**Test\_2015-01-15-1052**

**([project acronym not provided])**

**[project ID not provided]**

**System Security Plan**

**(SSP)**

Prepared for  
**Department of Homeland Security Headquarters (DHS HQ)**

**16 January 2015**

(Content Version – 2012-01)

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS UNCLASSIFIED UNTIL FILLED IN (FOR OFFICIAL USE ONLY) INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS MUST BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH PUBLIC LAW, EXECUTIVE ORDERS, DHS MANAGEMENT DIRECTIVES, AND OTHER REGULATIONS GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, MUST BE STORED IN AN APPROPRIATE MANNER AS DIRECTED BY PUBLIC LAW, EXECUTIVE ORDERS, DHS MANAGEMENT DIRECTIVES, AND OTHER REGULATIONS REGARDING PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS, AND UNAUTHORIZED DISCLOSURE.

**DOCUMENT CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
|  |  |  |  |
|  |  |  |  |

# Preface

This system security plan (SSP) was developed by Department of Homeland Security Headquarters (DHS HQ) under the direction of the Department of Homeland Security Headquarters (DHS HQ)for use on designated National Security Systems.

This plan is based upon a review of the environment, documentation, DHS regulations/guidance, and interviews with the information system personnel conducted between dates. In addition to this plan, Risk Assessment (RA), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M)] have been developed under this task.

This SSP documents the current and planned controls for the system and addresses security concerns that may affect the system’s operating environment.

TABLE OF CONTENTS

[Preface 2](#_Toc256000000)

[1.0 System Identification 5](#_Toc256000001)

[1.1 Definition 5](#_Toc256000002)

[1.2 System Name 5](#_Toc256000003)

[1.3 Information Categorization 5](#_Toc256000004)

[1.4 Responsible Organization/Personnel and Contact Information 6](#_Toc256000005)

[1.5 System Operation 7](#_Toc256000006)

[1.5.1 System Operational Status 7](#_Toc256000007)

[1.5.2 Authorization Status 7](#_Toc256000008)

[1.5.3 System Operation (Government or Contractor Operation) 7](#_Toc256000009)

[1.6 General Description/Mission 7](#_Toc256000010)

[1.6.1 Authorization Boundary 7](#_Toc256000011)

[1.6.2 System Users 7](#_Toc256000012)

[1.6.3 Architecture 8](#_Toc256000013)

[1.6.4 Major Applications 9](#_Toc256000014)

[1.6.5 Subsystems/Minor Applications 9](#_Toc256000015)

[1.6.6 Hardware/Virtual Machines/Software/Firmware Description 9](#_Toc256000016)

[1.6.7 Encryption/PKI 10](#_Toc256000017)

[1.6.8 Encryption Devices 10](#_Toc256000018)

[1.7 System Environment 10](#_Toc256000019)

[1.8 NSS Physical Environment Considerations 10](#_Toc256000020)

[1.9 System Interconnection/Information Sharing 11](#_Toc256000021)

[1.9.1 Information Flow 11](#_Toc256000022)

[1.9.2 System Interconnections 11](#_Toc256000023)

[1.9.3 Cross Domain Solutions 12](#_Toc256000024)

[1.9.4 Cloud Service Layers 12](#_Toc256000025)

[1.9.5 Mobile Code 12](#_Toc256000026)

[1.9.6 Ports, Protocols, & Services 12](#_Toc256000027)

[1.10 Privacy Considerations 12](#_Toc256000028)

[1.11 Overlays 13](#_Toc256000029)

[1.12 Applicable Laws/ Regulations/Policies Affecting the System 13](#_Toc256000030)

[1.12.1 Sensitive Systems Laws, Regulations, and Policies 13](#_Toc256000031)

[(with 800-53 Rev 4) 14](#_Toc256000032)

[1.12.2 National Security Systems Laws, Regulations, and Policies 14](#_Toc256000033)

[2.0 Access Control (AC) 15](#_Toc256000034)

[3.0 Awareness and Training (AT) 39](#_Toc256000035)

[4.0 Audit and Accountability (AU) 42](#_Toc256000036)

[5.0 Security Assessment and Authorization (CA) 57](#_Toc256000037)

[6.0 Configuration Management (CM) 71](#_Toc256000038)

[7.0 Contingency Planning (CP) 92](#_Toc256000039)

[8.0 Identification and Authentication (IA) 111](#_Toc256000040)

[9.0 Incident Response (IR) 126](#_Toc256000041)

[10.0 Maintenance (MA) 134](#_Toc256000042)

[11.0 Media Protection (MP) 142](#_Toc256000043)

[12.0 Physical and Environmental Protection (PE) 152](#_Toc256000044)

[13.0 Planning (PL) 165](#_Toc256000045)

[14.0 Personnel Security (PS) 172](#_Toc256000046)

[15.0 Risk Assessment (RA) 178](#_Toc256000047)

[16.0 System and Services Acquisition (SA) 184](#_Toc256000048)

[17.0 System and Communications Protection (SC) 199](#_Toc256000049)

[18.0 System and Information Integrity (SI) 223](#_Toc256000050)

[19.0 Program Management (PM) 240](#_Toc256000051)

[20.0 Privacy 250](#_Toc256000052)

[21.0 Plan Approval 268](#_Toc256000053)

[Acronyms 269](#_Toc256000054)

**LIST OF TABLES**

[Table 1‑1 System Name 5](#_Toc256000055)

[Table 1‑2 Security Categorization 5](#_Toc256000056)

[Table 1‑3 System Designations 5](#_Toc256000057)

[Table 1‑4 Information Types 5](#_Toc256000058)

# System Identification

This system security plan (SSP) provides an overview of security requirements for Test\_2015-01-15-1052([project acronym not provided]) and describes controls in place or planned for implementation to provide a level of security appropriate for the information processed.  The SSP includes user responsibilities, roles and limitations, and general security procedures for users and security personnel. This section describes the implementation status security controls.

