed maintenance.

(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

Supplemental Guidance: Related controls: SC-8, SC-13.

(7) NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION

The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

Supplemental Guidance: Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use. Related control: SC-13.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

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

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

Supplemental Guidance: [Withdrawn: Not applicable to COV]

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.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

MA-6 TIMELY MAINTENANCE

Control: The organization obtains 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.

Supplemental Guidance: Organizations specify the information 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 typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.

Control Enhancements:

(1) *TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*

The organization performs preventive maintenance on organization-defined information system components at the appropriate organization-defined time intervals to ensure that the business need is met.

Supplemental Guidance: Preventive maintenance includes proactive care and servicing of organizational information systems components for the purpose of maintaining 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/mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they actually fail. Methods of determining what preventive (or other) failure management policies to apply include, for example, original equipment manufacturer (OEM) recommendations, statistical failure records, requirements of codes, legislation, or regulations within a jurisdiction, expert opinion, maintenance that has already been conducted on similar equipment, or measured values and performance indications.

(2) *TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*

The organization performs predictive maintenance on information system components on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: Predictive maintenance, or condition-based maintenance, attempts to evaluate 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 point in 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 goal of predicting the future trend of the equipment's condition. This approach uses 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, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

(3) *TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*

The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

Supplemental Guidance: A computerized maintenance management system maintains a computer database of information about the maintenance operations of organizations and automates processing equipment condition data in order to trigger maintenance planning, execution, and reporting.

References: None.

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

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

MP-1-COV

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

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

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

   a. The business or technical justification;

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

c. A description of all associated risks;

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

e. Identification of any residual risks.

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

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

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

MP-2 MEDIA ACCESS

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

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Control Enhancements for Sensitive Systems:

(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

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

(2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION

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

MP-3 MEDIA MARKING

Control: The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts organization-defined types of information system media from marking as long as the media remain within organization-defined controlled areas.

Supplemental Guidance: The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3.

Control Enhancements: None.

References: FIPS Publication 199.

MP-4 MEDIA STORAGE

Control: The organization:

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

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

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information

systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

Control Enhancements for Sensitive Systems:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

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

(2) [Withdrawn: Not applicable to COV]

MP-4-COV

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

MP-5 MEDIA TRANSPORT

Control: The organization:

a. Protects and controls digital and non-digital media during transport outside of controlled areas using FIPS 140-2 validated encryption module for all digital media and a secured locked container for non-digital media;

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

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

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

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

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Control Enhancements for Sensitive Systems:

(1) MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS

[Withdrawn: Incorporated into MP-5].

(2) MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES

[Withdrawn: Incorporated into MP-5].

(3) MEDIA TRANSPORT | CUSTODIANS

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

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

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

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

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

MP-6 MEDIA SANITIZATION

Control: The organization:

a. Sanitizes information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined

sanitization techniques and procedures in accordance with applicable organizational standards and policies; and

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

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. Related controls: MA-2, MA-4, RA-3, SC-4.

Control Enhancements for Sensitive Systems:

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

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

Supplemental Guidance:

[Withdrawn: Not applicable to COV]

(2) MEDIA SANITIZATION | EQUIPMENT TESTING

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

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

(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES

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

Supplemental Guidance: Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices

are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

(4) MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION
[Withdrawn: Incorporated into MP-6].

(5) MEDIA SANITIZATION | CLASSIFIED INFORMATION
[Withdrawn: Incorporated into MP-6].

(6) MEDIA SANITIZATION | MEDIA DESTRUCTION
[Withdrawn: Incorporated into MP-6].

(7) [Withdrawn: Not applicable to COV]
(8) [Withdrawn: Not applicable to COV]

MP-6-COV

Control: Remove data from IT assets prior to disposal in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

MP-7 MEDIA USE

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

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations

may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4.

Control Enhancements for Sensitive Systems:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

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

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

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

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

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

MP-8 MEDIA DOWNGRADING

[Withdrawn: Not applicable to COV]

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

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

PE-1-COV

Control:

1. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.

2. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.

3. *All data centers must meet the requirements of a Tier III data center as defined by the Uptime Institute.*

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

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

b. Issues authorization credentials for facility access;

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

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

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

Control Enhancements for Sensitive Systems:

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

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

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

(2) [Withdrawn: Not applicable to COV]

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

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

PE-2-COV

Control: The organization:

a. Temporarily disables physical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.

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

Control Enhancements for Sensitive Systems: None

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations for all physical access points including organization-defined entry/exit points to the facility where the information system resides by;

   1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress/egress to the facility using organization-defined physical access control systems/devices; guards;

b. Maintains physical access audit logs for all organization-defined entry/exit points;

c. Provides organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity for organization-defined circumstances requiring visitor escorts and monitoring;

e. Secures keys, combinations, and other physical access devices;

f. Inventories organization-defined physical access devices every on an annual basis or more frequently if required to address an environmental change; and

g. Withdrawn: Not applicable to COV

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Control Enhancements for Sensitive Systems:

(1) PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS

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

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

(2) PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES

The organization performs security checks every 30-days or more frequently if required to address an environmental change at the physical boundary of the facility

or information system for unauthorized exfiltration of information or removal of information system components.

