Title of Document:	Information Technology Resource Management Standard Information Security Standard, 501-09.1 (2016)
Reference to:	6VAC35-160, Regulations Governing Juvenile Record Information and the Virginia Juvenile Justice Information System
Filed by:	State Board of Juvenile Justice
Date filed:	May 10, 2017
Doc available from	Virginia Information Technologies Agency http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/InformationSecurity_Standard_SEC501.pdf

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Security Standard

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to the VITA ~~Policy, Practice and~~ *Enterprise* Architecture ~~(PPA)~~ *(EA)* Division. ~~PPA~~ EA will issue a Change Notice Alert, post it on the VITA Web site, and provide an e-mail announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties ~~PPA~~ EA considers to be interested in the change.

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

Version	Date	Purpose of Revision
Original	12/07/2001	Base Document
Revision 1	07/01/2006	To update all sections of the Standard in accordance with changes to the Code of Virginia as well as incorporate emerging best practices.
	10/10/2006	To remove from section 2.1 (page 3) "Risk Response" that was erroneously left in the final version of this standard. Also, there are no requirements impacted by this correction.
Revision 2	07/1/07	Revision to align with changes (blue highlights) to the Code of Virginia and to document additional and substantively revised standards. The compliance date for these new and substantively revised standards is July 1, 2008.
Revision 3	10/30/2007	Revision to incorporate ITIB's directive (dated October 18, 2007) to change compliance date from July 2008 to November 1, 2007 for section 9.5.2 items 3 through 6.
Revision 4	07/24/08	Revision to align with changes (blue highlights) to the Code of Virginia, removed language in the scope section that excluded "Academic Instruction and Research" systems, and to document additional and revised standards. There is a new section for Application Security. The compliance date for these new and substantively revised standards is January 1, 2009 except for academic and research systems previously exempted, the compliance date shall be July 1, 2009.
Revision 5	08/11/09	Revision to establish a new Wireless Security section and enhance the Application Security section. Broaden scope to include recommendations for security best practices relative to non-electronic data. Refine intent and incorporate changes based on contributions and suggestions of the COV Information Security community. On October 19, 2009, Section 2.2.4 #1 was revised for clarity. Effective February 2, 2010, Section 5.3.2, # 8, page 29 - the requirement related to the frequency of changing user passwords for sensitive systems was changed from 42 days to 90 days to be consistent with current COV network password change frequency requirements. Agencies may require users of sensitive systems to change their passwords on a more frequent basis.

Revision 6	07/11/11	Revision to clarify various requirements indicated in italics and line in the left margin. Revised to address the new IT governance structure in the Commonwealth. See section 2.7.2 #3, section 4.3.2 #s 9, 10, & 11, section 4.7.2 #8, section 9.2.2 # 6, and section 9.5.2 for new guidance and requirements.
Revision 7	11/19/12	Re-designation of COV ITRM SEC501-06 to COV ITRM SEC501-07 due to substantial rewrite of the Commonwealth's Information Security Standard. This Standard has been broadened to include security best practices in line with the National Institute of Standards and Technology (NIST) specifically NIST Special Publication SP800-53. Revision to clarify various NIST and SEC501 requirements indicated in italics and line in the left margin. New Requirements are: AC-2: f, j, 2, AC-4; AC-14; AC-17: 1, 3; AC-19; AC-20; AC-22; AU-2: c, 3; AU-3: 2; AU-4; AU-5; AU-6: b, 1, 3, 4, 5, AU-8, AU-9; AU-11; CA-1; CA-3; CA-6; CA-7; CM-3: 4; CM-7; CM-8; CM-9: 1; IR-2: 1; IR-3; IR-6: 2; IR-7; IR-8: c, d, e; MA-5: b; PE-3: f, 1; PE-11; PE-18: 1; PL-6; PS-4: c, d; RA-5: b, d; 1, 2, 3, 4, 5, 8; SA-2; SA-6: c; SC-2; SC-3; SC-7; SC-14; SC-17; SC-20; SI-3: d, 1, 2, 3; SI-8
Revision 7.1	01/28/2013	Administrative changes to clarify; 1.1, AC-2-COV, CA-3-COV, CM-2-COV, IR-4-COV-1, IR-4-COV-2, IR-6-COV, PL-2-COV, PL-4-COV, SC-8-COV, SC-9-COV, SC-13-COV, SI-2-COV, and minor corrections to Appendix B. Sections inserted that were left out at publication; AC-17-COV, CP-1-COV-1, CP-1-COV-2, CP-9-COV, MP-1-COV, MP-4-COV, PE-2-COV, PE-3-COV, and SI-3-COV.
Revision 8	04/03/2014	Administrative changes to Control Family Table indexes: 5.3.2.8, 5.3.2.10, 5.3.2.11 Clarifying language added to AC2-COV 1.b. Section inserted that was left out of previous publication: IA-5-COV-2 New Requirements are: IA-2 CESS 1, 6, IA-2-COV
Revision 9	02/20/2015	Updated in concert with NIST 800-53 Revision 4 and CyberSecurity Framework. New Requirements: AC-2: j, k 12, 13; AC-6: 5, 7, 9, 10; AC-19: 5; AC-20: 3, 4; AT-2: 1, 2; AU-4: 1; AU-5; AU-6: 1, 6, 7, 9, 10; AU-8: 1; AU-12; AU-13; CA-7: 3; CM-2-COV: 4; CM-3: 6; CM-5: 1; CM-10; CM-11; CP-2: 4, 7; CP-7: 6; IA-2: 5; IR-3: 2; IR-4: 6, 7, 8; IR-8: f; MA-2: f; MA-5: b, c; MP-5: c; PE-13: 1, 2, 3, 4; PE-14: 1, 2; PL-4: c, d; PS-4: b, f; PS-6: a, c; PS-7: b, d; RA-3: d; RA-5: 10; SA-3: d; SA-5: d, e; SA-11: 4, 6, 7; SA-15; SA-16; SA-17; SA-22; SC-5; SC-7: b, 11; SC-18; SC-19; SC-37; SC-41; SC-42; SC-42-COV; SC-43; SI-4: 13, 16; SI-10: 2, 3; May 21st, 2015, Table of Contents updated to include all sections and keep numbering consistent. Section inserted that was left out at publication; AC-2-COV Clarifying language added to section 2.5.7