Security safeguards for the system shall meet the policy requirements set forth in this SSP. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

## Definition

## System Name

Table 1.0‑1 System Name

|  |  |
| --- | --- |
| FISMA ID: |  |
| System Name: | Test\_2015-01-15-1052 |
| System Abbreviation: | [project acronym not provided] |
| Version: | [project version not provided] |

## Information Categorization

This section summarizes the [project acronym not provided] information security categorization levels as determined by the FIPS 199 Information Security Categorization. The [project acronym not provided] security impact levels for each of the three security objectives of confidentiality, integrity, and availability are identified in Table 1-2.

Table 1.0‑2 Security Categorization

|  |  |
| --- | --- |
| Confidentiality Impact Level: | High |
| Integrity Impact Level: | High |
| Availability Impact Level: | High |

Table 1.0‑3 System Designations

|  |  |
| --- | --- |
| Chief Financial Officer (CFO) Designated Financial System | No |
| System Contains Privacy Data or PII |  |
| Classification or Sensitivity Level | UNCLASSIFIED//FOUO |
| Mission Essential System | No |

Table 1.0‑4 Information Types

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| **Information Type** | **Highest Data Classification** | **Confidentiality impact** | **Integrity impact** | **Availability impact** | **Justification** |

## Responsible Organization/Personnel and Contact Information

The following DHS Component/Personnel are identified as the parties responsible for the system development of Test\_2015-01-15-1052, its software maintenance and patch management. Also identified are the roles of system owner, technical information point-of-contact, authorizing official, security control assessor, CISO/ISSM, ISSO and any other role that has a significant responsibility to ensure the system is appropriately secure. It is the functional proponent or advocate for the information system and the activity responsible for identifying the funding for system development, deployment, and maintenance throughout the system's life cycle.

**Table 1-5. Responsibility/Accountability Matrix**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Responsible Organization** | **Organization** | | **POC** | | | |
| **Name (Include sub-component/department name)** | **Address** | **Name** | **Address** | **Phone** | **Email** |

## System Operation

### System Operational Status

The information system is in the following life cycle status:

### Authorization Status

The information system has the following authorization status:

### System Operation (Government or Contractor Operation)

{Identify who owns the system and who operates the system. The values are Government Owned Government Operated (GOGO), Government Owned Commercially Operated (GOCO), Commercially Owned Government Operated (COGO), or Commercially Owned Commercially Operated (COCO).}

## General Description/Mission

The following section provides an overview of the [project acronym not provided]**,** and identifies the system’s mission, capabilities, users, and information data flow. It also describes the hardware, software and firmware implemented in support of [project acronym not provided]**.**

### Authorization Boundary

*{This section should include a description, in text, detailing the external boundary of the information system. The description should address applicable environments other than the primary production environment (i.e., maintenance, testing/development or backup environments). Where required the description should detail lines of responsibility demarcation that exist for any controls inherited from other information systems.}*

### System Users

|  |  |  |  |
| --- | --- | --- | --- |
| **System Users Categories** | | | |
| **Category Name** | **Minimum Clearance/Investigation** | **Foreign Nationals** | **Category Description** |
| Master Administrator | Confidential | Not Allowed | A master administrator has full access to the entire application and is able to create additional master administrators as well as all other account types. Only master administrators have access to all of the application’s administrative tools. |
| Administrator | Confidential | Not Allowed | Administrators have permission to view and edit any information to which they have access. Administrator accounts should be given to those who have a need to access, edit, or configure your organization’s projects, continuous assessment settings, and reports. |
| Security Administrator | Confidential | Not Allowed | Security Administrators are similar to master administrators, but they have read-only access to everything except the application’s Audit page (Administration > Audit). Only security administrators and master administrators can view, export and clear the Audit. |
| Audit/Executive | Confidential | Not Allowed | Auditor/Executive accounts are similar to administrators, but have read-only access. Executive accounts are intended for managers who need to monitor progress, compliance, and risk levels. |
| User | Confidential | Not Allowed | User accounts are typically given to analysts who will require basic access to the system. Users typically must be assigned to a project in order to access it. Users do not have administrative rights over their projects. |

There are no project personnel roles assigned to your system.

### Architecture

The following architectural drawings of Test\_2015-01-15-1052 provide a visual depiction of the major system hardware elements that constitute Test\_2015-01-15-1052.

### Major Applications

The following table(s) identifies the major applications supported by the information system.

**Table 1-6. Major Application Supported by Test\_2015-01-15-1052**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Application Name** | **Function** | **Type of Information** | **FISMA ID** | **Confidentiality Impact Level** | **Integrity Impact Level** | **Availability Impact Level** |
|  |  |  |  |  |  |  |

### Subsystems/Minor Applications

The following table(s) identify the subsystems/Minor Applications for Test\_2015-01-15-1052.

**Table 1-7. Test\_2015-01-15-1052 Subsystems/Minor Applications**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Application Name** | **Function** | **Type of Information** | **FISMA ID** | **Location** |
|  |  |  |  |  |

### Hardware/Virtual Machines/Software/Firmware Description

There is no hardware associated with the project.

There is no software in the project.

### Encryption/PKI

{*This section should address the types of encryption solutions deployed for the information system.*}

**Table 1-6. PKI Certificates**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Certificate Name** | **Certificate Type** | **Certificate Issuer** | **Expiration Date** | **Cryptography Algorithm Supported** |
|  |  |  |  |  |

### Encryption Devices

{Identify any encryption devices used in the system architecture. These should be identified in the system architecture diagram included in section 1.4.5, and described in the following table:}

**Table 1-10. Encryption Devices**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hostname** | **MFR** | **Model** | **Version** | **Location** |
|  |  |  |  |  |

## System Environment

{*This section should discuss the physical environment of the information system including any special circumstances that may increase the risk of the operating the system - For example: The system does not not reside in a DHS Datacenter (DC1 or DC2).   
  
This section should also detail any system elements, hardware or software that mitigates the security risks of operating the system.* }

## NSS Physical Environment Considerations

{*This section should address the types of encryption solutions deployed for the information system.*}

**Table 1-11 NSS Physical Environment Considerations**

|  |  |
| --- | --- |
| Is the secure facility authorized or approved to process and store information at the level covered by this SSP? | [ ]Yes [ ] No |
| Who authorized or approved the facility? |  |
| Provide date and location of approval letter. |  |
| State the classification and level approved for the facility. | [ ] Secret [ ] Top Secret [ ] Others (Please Specify) |
| Is the system approved for unattended processing? | [ ]Yes [ ] No |
| Is the facility approved for 24-hour operation? | [ ]Yes [ ] No |

## System Interconnection/Information Sharing

### Information Flow

*{This section should discuss how data flows across each interconnection listed in the tables above as well as describe the flow of data across key internal system boundaries.}*

### System Interconnections

There is no system interconnection/information sharing associated with your project.