Supplemental Guidance: 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) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

(6) [Withdrawn: Not applicable to COV]

PE-3-COV

Control: Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to organization-defined information system distribution and transmission lines within organizational facilities using the appropriate organization-defined security safeguards.

Supplemental Guidance: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Control Enhancements for Sensitive Systems: References: NSTISSI No. 7003.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

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

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

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

b. Reviews physical access logs at least once every 30-days and upon occurrence of organization-defined events or potential indications of events; and

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

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

Control Enhancements for Sensitive Systems:

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

The organization monitors physical intrusion alarms and surveillance equipment.

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

PE-7 VISITOR CONTROL

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

PE-8 ACCESS RECORDS

Control: The organization:

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

b. Reviews visitor access records at least once every 30-days.

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

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

PE-9 POWER EQUIPMENT AND POWER CABLING

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

PE-10 EMERGENCY SHUTOFF

Control: The organization:

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

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

c. Protects emergency power shutoff capability from unauthorized activation.

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

Control Enhancements for Sensitive Systems:

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

PE-11 EMERGENCY POWER

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

References: None.

PE-13 FIRE PROTECTION

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

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

Control Enhancements for Sensitive Systems:

(1) FIRE PROTECTION | DETECTION DEVICES / SYSTEMS

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

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain

access to facilities where sensitive operations are taking place or where there are information systems containing sensitive information.

(2) FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS

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

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

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

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

(4) [Withdrawn: Not applicable to COV]

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

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

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

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

Control Enhancements for Sensitive Systems:

(1) TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS

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

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

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

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

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

Control Enhancements:

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts the appropriate organization-defined personnel.

Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

References: None.

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls organization-defined types of information system components entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None.

References: None.

PE-17 ALTERNATE WORK SITE

Control: The organization:

a. Employs organization-defined security controls at alternate work sites;

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. Related controls: AC-17, CP-7.

Control Enhancements: None.

References: NIST Special Publication 800-46.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

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

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

Control Enhancements for Sensitive Systems:

(1) LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE

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

Supplemental Guidance: Related control: PM-8.

PE-18-COV

Control: The organization shall develop and publish a policy that requires all information system components such that:

1. All information system components and services remain within the continental United States ~~*unless the COV CISO has granted an exception*~~.
2. All data and system information associated with the information system components and services remain within the continental Unites States.
3. All physical components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must be housed within ~~the same~~ *approved storage locations* ~~dedicated for the exclusive use of the organization~~ and ~~are~~ clearly marked.
4. All virtual components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must reside in hypervisors ~~dedicated to the exclusive use of the organization~~ *that are hardened to meet or exceed commonwealth security requirements for the guest VMs or data being processed or stored within the hypervisors control*.
5. Each hypervisor can only host one tier of the application architecture and no hypervisor may host the application interface and the data storage component for any information system, even if the components in question do not interact within the same information system.

PE-19 INFORMATION LEAKAGE

[Withdrawn: Not applicable to COV]

PE-20 ASSET MONITORING AND TRACKING

[Withdrawn: Not applicable to COV]

1.12. *FAMILY: PLANNING* *CLASS: MANAGEMENT*

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:

   1. Is consistent with the organization's enterprise architecture;

   2. Explicitly defines the authorization boundary for the system;

   3. Describes the operational context of the information system in terms of missions and business processes;

   4. Provides the security categorization of the information system including supporting rationale;

   5. Describes the operational environment for the information system and relationships with or connections to other information systems;

6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to the appropriate organization-defined personnel;

c. Reviews the security plan for the information system on an annual basis or more frequently if required to address an environmental change;

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and Control Enhancements for Sensitive Systems. Security plans also describe, at a high level, how the security controls and Control Enhancements for Sensitive Systems meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Control Enhancements for Sensitive Systems:

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

(2) [Withdrawn: Incorporated into PL-7]. SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE

[Withdrawn: Incorporated into PL-8].

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

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

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

PL-2-COV

Control: The organization shall:

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:

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

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

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

3. Plan, document, and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control: The organization:

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

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

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

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

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

Control Enhancements for Sensitive Systems:

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

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

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

PL-4-COV

Control: Organization shall:

1. Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management (DHRM) Policy

1.75 – Use of Internet and Electronic Communication Systems. Each Executive branch agency shall supplement the policy as necessary to address specific agency needs.

2. Prohibit users from:

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

   b. Tampering with security controls configured on COV workstations;

   c. Installing personal software on a Commonwealth system;

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

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

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

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

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

   > The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).
>
> No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

PL-5 PRIVACY IMPACT ASSESSMENT

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

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2].

PL-7 SECURITY CONCEPT OF OPERATIONS

[Withdrawn: Not applicable to COV]

PL-8 INFORMATION SECURITY ARCHITECTURE

Control: The organization:

a. Develops an information security architecture for the information system that:

1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture annual basis or more frequently if required to address an environmental change to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of

information and information system services, and any other specific protection needs.
In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.