Revision 9.1	*12/8/2016*	*This administrative update is necessitated by changes in the Code of Virginia and organizational changes in VITA. No substantive changes were made to this document.*

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.*

Review Process

~~Policy, Practices, and~~ *Enterprise* Architecture ~~(PPA)~~ *(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 SEC501-09.1

Subject
Information Security

Effective Date
December 8, 2016

Compliance Date
December 8, 2016

Supersedes
COV ITRM Standard SEC501-09 dated ~~April 3, 2014~~ May 01 2051.

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)*

~~**Secretary of Technology**~~
~~Reviews and approves statewide technical and data policies, standards and guidelines for information technology and related systems recommended by the CIO.~~

Chief Information Officer of the Commonwealth (CIO)
Develops and *approves* ~~recommends to the Secretary of Technology~~ 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."*

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

1. INTRODUCTION

1.1 Intent

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

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

This Standard has been created using the National Institute of Standards and Technology (NIST) Special Publication 800-53 rev. *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:

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

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

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:

- Obtaining the commonwealth ISO Certification
  - Attending Information Security Orientation training, *biennially*
  - Successfully completing at least 3 security courses authorized by the CISO (i.e. Knowledge Center "ISO Academy"). Possessing a recognized professional IT Security Certification, i.e., CISSP, CISM, CISA, SANS, may substitute for 2 courses.
  - Attending the mandatory ISOAG meeting, as designated by the CISO.

- Annually maintaining the ISO certification:
  - Obtaining 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 other recognized professional IT Security Certifications may be applied to this requirement.
  - At least 1 hour of the 20 hours should be authorized by the CISO (i.e. Knowledge Center "ISO Academy").
  - Continue attending Information Security Orientation training, biennially
  - Continue attending the mandatory ISOAG meeting, as designated by the CISO.

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.

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 Records	High	High	High

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.

8.1. 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 commensurate 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-2-COV

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

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

1. For all internal and external IT systems:

   a. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.

   b. Disable unneeded accounts in a timely manner.

   c. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.

   d. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.

   e. Require that the System Owner and the System Administrator investigate any unusual system access activities and approve changes to access level authorizations.

   f. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.

   g. Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined residual risks.

   h. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

   i. The information system automatically audits account creation, disabling, and termination actions and notifies, as required, appropriate individuals.

j. Temporarily disable logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.

k. Disable logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

2. For all internal IT systems:

a. Require a documented request from the user to establish an account on any internal IT system.

b. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.

c. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the Data Owner, Data Owner or designee, or ISO to establish accounts for all sensitive IT systems.

d. Require secure delivery of access credentials to the user based on information already on file.

e. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.

f. Promptly remove access when no longer required.

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

4. For all service and hardware accounts:

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

Supplemental Guidance: None

Control Enhancements for Sensitive Systems:

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

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

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

b. Include access attributes for the account.

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

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

3. For all external IT systems:

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

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

AC-3 ACCESS ENFORCEMENT

Control: 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. 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 10 consecutive invalid logon attempts by a user during a 15 minute period; and

b. Automatically locks the account/node for a minimum of a 15 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 30 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 60 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 30 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]

8.2. 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].

8.3. 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: authentication attempt, authenticated individual, access time, source of access, duration of access, and actions executed;

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 every 30-days 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, and applications;

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

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

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;

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

[Withdrawn: Not applicable to COV]

CA-9 INTERNAL SYSTEM CONNECTIONS

[Withdrawn: Not applicable to COV]

8.5. 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 an annual 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, 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 an annual 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 an annual 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.

8.6. 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 30-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]

8.7. 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;