### Cross Domain Solutions

{Is there a Cross Domain Solution associated with the system? A CDS is required for any information that crosses a security domain electronically. Manual (i.e., sneaker-net) transfers must also be identified. If there is a cross domain system associated with the system a table like the one below should be completed. }

**Table 1-13: Cross Domain Solutions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hostname** | **MFR** | **Model** | **Version** | **Ticket No.** | **Location** |
|  |  |  |  |  |  |

### Cloud Service Layers

Information systems, particularly those based on cloud architecture models, are made up of different service layers. The layers of the Test\_2015-01-15-1052 that are defined in this SSP, and are not leveraged by any other Provisional Authorizations, are indicated in the table that follows.

**Table 1-14: Cloud Service Layers Represented in this SSP**

|  |  |  |
| --- | --- | --- |
| **Service Provider Architecture Layers** | | |
| [ ] | Software as a Service (SaaS) | Major Application |
| [ ] | Platform as a Service (PaaS) | Major Application |
| [ ] | Infrastructure as a Service (IaaS) | General Support System |
| [ ] | Other | Explain: |

### Mobile Code

{*This section should declare the use and approval of any mobile code deployed within the boundaries of the information system.*}

### Ports, Protocols, & Services

## Privacy Considerations

{Section 208 of the E-Government Act of 2002 and Section 522 of the Consolidated Appropriations Act of 2005 require that when developing or procuring IT systems or projects that collect, use, store, and/or disclose information in identifiable form from or about members of the public or organization employees (the latter prescribed by sect. 522), to identify potential privacy risks and implement appropriate privacy controls and compliance requirements. Insert the system "does" or "does not" contain privacy information. Determine and document if the Privacy Act applies to this system. If the Privacy Act applies and the system contains privacy information, insert a reference to privacy-related documentation (e.g., A Privacy Impact Assessment (PIA), Privacy Threshold Analysis (PTA) was conducted as part of the current authorization process), and the date the documentation was submitted.}

## Overlays

{This section provides a listing of any applicable overlays applied to the NSS. An applied overlay should be used to complement the security control baselines and parameter values, and provides a specification of security controls and supporting guidance that may be more stringent or less stringent than the security controls and guidance complemented.

CNSSI 1253 Appendix K provides additional guidance on overlays.

The below format is a suggested way to capture those overlays that may be applied to an NSS, and should be a comprehensive listing of all applied overlays. If no overlays applied to this NSS, include a statement in this section along to the effect of, "No overlays apply to this NSS."

[Name of Overlay applicable to NSS, if any]   
[Name of Overlay applicable to NSS, if any]}

{For DHS sensitive systems, use "No overlays apply to this system."}

## Applicable Laws/ Regulations/Policies Affecting the System

### Sensitive Systems Laws, Regulations, and Policies

Following are the laws and regulations that affect the system:

* Federal Information Security Management Act of 2002 (FISMA), 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899
* Office of Management and Budget (OMB) Circular A-130, *"Management of Federal Information Resources,"* revised, November 30, 2000
* DHS Management Directive MD 140-01, *"Information Technology Systems Security,"* July 31, 2007
* National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* March 2006
* NIST SP 800-53, Rev 3, *"Recommended Security Controls for Federal Information Systems and Organizations,"* August 2009, with updated errata May 01, 2010
* *DHS Sensitive Systems Policy Directive 4300A*
* *DHS Sensitive Systems Handbook 4300A*

Component and System Specific Laws/Regulations/Policies:

* Department of Homelad Security Department of Homeland Security Sensitive Systems Policy Directive 4300A Version 10 TBD

# (with 800-53 Rev 4)

### National Security Systems Laws, Regulations, and Policies

For laws, regulations, and policies that apply to DHS national security systems, refer to 4300B.108-1.