Control Enhancements:

(1) *INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*

The organization designs its security architecture using a defense-in-depth approach that:

(a) Allocates *organization-defined security safeguards* to *organization-defined locations and architectural layers*; and

(b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

Supplemental Guidance: Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources (i.e., increases adversary work factor) and also increases the likelihood of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences (e.g., lockout, cascading alarms) by interfering with another safeguard. Placement of security safeguards is a key activity. Greater asset criticality or information value merits additional layering. Thus, an organization may choose to place anti-virus software at organizational

boundary layers, email/web servers, notebook computers, and workstations to maximize the number of related safeguards adversaries must penetrate before compromising the information and information systems. Related controls: SC-29, SC-36.

(2) *INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*

The organization requires that organization-defined security safeguards allocated to organization-defined locations and architectural layers are obtained from different suppliers.

Supplemental Guidance: Different 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 according to their priorities and development schedules. By having different products at different locations (e.g., server, boundary, desktop) there is an increased likelihood that at least one will detect the malicious code. Related control: SA-12.

References: None.

PL-9 CENTRAL MANAGEMENT

[Withdrawn: Not applicable to COV]

1.13. *FAMILY: PERSONNEL SECURITY* *CLASS: OPERATIONAL*

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:
   1. Personnel security policy on an annual basis or more frequently if required to address an environmental change; and
   2. Personnel security procedures on an annual basis or more frequently if required to address an environmental change.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and Control Enhancements for Sensitive Systems in the PS family. Policy and procedures reflect applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the

organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements for Sensitive Systems: None.

PS-2 POSITION RISK DESIGNATION

Control: The organization:

a. Assigns a risk designation to all organizational positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and updates position risk designations annual basis or more frequently if required to address an environmental change

Supplemental Guidance: Position risk designations reflect Department of Human Resource Management as well as Commonwealth of Virginia policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). Related controls: AT-3, PL-2, PS-3.

Control Enhancements: None.

References: 5 C.F.R. 731.106.

PS-3 PERSONNEL SCREENING

Control: The organization:

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

b. Rescreens individuals according to organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.

Supplemental Guidance: Personnel screening and rescreening activities reflect applicable commonwealth laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2.

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

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:

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

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

c. [Withdrawn: Not applicable to COV]

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

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

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

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

PS-5 PERSONNEL TRANSFER

Control: The organization:

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

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

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

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

Supplemental Guidance: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include,

for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4.

Control Enhancements for Sensitive Systems: None.

PS-6 ACCESS AGREEMENTS

Control: The organization:

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

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

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

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

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

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

Control Enhancements for Sensitive Systems:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL *PROTECTION*

[Withdrawn: Incorporated into PS-3].

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:

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

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

c. Documents personnel security requirements;

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

e. Monitors provider compliance.

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

Control Enhancements for Sensitive Systems: None.

PS-8 PERSONNEL SANCTIONS

Control: The organization:

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

b. [Withdrawn: Not applicable to COV]

Control Enhancements for Sensitive Systems: None.

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

1.14. *FAMILY: RISK ASSESSMENT* *CLASS: MANAGEMENT*

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

RA-2 SECURITY CATEGORIZATION

Control: The organization:

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

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

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

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

Control Enhancements for Sensitive Systems: None.

RA-3 RISK ASSESSMENT

Control: The organization:

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

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

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

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

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

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

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.
Control Enhancements for Sensitive Systems: None.

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3]

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications at least once every 30-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;

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

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

   2. Formatting checklists and test procedures; and

   3. Measuring vulnerability impact;

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

d. Remediates legitimate vulnerabilities within 30-days in accordance with an organizational assessment of risk; and

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

Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

Control Enhancements for Sensitive Systems:

(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY

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

Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in

the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.

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

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

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

(3) VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE

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

(4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION

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

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

(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

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

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

(6) VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Supplemental Guidance: Related controls: IR-4, IR-5, SI-4.

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

[Withdrawn: Incorporated into CM-8].

(8) VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS

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

Supplemental Guidance: Related control: AU-6.

(9) VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES

[Withdrawn: Incorporated into CA-8].

(10) VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION

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

RA-5-COV

[Withdrawn: Incorporated into CA-8]

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

[Withdrawn: Not applicable to COV]

1.15. *FAMILY:* *SYSTEM AND SERVICES ACQUISITION* *CLASS:* *MANAGEMENT*

SYSTEM AND SERVICES ACQUISITION CONTROLS

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

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

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

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

Control Enhancements for Sensitive Systems: None.

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

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

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

c. Withdrawn: Not applicable to COV

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

Control Enhancements for Sensitive Systems: None.

SA-3 LIFE CYCLE SUPPORT

Control: The organization:

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

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

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

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

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

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

Control Enhancements for Sensitive Systems: None.

SA-3-COV-1

Control: Each Agency shall:

1. Project Initiation

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

   b. Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system.

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

   d. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.

2. Project Definition

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

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

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

   d. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.

   e. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

3. Implementation

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

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

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

d. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see IT Systems Security Plans) of this document.

4. Disposition

a. Require retention of the data handled by an IT system in accordance with the agency's records retention policy prior to disposing of the IT system.

b. Require that electronic media is sanitized prior to disposal, as documented (see Data Storage Media Protection), so that all data is removed from the IT system.

c. Verify the disposal of hardware and software in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SA-3-COV-2

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

1. Application Planning

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

b. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.

c. Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.

d. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:

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

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

   iii. Sensitive information shall not be stored in hidden fields that are part of the application interface.

2. Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.

a. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.

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

c. Data storage shall be separated 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).

d. Agencies shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).

e. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.

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

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

h. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.

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

3. Production and Maintenance

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

   b. Internet-facing applications classified as sensitive shall have periodic, not to exceed 90 days, vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SA-4 ACQUISITIONS

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable commonwealth laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

Supplemental Guidance: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security

documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Control Enhancements:

(1) *ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security 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 control: SA-5.

(2) *ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: *security-relevant external system interfaces; high-level design; and design/implementation information* at the appropriate *level of detail*.

Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information 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 multiple subsystems and the interfaces between subsystems providing security-relevant

functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.

(3) *ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*

The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes the organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes. The quality control process must ensure both the integrity and availability of the information to be utilized by the information system.

Supplemental Guidance: Following a well-defined system development life cycle that includes state-of-the-practice software development methods, systems/security engineering methods, quality control processes, and testing, evaluation, and validation techniques helps to reduce the number and severity of latent errors within information systems, system components, and information system services. Reducing the number/severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Related control: SA-12.

(4) *ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

[Withdrawn: Incorporated into CM-8 (9)].

(5) *ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*

The organization requires the developer of the information system, system component, or information 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.

Supplemental Guidance: Security configurations include the Commonwealth of Virginia system hardening standards as well as the Center for Internet Security (CIS) system hardening standards. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8.

(6) *ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*

[Withdrawn].

(7) *ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*

[Withdrawn: Incorporated into SA-4-COV-1].

(8) *ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains the appropriate organization-defined level of detail.

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information 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 the continuous monitoring strategies and programs implemented by organizations. Related control: CA-7.

(9) *ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to 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 when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying 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*

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Supplemental Guidance: Related controls: IA-2, IA-8.

References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Web: http://www.niap-ccevs.org, http://fips201ep.cio.gov.

SA-4-COV-1

The organization:

(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.

Supplemental Guidance: Related controls: SC-12, SC-13.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

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

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to the appropriate organization-defined personnel.

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements for Sensitive Systems:

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

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

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

(4) INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN
[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.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SA-7 USER-INSTALLED SOFTWARE

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

SA-8 SECURITY ENGINEERING PRINCIPLES

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

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

Control Enhancements for Sensitive Systems: None.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

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

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

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

Supplemental Guidance: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures,

business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Enhancements for Sensitive Systems:

(1) *EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by the appropriate organization-defined personnel.

Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3.

(2) *EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*

The organization requires providers of organization-defined external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.

(3) *EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*

The organization establishes, documents, and maintains trust relationships with external service providers based on organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships.

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. Such relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and the types of interactions between the parties. In some cases, the degree of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls. The level of control is typically established by the terms and conditions of the contracts or service-level agreements and can range from extensive control (e.g., negotiating contracts or agreements that specify security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services). In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.

(4) *EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*

The organization employs organization-defined security safeguards to ensure that the interests of the organization-defined external service providers are consistent with and reflect organizational interests.

Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive

experiences), and conducting periodic/unscheduled visits to service provider facilities.

(5) *EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*

The organization restricts the location of information processing; information/data; information system services to locations within the continental Unites States of America..

Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.

References: NIST Special Publication 800-35.

SA-9-COV-1

- Control: Each Agency shall:
  1) Establish the exact geographically location of all data if not stored within the Commonwealth. The Commonwealth will define the parameters and costs for data location options prior to making any contractual commitments.
  2) Confirm the exact geographically location of the sensitive data on a monthly basis and report the location to the appropriate regulatory authority every 90 days.

Supplemental Guidance: None

SA-9-COV-2

- Control: Each Agency shall
  1) Establish a Data Escrow policy to address the data recovery process in case of system failure or facility issues and ensure all copies of data are returned to the Commonwealth at the end of contract.
  2) Establish a validated copy of any data elements classified as sensitive with respect to integrity or availability or are considered components in a system of record for the Commonwealth. The validated copy must be stored within a secured environment maintained by the Commonwealth

Supplemental Guidance: None

SA-9-COV-3

- Control: Each Agency shall

  (1) Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis
  (2) Perform a monthly review of activity logs related to the operation of the service. At a minimum, the activity review must include the access time and action of each individual using the system during the review period.
  (3) Receive reports from the vendor on vulnerability scans of the operating system and supporting software at least once every 90-days
  (4) Ensure that the vendor conduct an independent vulnerability scan of the service at least once every 90-days and provide the results to Agency within 10-business days
  (5) Submit a summary of all findings from the monthly activity log review once every 90-days to the appropriate regulatory authority
  (6) Submit the vulnerability scan information within 30-days of receipt from the vendor to the appropriate regulatory authority
  (7) Submit the results from the Data Owning Agency vulnerability scan of the service within 30 days of scan completion

  Supplemental Guidance: None

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

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

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

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

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

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

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

Supplemental Guidance: This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the

system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.

Control Enhancements for Sensitive Systems:

(1) *DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. 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 control: SI-7.