# 2.0 Access Control (AC)

|  |  |  |
| --- | --- | --- |
| 2.1 | Access Control Policy and Procedures | AC-1 |
| Control: Access Control Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (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.  (b) Reviews and updates the current:  (1) Access control policy [Assignment: organization-defined frequency]; and, (2) Access control procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.2 | Access Control Policy and Procedures | AC-1 (DHS-5.1.1.c) |
| Control: Sharing of Personal Passwords  DHS users shall not share personal passwords.  Related control: IA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.3 | Account Management | AC-2 |
| Control: Account Management  The organization:  (a) Identifies the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];  (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 [Assignment: organization-defined personnel or roles] for requests to create information system accounts;  (f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];  (g) Authorizes, and 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 [Assignment: organization-defined frequency]; 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.4 | Account Management | AC-2 (1) |
| Control: Account Management  The organization employs automated mechanisms to support the management of information system accounts.  Supplemental Guidance  The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.5 | Account Management | AC-2 (2) |
| Control: Account Management  The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].  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.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.6 | Account Management | AC-2 (3) |
| Control: Account Management  The information system automatically disables inactive accounts after [Assignment: organization-defined time period].  Supplemental Guidance  None.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.7 | Account Management | AC-2 (4) |
| Control: Account Management  The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required, [Assignment: organization-defined personnel or roles].  Supplemental Guidance  None.  Related controls: AU-2, AU-12.   References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.8 | Account Management | AC-2 (5) |
| Control: Account Management  The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].  Supplemental Guidance  None.  Related control: SC-23.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.9 | Account Management | AC-2 (11) |
| Control: Account Management  The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].   Supplemental Guidance  Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.10 | Access Enforcement | AC-3 |
| Control: Access Enforcement  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.11 | Access Enforcement | AC-3 (DHS-5.1.1.d) |
| Control: Access Enforcement  Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password shall be approved by the appropriate Authorizing Official (AO).  Related control: IA-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.12 | Information Flow Enforcement | AC-4 |
| Control: Information Flow Enforcement  The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: 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 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-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.  References: Web: ucdmo.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.13 | Separation of Duties | AC-5 |
| Control: Separation of Duties  The organization:  (a) Separates [Assignment: organization-defined duties of individuals]; (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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.14 | Least Privilege | AC-6 |
| Control: Least Privilege  The organization employs the concept of least privilege, allowing only authorized accesses for users (and 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 concept 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.15 | Least Privilege | AC-6 (1) |
| Control: Least Privilege  The organization explicitly authorizes access to [Assignment: 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.16 | Least Privilege | AC-6 (2) |
| Control: Least Privilege  The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing non-security 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.17 | Least Privilege | AC-6 (3) |
| Control: Least Privilege  The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.  Supplemental Guidance  Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).  Related control: AC-17.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.18 | Least Privilege | AC-6 (5) |
| Control: Least Privilege  The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.19 | Least Privilege | AC-6 (9) |
| Control: Least Privilege  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.20 | Least Privilege | AC-6 (10) |
| Control: Least Privilege  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. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.21 | Unsuccessful Logon Attempts | AC-7 |
| Control: Unsuccessful Logon Attempts  The information system:  (a) Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and (b) Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.22 | System Use Notification | AC-8 |
| Control: System Use Notification  The information system:  (a) Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:  (1) Users are accessing a U.S. Government 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 to users the system use information [Assignment: organization-defined conditions], before granting further access; (2) Displays to users 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 in the notice given to public users of the information system, 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 Office of the General Counsel for legal review and approval of warning banner content.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.23 | System Use Notification | AC-8 (DHS-4.8.5.d) |
| Control: System Use Notification  The use of Government office equipment and DHS systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.  Related control: AC-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.24 | Concurrent Session Control | AC-10 |
| Control: Concurrent Session Control  The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].  Supplemental Guidance  Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.25 | Session Lock | AC-11 |
| Control: Session Lock  The information system:  (a) Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] 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.  References: OMB Memorandum 06-16. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.26 | Session Lock | AC-11 (1) |
| Control: Session Lock  The information system conceals 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.  Related control: None.  References: OMB Memorandum 06-16. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.27 | Session Termination | AC-12 |
| Control: Session Termination  The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.28 | Permitted Actions without Identification or Authentication | AC-14 |
| Control: Permitted Actions without Identification or Authentication  The organization:  (a) Identifies [Assignment: organization-defined 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 federal 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.29 | Remote Access | AC-17 |
| Control: Remote Access  The organization:  (a) Establishes 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 virtual private networks (VPN) to enhance confidentiality and integrity over remote connections. The use of VPNs, does not technically make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls 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 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.  References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.30 | Remote Access | AC-17 (1) |
| Control: Remote Access  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.  References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.31 | Remote Access | AC-17 (2) |
| Control: Remote Access  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.  References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.32 | Remote Access | AC-17 (3) |
| Control: Remote Access  The information system routes all remote accesses through [Assignment: organization-defined number] 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.  References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.33 | Remote Access | AC-17 (4) |
| Control: Remote Access  The organization:  (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: 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.  References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.34 | Remote Access | AC-17 (DHS-5.4.1.b) |
| Control: Remote Access  Components shall centrally manage all remote access and dial-in connections to their systems and shall ensure that remote access and approved dial-in capabilities provide strong two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on Department-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, Security Requirements for Cryptographic Modules. See Section 3.14 of this Policy Directive, “Privacy and Data Security” for additional requirements involving remote access of PII.  Related Controls: AC-4, AC-17, AU-2 SC-7, SC-8, and SC-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.35 | Remote Access | AC-17 (DHS-5.4.1.c) |
| Control: Remote Access  Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished by means of virtual private network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and Security Plan (SP) shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.  Related controls: AC-4, AC-17, AU-2 SC-7, SC-8, and SC-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.36 | Wireless Access | AC-18 |
| Control: Wireless Access  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.  References: NIST Special Publications 800-48, 800-94, 800-97. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.37 | Wireless Access | AC-18 (1) |
| Control: Wireless Access  The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.  Supplemental Guidance  None.  Related controls: SC-8, SC-13.  References: NIST Special Publications 800-48, 800-94, 800-97. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.38 | Wireless Access | AC-18 (4) |
| Control: Wireless Access  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.  References: NIST Special Publications 800-48, 800-94, 800-97. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.39 | Wireless Access | AC-18 (5) |
| Control: Wireless Access  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.  References: NIST Special Publications 800-48, 800-94, 800-97. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.40 | Access Control for Mobile Devices | AC-19 |
| Control: Access Control for Mobile Devices  The organization:  (a) Establishes usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices; and (b) Authorizes 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.  References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.41 | Access Control for Mobile Devices | AC-19 (5) |
| Control: Access Control for Mobile Devices  The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined 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 control: MP-5, SC-13, SC-28.  References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.42 | Use of External Information Systems | AC-20 |
| Control: Use of External Information Systems  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 nonfederal governmental organizations; and (iv) federal 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 federal 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 federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable 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 (e.g., individuals accessing federal information through www.usa.gov). 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.  References: FIPS Publication 199. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.43 | Use of External Information Systems | AC-20 (1) |
| Control: Use of External Information Systems  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.  References: FIPS Publication 199. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.44 | Use of External Information Systems | AC-20 (2) |
| Control: Use of External Information Systems  The organization [Selection: restricts; prohibits] 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.  Related control: None.  References: FIPS Publication 199. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.45 | Information Sharing | AC-21 |
| Control: User-Based Collaboration and Information Sharing  The organization:  (a) Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and  (b) Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.  Supplemental Guidance  This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.  Related control: AC-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 2.46 | Publicly Accessible Content | AC-22 |
| Control: Publicly Accessible Content  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 [Assignment: organization-defined frequency] and removes such information, if discovered.  Supplemental Guidance  In accordance with federal 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 3.0 Awareness and Training (AT)

|  |  |  |
| --- | --- | --- |
| 3.47 | Security Awareness and Training Policy and Procedures | AT-1 |
| Control: Security Awareness and Training Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (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 [Assignment: organization-defined frequency]; and (2) Security awareness and training procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-16, 800-50, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 3.47 | Security Awareness Training | AT-2 |
| Control: Security Awareness  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) [Assignment: organization-defined frequency] 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.  References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); Executive Order 13587; NIST Special Publication 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 3.47 | Security Awareness Training | AT-2 (2) |
| Control: Security Awareness  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 control: PL-4, PM-12, PS-3, PS-6.  References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); Executive Order 13587; NIST Special Publication 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 3.47 | Role-Based Security Training | AT-3 |
| Control: Security Training  The organization provides role-based security-related training:  (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.  Supplemental Guidance  The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program.  Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.  References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 3.47 | Security Training Records | AT-4 |
| Control: Security Training Records  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 [Assignment: organization-defined time period].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 4.0 Audit and Accountability (AU)