(2) *DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*

The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Supplemental Guidance: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf (COTS) information technology products. Alternate configuration management processes include organizational personnel that: (i) are responsible for reviewing/approving proposed changes to information systems, system components, and information system services; and (ii) conduct security impact analyses prior to the implementation of any changes to systems, components, or services (e.g., a configuration control board that considers

security impacts of changes during development and includes representatives of both the organization and the developer, when applicable).

(3) *DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components. Related control: SI-7.

(4) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*

The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components between versions during development. In contrast, SA-10 (1) and SA-10 (3) allow organizations to detect unauthorized changes to hardware, software, and firmware components through the use of tools, techniques, and/or mechanisms provided by developers.

(5) *DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*

The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational information systems supporting critical missions and/or business functions.

(6) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*

The organization requires the developer of the information system, system component, or information 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.

Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that such updates are faithful representations of the master copies maintained by the developer and have not been tampered with during distribution.

References: NIST Special Publication 800-128.

SA-11 DEVELOPER SECURITY TESTING

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

a. Create and implement a security assessment plan;

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

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

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

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

the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Control Enhancements for Sensitive Systems:

(1) DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

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

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

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.

(3) [Withdrawn: Not applicable to COV]

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

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

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application's requirements or context which are generally unavailable to

more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.

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

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

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

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

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

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

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

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

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

(8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Dynamic code analysis provides run-time 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 run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (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 (checking for words that are out of place in software code such as non-English language words or derogatory terms).

References: ISO/IEC 15408; NIST Special Publication 800-53A;

SA-12 SUPPLY CHAIN PROTECTION

[Withdrawn: Not applicable to COV]

SA-13 TRUSTWORTHINESS

[Withdrawn: Not applicable to COV]

SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS

[Withdrawn: Not applicable to COV]

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
    1. Explicitly addresses security requirements;
    2. Identifies the standards and tools used in the development process;
    3. Documents the specific tool options and tool configurations used in the development process; and
    4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
b. Reviews the development process, standards, tools, and tool options/configurations on an annual basis or more frequently if required to address an environmental change to determine if the process, standards, tools,

and tool options/configurations selected and employed can satisfy organization-defined security requirements.

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SA-16 DEVELOPER-PROVIDED TRAINING

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

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

Control Enhancements for Sensitive Systems: None.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

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

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

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

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

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

[Withdrawn: Not applicable to COV]

SA-18 TAMPER RESISTANCE AND DETECTION

[Withdrawn: Not applicable to COV]

SA-19 COMPONENT AUTHENTICITY

[Withdrawn: Not applicable to COV]

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

[Withdrawn: Not applicable to COV]

SA-21 DEVELOPER SCREENING

[Withdrawn: Not applicable to COV]

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control: The organization:

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

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

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

Control Enhancements for Sensitive Systems:

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

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

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

1.16. *FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION* *CLASS: TECHNICAL*

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:

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

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

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

b. Reviews and updates the current:

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

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

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

Control Enhancements for Sensitive Systems: None.

SC-2 APPLICATION PARTITIONING

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

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating

systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

SC-3 SECURITY FUNCTION ISOLATION

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

SC-4 INFORMATION IN SHARED RESOURCES

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

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information

protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.

Control Enhancements for Sensitive Systems:

(1) INFORMATION IN SHARED RESOURCES | SECURITY LEVELS

[Withdrawn: Incorporated into SC-4].

(2) [Withdrawn: Not applicable to COV]

SC-5 DENIAL OF SERVICE PROTECTION

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

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

Control Enhancements for Sensitive Systems:

(1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS

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

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

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

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

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

(3) DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING

The organization:

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

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

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

SC-6 RESOURCE PRIORITY

Control: The information system protects the availability of resources by allocating organization-defined resources by priority.

Supplemental Guidance: Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtainieng more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.

Control Enhancements: None.

References: None.

SC-7 BOUNDARY PROTECTION

Control: The information system:

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

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

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

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces

and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Control Enhancements for Sensitive Systems:

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

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

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

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

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

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

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

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

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

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

Supplemental Guidance: Related control: SC-8.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION
The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

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

(6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES

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

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

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

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

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces. Each managed interface must provide a traffic inspection point for authorized investigations.

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

The information system only allows incoming communications from

organization-defined authorized sources routed to organization-defined authorized destinations.

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

(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

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

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

(13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS

The organization isolates 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.

Supplemental Guidance: Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations. Related controls: SA-8, SC-2, SC-3.

(14) [Withdrawn: Not applicable to COV]

(15) [Withdrawn: Not applicable to COV]

(16) [Withdrawn: Not applicable to COV]

(17) [Withdrawn: Not applicable to COV]

(18) BOUNDARY PROTECTION | FAIL SECURE

The information system fails securely in the event of an operational failure of a boundary protection device.

Supplemental Guidance: Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. 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, SC-24. [Withdrawn: Not applicable to COV]

(19) [Withdrawn: Not applicable to COV]

(20) [Withdrawn: Not applicable to COV]

(21) [Withdrawn: Not applicable to COV]

(22) [Withdrawn: Not applicable to COV]

(23) [Withdrawn: Not applicable to COV]

SC-8 TRANSMISSION INTEGRITY

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

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Enhancements for Sensitive Systems:

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

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

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

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

SC-8-COV

Control: Require the use of data protection mechanisms for the transmission of all email and attached data that is sensitive.