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit and Accountability Policy and Procedures | AU-1 |
| Control: Audit and Accountability Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or 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 [Assignment: organization-defined frequency]; and (2) Audit and accountability procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Events | AU-2 |
| Control: Audit Events  The organization:  (a) Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events]; (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 list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and, (d) Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].  Supplemental Guidance  The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system 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 extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.  Related control: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.  References: NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Events | AU-2 (3) |
| Control: Auditable Events  The organization reviews and updates the list of auditable events [Assignment: organization-defined frequency].  Supplemental Guidance  The list of auditable events is defined in AU-2.  Related control: None.  References: NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Content of Audit Records | AU-3 |
| Control: Content of Audit Records  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Content of Audit Records | AU-3 (1) |
| Control: Content of Audit Records  The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].  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.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Content of Audit Records | AU-3 (2) |
| Control: Content of Audit Records  The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Storage Capacity | AU-4 |
| Control: Audit Storage Capacity  The organization allocates audit record storage capacity in accordance with [Assignment: 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Response to Audit Processing Failures | AU-5 |
| Control: Response to Audit Processing Failures  The information system:  (a) Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and (b) Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Response to Audit Processing Failures | AU-5 (1) |
| Control: Response to Audit Processing Failures  The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.  Supplemental Guidance  Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Response to Audit Processing Failures | AU-5 (2) |
| Control: Response to Audit Processing Failures  The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].  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).  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 |
| Control: Audit Review, Analysis, and Reporting  The organization:  (a) Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and (b) Reports findings to [Assignment: organization-defined personnel or roles].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 (1) |
| Control: Audit Review, Analysis, and Reporting  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 (3) |
| Control: Audit Review, Analysis, and Reporting  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 (5) |
| Control: Audit Review, Analysis, and Reporting  The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 (6) |
| Control: Audit Review, Analysis, and Reporting  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 identify 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.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 (DHS-5.3.b) |
| Control: Audit Review, Analysis, and Reporting  Audit records for financial systems or for systems hosting or processing Personally Identifiable Information (PII) shall be reviewed each month. Unusual activity or unexplained access attempts shall be reported to the System Owner and Component CISO/ISSM.  Related control: AU-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Review, Analysis, and Reporting | AU-6 (DHS-5.4.6.f) |
| Control: Audit Review, Analysis, and Reporting  Components shall conduct mail server administration in a secure manner. This includes: - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Reduction and Report Generation | AU-7 |
| Control: Audit Reduction and Report Generation  The information system provides an audit reduction and report generation capability that:  (a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and (b) Does not alter the original content or time ordering of audit records.  Supplemental Guidance  Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.  Related control: AU-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Reduction and Report Generation | AU-7 (1) |
| Control: Audit Reduction and Report Generation  The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].  Supplemental Guidance  Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.  Related controls: AU-2, AU-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Time Stamps | AU-8 |
| Control: Time Stamps  The information system:  (a) Uses internal system clocks to generate time stamps for audit records; and (b) Generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Time Stamps | AU-8 (1) |
| Control: Time Stamps  The information system:  (a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].  Supplemental Guidance  This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Protection of Audit Information | AU-9 |
| Control: Protection of Audit Information  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Protection of Audit Information | AU-9 (2) |
| Control: Protection of Audit Information  The information system backs up audit records [Assignment: organization-defined frequency] 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Protection of Audit Information | AU-9 (3) |
| Control: Protection of Audit Information  The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.  Supplemental Guidance  Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.  Related controls: AU-10, SC-12, SC-13.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Protection of Audit Information | AU-9 (4) |
| Control: Protection of Audit Information  The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Non-repudiation | AU-10 |
| Control: Non-repudiation  The information system protects against an individual falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].  Supplemental Guidance  Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).  Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Record Retention | AU-11 |
| Control: Audit Record Retention  The organization retains audit records for [Assignment: organization-defined time period consistent with 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. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.  Related controls: AU-4, AU-5, AU-9, MP-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Record Retention | AU-11 (DHS-5.3.d) |
| Control: Audit Record Retention  Components shall ensure that audit logs are recorded and retained in accordance with the Component’s Record Schedule or with the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least ninety (90) days. Audit trail records shall be preserved for a period of seven (7) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.  Related control: AU-11.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Generation | AU-12 |
| Control: Audit Generation  The information system: (a) Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; (b) Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and (c) Generates audit records for the events defined in AU-2 d. with the 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Generation | AU-12 (1) |
| Control: Audit Generation  The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].  Supplemental Guidance  Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.  Related controls: AU-8, AU-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 4.47 | Audit Generation | AU-12 (3) |
| Control: Audit Generation  The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].  Supplemental Guidance  This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours.  Related control: AU-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 5.0 Security Assessment and Authorization (CA)

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessment and Authorization Policies and Procedures | CA-1 |
| Control: Security Assessment and Authorization Policies and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (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 [Assignment: organization-defined frequency]; and (2) Security assessment and authorization procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security assessment and authorization family. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy.  Related control: PM-9.  References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessment and Authorization Policies and Procedures | CA-1 (DHS-3.9.m) |
| Control: Security Assessment and Authorization Policies and Procedures  Currently, all DHS systems shall be authorized using the automated IACS tools that have been approved by the DHS CISO.  Related control: CA-1, CA-2, and PM-10.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessment and Authorization Policies and Procedures | CA-1 (DHS-3.18.c) |
| Control: Security Assessment and Authorization Policies and Procedures  The use of cloud environments shall follow normal DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the Component or DHS-designated risk executive.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessment and Authorization Policies and Procedures | CA-1 (DHS-3.18.d) |
| Control: Security Assessment and Authorization Policies and Procedures  All DHS cloud services (whether hosted internally in the DHS data centers or in a FedRAMP CSP) intended for internal use only do not require a 3PAO assessment but shall use FedRAMP documentation templates, be assessed using existing processes, and be categorized in the FISMA inventory as either a major application, minor application or subsystem. DHS cloud services shall not be categorized as External Information Systems (EIS).  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessment and Authorization Policies and Procedures | CA-1 (DHS-3.18.e) |
| Control: Security Assessment and Authorization Policies and Procedures  All DHS cloud services hosted in a public CSP shall provide documentation to the FedRAMP PMO as required by current FedRAMP CONOPS.  Related control: None.  Referenes: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessments | CA-2 |
| Control: Security Assessments  The organization:  (a) Develops a security assessment plan that describes the scope of the assessment including:  (1) Security controls and control enhancements under assessment; (2) Assessment procedures to be used to determine security control effectiveness; and (3) Assessment environment, assessment team, and assessment roles and responsibilities;  (b) Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;  (c) Produces a security assessment report that documents the results of the assessment; and (d) Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].  Supplemental Guidance  Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.  To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.  Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.  References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessments | CA-2 (1) |
| Control: Security Assessments  The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.  Supplemental Guidance  Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.  Related control: None.  References: FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessments | CA-2 (2) |
| Control: Security Assessments  The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].  Supplemental Guidance  Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of:  (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and, (iii) testing designed to determine exploitability of identified vulnerabilities.  Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions. Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Testing is conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Testing methods are approved by authorizing officials in coordination with the organization's Risk Executive Function. Vulnerabilities uncovered during red team exercises are incorporated into the vulnerability remediation process.  Related controls: PE-3, SI-2.  References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Assessments | CA-2 (DHS-3.18.b) |
| Control: Security Assessments  All DHS cloud services shall be assessed by a Third Party Assessment Organization (3PAO) that has been accredited using a process that follows the conformity assessment approach outlined in ISO/IEC 17020, General Criteria for the operation of various types of bodies performing inspection (1998).  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 |
| Control: Information System Connections  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 [Assignment: organization-defined frequency].  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 federal agencies and nonfederal (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.  References: FIPS Publication 199; NIST Special Publication 800-47. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (5) |
| Control: Information System Connections  The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.  Supplemental Guidance  Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable.  Related control: CM-7.  References: FIPS Publication 199; NIST Special Publication 800-47. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (DHS-5.4.3.b) |
| Control: Information System Connections  Interconnections between DHS and non-DHS systems shall be established only through the Trusted Internet Connection (TIC) and by approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memorandums of understanding, service level agreements or interconnection security agreements.  Related control: CA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (DHS-5.4.3.c) |
| Control: Information System Connections  Components shall document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO and by each appropriate AO. Additional information on ISAs is published in, “Preparation of Interconnection Security Agreements,” Attachment N to the DHS 4300A Sensitive Systems Handbook.  Related control: CA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (DHS-5.4.3.d) |
| Control: Information System Connections  ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.  Related controls: CA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (DHS-5.4.3.f) |
| Control: Information System Connections  Components may complete a master Interconnection Security Agreement (ISA) that includes all transitioning systems as part of their initial OneNet transition. After transition, each additional system or General Support System (GSS) shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, security policies refers to the set of rules that controls a system’s working environment, and not to DHS information security policy). ISAs shall be signed by the appropriate AO.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (DHS-5.4.3.m) |
| Control: Information System Connections  Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as a Service Level Agreement (SLA) or contract, and the risks have been assessed and accepted by all involved AOs.  Related controls: CA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | System Interconnections | CA-3 (DHS-5.4.3.n) |
| Control: Information System Connections  Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Plan of Action and Milestones | CA-5 |
| Control: Plan of Action and Milestones  The organization:  (a) Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and, (b) Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.  Supplemental Guidance  The plan of action and milestones is a key document in the security authorization package and is subject to federal reporting requirements established by OMB.  Related control: CA-2, CA-7, CM-4, PM-4.  References: OMB Memorandum 02-01; NIST Special Publication 800-37. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Plan of Action and Milestones | CA-5 (DHS-2.2.8.d) |
| Control: Plan of Action and Milestones  Program Managers shall ensure that POA&Ms address the following:  - known vulnerabilities in the information system  - the security categorization of the information system  - the specific weaknesses or deficiencies in the information system security controls  - the importance of the identified security control weakness or deficiencies  - the Component’s proposed risk mitigation approach while addressing the identified weaknesses or deficiencies in the security controls the rationale for accepting certain weaknesses or deficiencies in the security controls.  Related control: CA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Authorization | CA-6 |
| Control: Security Authorization  The organization:  (a) Assigns a senior-level executive or manager to the role of 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 [Assignment: organization-defined frequency].  Supplemental Guidance  Security authorization is the official management decision given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system. The organization defines what constitutes a significant change to the information system.  Related controls: CA-2, CA-7, PM-9, PM-10.  References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Security Authorization | CA-6 (DHS-3.9.h) |
| Control: Security Authorization  Components shall authorize systems at initial operating capability and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. An ATO of six (6) months or less shall receive an ATO authorization period waiver from the DHS CISO before submission to the AO for a final authorization decision.  Related controls: CA-6 and PM-10.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Continuous Monitoring | CA-7 |
| Control: Continuous Monitoring  The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:  (a) Establishment of [Assignment: organization-defined metrics] to be monitored; (b) Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: 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 [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].  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.  References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Continuous Monitoring | CA-7 (1) |
| Control: Continuous Monitoring  The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.  Supplemental Guidance  Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.  Related control: None.  References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Continuous Monitoring | CA-7 (DHS-4.6.3.a) |
| Control: Continuous Monitoring  AOs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.  Related control: CM-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Penetration Testing | CA-8 |
| Control: Penetration Testing  The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].  Supplemental Guidance  Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.  Related control: SA-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 5.47 | Internal System Connections | CA-9 |
| Control: Internal System Connections  The organization:  (a) Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and (b) Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.  Supplemental Guidance  This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, printers, copiers, facsimile machines, scanners, and sensors. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.  Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 6.0 Configuration Management (CM)