1) Require the use of encryption or digital signatures for the transmission of email and attached data that is sensitive relative to integrity.
2) Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after 15-minutes of inactivity.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.

Control Enhancements: None.

References: None.

SC-11 TRUSTED PATH

[Withdrawn: Not applicable to COV]

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

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

Supplemental Guidance: Cryptographic key management and establishment can be

performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable Commonwealth laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Control Enhancements for Sensitive Systems:

(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

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

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

(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS 140-2-compliant key management technology and processes.

(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES

[Withdrawn: Incorporated into SC-12].

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

[Withdrawn: Incorporated into SC-12].

SC-12-COV

Control: The organization shall:

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.

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

3. Ensures that the cryptographic keying material remain under the exclusive control of the commonwealth.

SC-13 USE OF CRYPTOGRAPHY

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

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements for Sensitive Systems: None.

(1) CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY

[Withdrawn: Incorporated into SC-13].

(2) CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY

[Withdrawn: Incorporated into SC-13].

(3) CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS

[Withdrawn: Incorporated into SC-13].

(4) CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SC-13].

SC-13-COV

Control: The organization shall:

1. Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data.

2. Document appropriate processes before implementing encryption. These processes must include the following components:

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

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

    c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

3. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain.

Digital signatures may be utilized for data that is sensitive solely relative to integrity.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SC-14 PUBLIC ACCESS PROTECTIONS

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

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system:

a. Prohibits remote activation of collaborative computing devices; and

b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21.

Control Enhancements:

(1) *COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*

The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Supplemental Guidance: Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

(2) *COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*

[Withdrawn: Incorporated into SC-7].

(3) *COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*

The organization disables or removes collaborative computing devices from information systems or information system components in secure work areas.

Supplemental Guidance: Failing to disable or remove collaborative computing devices from information systems or information system components can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations.

(4) *COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*

The information system provides an explicit indication of current participants in all online meetings and teleconferences.

Supplemental Guidance: This control enhancement helps to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

References: None.

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

[Withdrawn: Not applicable to COV]

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

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

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

Control Enhancements for Sensitive Systems: None.

SC-18 MOBILE CODE

Control: The organization:

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

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

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) [Withdrawn: Not applicable to COV]

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

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

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

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

Control Enhancements for Sensitive Systems: None.

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

Control: The information system:

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

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Supplemental Guidance: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data.

The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements for Sensitive Systems:

(1) SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES

[Withdrawn: Incorporated into SC-20].

(2) [Withdrawn: Not applicable to COV]

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

Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, 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. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide 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 / INTEGRITY*

[Withdrawn: Incorporated into SC-21]**.**

References: NIST Special Publication 800-81.

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

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to 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 particular roles (e.g., by address ranges, explicit lists). Related controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

References: NIST Special Publication 800-81.

SC-23 SESSION AUTHENTICITY

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

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

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

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

(3) [Withdrawn: Not applicable to COV]

(4) [Withdrawn: Not applicable to COV]

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

SC-24 FAIL IN KNOWN STATE

[Withdrawn: Not applicable to COV]

SC-25 THIN NODES

[Withdrawn: Not applicable to COV]

SC-26 HONEYPOTS

[Withdrawn: Not applicable to COV]

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

[Withdrawn: Not applicable to COV]

SC-28 PROTECTION OF INFORMATION AT REST

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

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

Control Enhancements for Sensitive Systems:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of organization-defined sensitive information stored on any cloud-based information system components. The cryptographic keying material must remain in the control of the commonwealth and cannot be transferred to the owner/operator of the cloud facility

Supplemental Guidance: 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 and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12.

(2) [Withdrawn: Not applicable to COV]

SC-29 HETEROGENEITY

[Withdrawn: Not applicable to COV]

SC-30 VIRTUALIZATION TECHNIQUES

[Withdrawn: Not applicable to COV]

SC-31 COVERT CHANNEL ANALYSIS

[Withdrawn: Not applicable to COV]

SC-32 INFORMATION SYSTEM PARTITIONING

[Withdrawn: Not applicable to COV]

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

[Withdrawn: Not applicable to COV]

SC-35 HONEYCLIENTS

[Withdrawn: Not applicable to COV]

SC-36 DISTRIBUTED PROCESSING AND STORAGE

[Withdrawn: Not applicable to COV]

SC-37 OUT-OF-BAND CHANNELS

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

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

Control Enhancements for Sensitive Systems:

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

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

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

SC-38 OPERATIONS SECURITY

[Withdrawn: Not applicable to COV]

SC-39 PROCESS ISOLATION

Control: The information system maintains a separate execution domain for each executing process.

Supplemental Guidance: Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information 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. This capability is available in most commercial operating systems that employ multi-state processor technologies. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Control Enhancements:

(1) *PROCESS ISOLATION | HARDWARE SEPARATION*

The information system implements underlying hardware separation mechanisms to facilitate process separation.

Supplemental Guidance: Hardware-based separation of information system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Underlying hardware separation mechanisms include, for example, hardware memory management.

(2) *PROCESS ISOLATION | THREAD ISOLATION*

The information system maintains a separate execution domain for each thread in organization-defined sensitive information system multi-threaded processing.

References: None.

SC-40 WIRELESS LINK PROTECTION

[Withdrawn: Not applicable to COV]

SC-41 PORT AND I/O DEVICE ACCESS

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

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.

SC-42 SENSOR CAPABILITY AND DATA

Control: The information system:

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

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

Supplemental Guidance: [Withdrawn: Not applicable to COV]

Control Enhancements: [Withdrawn: Not applicable to COV]

Supplemental Guidance: This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.

Control Enhancements for Sensitive Systems:

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

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

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

(2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

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

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

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

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

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

SC-42-COV

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SC-43 USAGE RESTRICTIONS

Control: The organization:

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

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

Control Enhancements: None.

SC-44 DETONATION CHAMBERS

[Withdrawn: Not applicable to COV]

1.17. *FAMILY:* *SYSTEM AND INFORMATION INTEGRITY* ***CLASS:*** *OPERATIONAL*

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization:

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

b. Reviews and updates the current:
   1. System and information integrity policy on an annual basis or more frequently if required to address an environmental change; and
   2. System and information integrity procedures on an annual basis or more frequently if required to address an environmental change.

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

Control Enhancements for Sensitive Systems: None.

SI-2 FLAW REMEDIATION

Control: The organization:

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

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

c. Installs security-relevant software and firmware updates within 30-days of the release of the updates; and

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

Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

The organization employs automated mechanisms once every 30-days to determine the state of information system components with regard to flaw remediation.

Supplemental Guidance: Related controls: CM-6, SI-4.

(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS

The organization:

(a) Measures the time between flaw identification and flaw remediation; and

(b) Establishes organization-defined benchmarks for taking corrective actions.

Supplemental Guidance: This control enhancement requires organizations to determine the current time it takes on the average to correct information 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 type of flaw and/or severity of the potential vulnerability if the flaw can be exploited.

(4) [Withdrawn: Not applicable to COV]

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

(6) [Withdrawn: Not applicable to COV]

SI-2-COV

Control: The organization:

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

b. Applies all security updates as soon as possible after appropriate testing, not to exceed ~~60~~ *30* days for implementation.

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

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

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

c. Configures malicious code protection mechanisms to:

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

   2. Quarantine malicious code; send alert to administrator in response to malicious code detection; and

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

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious

code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Control Enhancements for Sensitive Systems:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages malicious code protection mechanisms.

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

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

The information system automatically updates malicious code protection mechanisms.

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

(3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS

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

(4) [Withdrawn: Not applicable to COV]

(5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7].

(6) [Withdrawn: Not applicable to COV]

(7) MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION

The information system implements nonsignature-based malicious code detection mechanisms.

Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.

(8) [Withdrawn: Not applicable to COV]

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

SI-3-COV

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

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

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

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

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

   a. Eliminates or quarantines malicious programs that it detects;

   b. Provides an alert notification;

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

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

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

   f. Maintains a log of protection activities.

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

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

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

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

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

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

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

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

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

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

c. [Withdrawn: Not applicable to COV]

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

e. [Withdrawn: Not applicable to COV]

f. [Withdrawn: Not applicable to COV]

g. [Withdrawn: Not applicable to COV]

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The

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

Control Enhancements for Sensitive Systems:

(1) INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

(2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

The organization employs automated tools to support near real-time analysis of events.

Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

(3) [Withdrawn: Not applicable to COV]

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

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

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

(5) INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

The information system alerts the appropriate organization personnel when the organization-defined indicators of compromise or potential compromise occur.

Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, 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 transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.

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

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

(7) [Withdrawn: Not applicable to COV]

(8) INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION

[Withdrawn: Incorporated into SI-4].

(9) [Withdrawn: Not applicable to COV]

(10) [Withdrawn: Not applicable to COV]

(11) [Withdrawn: Not applicable to COV]

(12) [Withdrawn: Not applicable to COV]

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

The organization:

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

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

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

(14) INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

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

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

(15) INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

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

Supplemental Guidance: Related control: AC-18.

(16) INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

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

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

(17) [Withdrawn: Not applicable to COV]

(18) [Withdrawn: Not applicable to COV]

(19) [Withdrawn: Not applicable to COV]

(20) [Withdrawn: Not applicable to COV]

(21) [Withdrawn: Not applicable to COV]

(22) [Withdrawn: Not applicable to COV]

(23) INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES

The organization implements the appropriate organization-defined host-based monitoring mechanisms on all organization-defined sensitive information system components.

Supplemental Guidance: Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers

(24) [Withdrawn: Not applicable to COV]

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

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

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

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

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

Supplemental Guidance: Related control: SI-2.

Control Enhancements for Sensitive Systems:

[Withdrawn: Not applicable to COV]

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system:

a. Verifies the correct operation of organization-defined security functions;

b. Performs this verification at organization-defined system transitional states, upon command by user with appropriate privilege, or at least once every 90-days;

c. Notifies organization-defined personnel of failed security verification tests; and

d. Shuts the information system down when anomalies are discovered.