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Management Policy and Procedures | CM-1 |
| Control: Configuration Management Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (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 [Assignment: organization-defined frequency]; and (2) Configuration management procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 |
| Control: Baseline Configuration  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.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 (1) |
| Control: Baseline Configuration  The organization reviews and updates the baseline configuration of the information system:  (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades.  Supplemental Guidance  None.  Related control: CM-5.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 (2) |
| Control: Baseline Configuration  The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.  Supplemental Guidance  Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities.   Related controls: CM-7, RA-5.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 (3) |
| Control: Baseline Configuration  The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.  Supplemental Guidance  Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.  Related control: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 (7) |
| Control: Baseline Configuration  The organization:  (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and  (b) Applies [Assignment: organization-defined security safeguards] 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.  Related controls: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 (DHS-3.9.b) |
| Control: Baseline Configuration  Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).   Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Baseline Configuration | CM-2 (DHS-4.12.b) |
| Control: Baseline Configuration  Components shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.  Related controls: CM-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Change Control | CM-3 |
| Control: Configuration Change 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 [Assignment: organization-defined time period]; (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 [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions].  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.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Change Control | CM-3 (1) |
| Control: Configuration Change Control  The organization employs automated mechanisms to:  (a) Document proposed changes to the information system; (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.  Supplemental Guidance  None.  Related control: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Change Control | CM-3 (2) |
| Control: Configuration Change Control  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).  Related control: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Change Control | CM-3 (DHS-2.1.8.g) |
| Control: Configuration Change Control  The ISSO shall ensure that timely responses are provided to Infrastructure Change Control Board (ICCB) change request packages.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Change Control | CM-3 (DHS-5.4.3.l) |
| Control: Configuration Change Control  The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.  Related control: CM-3  Referenes: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Security Impact Analysis | CM-4 |
| Control: Security Impact Analysis  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.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Security Impact Analysis | CM-4 (1) |
| Control: Security Impact Analysis  The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.  Supplemental Guidance  Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines).  Related controls: SA-11, SC-3, SC-7.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Access Restrictions for Change | CM-5 |
| Control: Access Restrictions for Change  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Access Restrictions for Change | CM-5 (1) |
| Control: Access Restrictions for Change  The information system enforces access restrictions and supports auditing of the enforcement actions.  Supplemental Guidance  None.  Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Access Restrictions for Change | CM-5 (2) |
| Control: Access Restrictions for Change  The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.  Supplemental Guidance  Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process.  Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Access Restrictions for Change | CM-5 (3) |
| Control: Access Restrictions for Change  The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.  Supplemental Guidance  Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication.  Related controls: CM-7, SC-13, SI-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 |
| Control: Configuration Settings  The organization:  (a) Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] 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 [Assignment: organization-defined information system components] based on [Assignment: organization-defined 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. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.   Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.  References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (1) |
| Control: Configuration Settings  The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].  Supplemental Guidance  None.  Related controls: CA-7, CM-4.  References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (2) |
| Control: Configuration Settings  The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].  Supplemental Guidance  Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing.   Related controls: IR-4, SI-7.  References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-3.7.e) |
| Control: Configuration Settings  Workstations shall be configured in accordance with DHS guidance on the U.S Government Configuration Baseline (USGCB) (formerly known as the Federal Desktop Core Configuration [FDCC]). Configuration shall include installation of the DHS Common Policy Object identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.  Related controls: CM-2, CM-6, and CM-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-3.7.f) |
| Control: Configuration Settings  Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-3.7.g) |
| Control: Configuration Settings  The System Owner shall request an exception for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in DHS Sensitive Systems Handbook, Enclosure 1, DHS Secure Baseline Configuration Guides. Requests shall include a proposed alternative secure configuration.   Related controls: CM-2 and CM-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-4.5.2.b) |
| Control: Configuration Settings  Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.  Related control: AC-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-4.8.4.a) |
| Control: Configuration Settings  Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications promulgated by the DHS CISO. DHS Sensitive Systems Handbook, Enclosure 1, includes the DHS Secure Baseline Configuration Guides.  Related controls: CM-2 and CM-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-4.12.f) |
| Control: Configuration Settings  Components shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.  Related controls: MA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-4.12.j) |
| Control: Configuration Settings  Any multifunction device connected to a DHS network or other information system containing sensitive data shall have the inbound dial in capabilities disabled.  Related controls: AC-17.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-5.4.5.d) |
| Control: Configuration Settings  Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two-factor, encrypted, key exchange) and is approved by the Component shall be used instead.  Related controls: CM-7, SC-7, SC-8, and SC-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Settings | CM-6 (DHS-5.4.5.e) |
| Control: Configuration Settings  File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two-factor, encrypted, key exchange) and is approved by the Component shall be used instead.  Related controls: CM-7, SC-7, SC-8, and SC-9.   References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Least Functionality | CM-7 |
| Control: Least Functionality  The organization:  (a) Configures the information system to provide only essential capabilities; and (b) Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].  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.  References: DoD Instruction 8551.01. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Least Functionality | CM-7 (1) |
| Control: Least Functionality  The organization:  (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].  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.  References: DoD Instruction 8551.01. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Least Functionality | CM-7 (2) |
| Control: Least Functionality  The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].  Supplemental Guidance  None.  Related controls: CM-8, PM-5.  References: DoD Instruction 8551.01. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Least Functionality | CM-7 (5) |
| Control: Least Functionality  The organization:  (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency].  Supplemental Guidance  The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.   Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.  References: DoD Instruction 8551.01. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Least Functionality | CM-7 (DHS-4.8.6.a) |
| Control: Least Functionality  Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive data.  Related controls: CM-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Least Functionality | CM-7 (DHS-5.4.5.f) |
| Control: Least Functionality  Remote Desktop connections, such as Microsoft’s Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange).  Related controls: AC-17 and IA-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Information System Component Inventory | CM-8 |
| Control: Information System Component Inventory  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 [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and  (b) Reviews and updates the information system component inventory [Assignment: organization-defined frequency].  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.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Information System Component Inventory | CM-8 (1) |
| Control: Information System Component Inventory  The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.  Supplemental Guidance  None.  Related control: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Information System Component Inventory | CM-8 (2) |
| Control: Information System Component Inventory  The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.  Supplemental Guidance  Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration activities.  Related control: SI-7.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Information System Component Inventory | CM-8 (3) |
| Control: Information System Component Inventory  The organization:  (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].  Supplemental Guidance  This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.  Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Information System Component Inventory | CM-8 (4) |
| Control: Information System Component Inventory  The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; 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).  Related control: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Information System Component Inventory | CM-8 (5) |
| Control: Information System Component Inventory  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.  Related control: None.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | Configuration Management Plan | CM-9 |
| Control: Configuration Management Plan  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.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | SW Usage Restrictions | CM-10 |
| Control: Software Usage Restrictions  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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 6.47 | User-Installed SW | CM-11 |
| Control: User-Installed Software  The organization:  (a) Establishes [Assignment: organization-defined policies] governing the installation of software by users; (b) Enforces software installation policies through [Assignment: organization-defined methods]; and (c) Monitors policy compliance at [Assignment: 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.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 7.0 Contingency Planning (CP)