Supplemental Guidance: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

Control Enhancements:

(1) *SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*

[Withdrawn: Incorporated into SI-6].

(2) *SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*

The information system implements automated mechanisms to support the management of distributed security testing.

Supplemental Guidance: Related control: SI-2.

(3) *SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*

The organization reports the results of security function verification to the appropriate organization-defined personnel.

Supplemental Guidance: Organizational personnel with potential interest in security function verification results include, for example, senior information security officers, information system security managers, and information systems security officers. Related controls: SA-12, SI-4, SI-5.

References: None.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information.

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components

such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

Control Enhancements:

(1) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*

The information system performs 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.

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

(2) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*

The organization employs automated tools that provide notification to the appropriate organization-defined personnel upon discovering discrepancies during integrity verification.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.

(3) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS*

The organization employs centrally managed integrity verification tools.
Supplemental Guidance: 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*

The information system automatically shuts the information system down when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

(6) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, 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. Related control: SC-13.

(7) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*

The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.

(8) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*

The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: *generates an audit record and alerts the organization-defined personnel*.

Supplemental Guidance: 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*

The information system verifies the integrity of the boot process of *devices*.

Supplemental Guidance: Ensuring the integrity of boot processes is critical to starting devices in known/trustworthy states. Integrity verification mechanisms provide organizational personnel with assurance that only trusted code is executed during boot processes.

(10) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY* | *PROTECTION OF BOOT FIRMWARE*

The information system implements *security safeguards* to protect the integrity of boot firmware in *devices*.

Supplemental Guidance: Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted cyber attack. These types of cyber attacks can result in a permanent denial of service (e.g., if the firmware is corrupted) or a persistent malicious code presence (e.g., if code is embedded within the firmware). Devices can protect the integrity of the boot firmware in organizational information systems by: (i) verifying the integrity and authenticity of all updates to the boot firmware prior to applying changes to the boot devices; and (ii) preventing unauthorized processes from modifying the boot firmware.

(11) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY* | *CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*

The organization requires that *user-installed software* execute in a confined physical or virtual machine environment with limited privileges.

Supplemental Guidance: Organizations identify software that may be of greater concern with regard to 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.

(12) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY* | *INTEGRITY VERIFICATION*

The organization requires that the integrity of user-installed software be verified prior to execution.

Supplemental Guidance: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software

integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

(13) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*

The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of the appropriate *organization-defined personnel*.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software.

(14) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*

The organization:

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

(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.

(15) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*

The information system implements cryptographic mechanisms to authenticate software or firmware components prior to installation.

Supplemental Guidance: Cryptographic authentication includes, for example, 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.

(16) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION W/O SUPERVISION*

The organization does not allow processes to execute without supervision for more than 24 hours.

Supplemental Guidance: This control enhancement addresses processes for which normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes, for example, operating system timers, automated responses, or manual oversight and response when information system process anomalies occur.

References: NIST Special Publications 800-147, 800-155.

SI-8 SPAM PROTECTION

Control: The organization:

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

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

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

Control Enhancements for Sensitive Systems:

(1) SPAM PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.

(2) SPAM PROTECTION | AUTOMATIC UPDATES

The information system automatically updates spam protection mechanisms.

(3) [Withdrawn: Not applicable to COV]

SI-8-COV

Control: The organization:

1. Automatically updates spam protection mechanisms of all systems when new releases are available in accordance with organizational configuration management policy and procedures.

SI-9 INFORMATION INPUT RESTRICTIONS

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

SI-10 INFORMATION INPUT VALIDATION

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

Supplemental Guidance: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Control Enhancements for Sensitive Systems:

(1) [Withdrawn: Not applicable to COV]

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

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

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

(3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR

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

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

(4) [Withdrawn: Not applicable to COV]

(5) [Withdrawn: Not applicable to COV]

SI-11 ERROR HANDLING

Control: The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to the appropriate organization-defined personnel.

Supplemental Guidance: Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.

Control Enhancements: None.

References: None.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable commonwealth laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The Library of Virginia provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Control Enhancements: None.

References: 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: The information system implements security safeguards to protect its memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example,

data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.

Control Enhancements: None.

References: None.

SI-17 FAIL-SAFE PROCEDURES

[Withdrawn: Not applicable to COV]

FAMILY: *PM – Program Management*

[Withdrawn: Not applicable to COV]

This page intentionally left blank

GLOSSARY OF SECURITY DEFINITIONS

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

INFORMATION SECURITY ACRONYMS

AITR: Agency Information Technology Representative

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

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

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

ISO: Information Security Officer

ISO/IEC: International Organization for Standardization/

International Electrotechnical Commission

ITIES: Information Technology Investment and Enterprise

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

PCI: Payment Card Industry

PDA: Personal Digital Assistant

PI: Personal Information

PIN: Personal Identification Number

RA: Risk Assessment

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SDLC: Systems Development Life Cycle

Solutions Directorate (VITA)

SSID: Service Set Identifier

SSP: Security Program Plan

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX A – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

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

COV 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	