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Planning Policy and Procedures | CP-1 |
| Control: Contingency Planning Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: 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 [Assignment: organization-defined frequency]; and (2) Contingency planning procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal 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.  References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Planning Policy and Procedures | CP-1 (DHS-3.5.1.a) |
| Control: Contingency Planning Policy and Procedures  When available, a DHS-wide process for continuity of operations (CO) planning shall be used in order to ensure continuity of operations under all circumstances.  Related control: CP-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Planning Policy and Procedures | CP-1 (DHS-3.5.2.d) |
| Control: Contingency Planning Policy and Procedures  The DHS CIO shall ensure that each DHS system has contingency capabilities commensurate with the availability security objective. The minimum contingency capabilities for each impact level are as follows: High impact – System functions and information have a high priority for recovery after a short period of loss. Moderate impact – System functions and information have a moderate priority for recovery after a moderate period of loss. Low impact – System functions and information have a low priority for recovery after prolonged loss.  Related control: CP-1.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 |
| Control: Contingency Plan  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 [Assignment: organization-defined personnel or roles];  (b) Distributes copies of the contingency plan to [Assignment: 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 [Assignment: organization-defined frequency]; (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 [Assignment: 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.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (1) |
| Control: Contingency Plan  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.  Related control: None.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (2) |
| Control: Contingency Plan  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.  Related control: None.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (3) |
| Control: Contingency Plan  The organization plans for the resumption of essential missions and business functions within [Assignment: 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.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (4) |
| Control: Contingency Plan  The organization plans for the resumption of all missions and business functions within [Assignment: 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.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (5) |
| Control: Contingency Plan  The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.  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. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites).  Related control: PE-12.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (8) |
| Control: Contingency Plan  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.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan | CP-2 (DHS-3.5.2.e) |
| Control: Contingency Plan  CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the availability security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.  Related controls: CP-1 and CP-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Training | CP-3 |
| Control: Contingency Training  The organization provides contingency training to information system users consistent with assigned roles and responsibilities:  (a) Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; (b) When required by information system changes; and (c) [Assignment: organization-defined frequency] 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.  References: NIST Special Publications 800-16, 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Training | CP-3 (1) |
| Control: Contingency Training  The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.  Supplemental Guidance  None.  Related control: None.  References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan Testing | CP-4 |
| Control: Contingency Plan Testing and Exercises  The organization:  (a) Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined 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.  References: FIPS Publication 199; NIST Special Publications 800-34, 800-84. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan Testing | CP-4 (1) |
| Control: Contingency Plan Testing and Exercises  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.  References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan Testing | CP-4 (2) |
| Control: Contingency Plan Testing and Exercises  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.  References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Contingency Plan Testing | CP-4 (DHS-3.5.2.f) |
| Control: Contingency Plan Testing and Exercises  The DHS CIO shall ensure that CP testing is performed in accordance with the availability security objective. The minimum contingency testing for each impact level follows: High impact – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used within a year prior to authorization to recover from a simulated contingency event at the alternate processing site. The system recovery procedures in the CP shall be used at least annually to simulate system recovery in a test facility. Moderate impact – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This is achieved by performing a walk-through/tabletop exercise. Low impact – CP contact information shall be verified at least annually.  Related controls: CP-4 and CP-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Storage Site | CP-6 |
| Control: Alternate Storage Site  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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Storage Site | CP-6 (1) |
| Control: Alternate Storage 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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Storage Site | CP-6 (2) |
| Control: Alternate Storage Site  The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.  Supplemental Guidance  None.  Related control: None.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Storage Site | CP-6 (3) |
| Control: Alternate Storage Site  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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Processing Site | CP-7 |
| Control: Alternate Processing Site  The organization:  (a) Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: 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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Processing Site | CP-7 (1) |
| Control: Alternate Processing 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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Processing Site | CP-7 (2) |
| Control: Alternate Processing Site  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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Processing Site | CP-7 (3) |
| Control: Alternate Processing Site  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.  Related control: None.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Alternate Processing Site | CP-7 (4) |
| Control: Alternate Processing Site  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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Telecommunications Services | CP-8 |
| Control: Telecommunications Services  The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: 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.  References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Telecommunications Services | CP-8 (1) |
| Control: Telecommunications Services  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.   Related controls: None.  References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Telecommunications Services | CP-8 (2) |
| Control: Telecommunications Services  The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.  Supplemental Guidance  None.  Related control: None.  References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Telecommunications Services | CP-8 (3) |
| Control: Telecommunications Services  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.  Related control: None.  References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Telecommunications Services | CP-8 (4) |
| Control: Telecommunications Services  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) Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency].  Supplemental Guidance  Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.  Related control: None.  References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Backup | CP-9 |
| Control: Information System Backup  The organization:  (a) Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; (b) Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; (c) Conducts backups of information system documentation including security-related documentation [Assignment: 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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Backup | CP-9 (1) |
| Control: Information System Backup  The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.  Supplemental Guidance  None.  Related control: CP-4.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Backup | CP-9 (2) |
| Control: Information System Backup  The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.  Supplemental Guidance  None.  Related control: CP-4.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Backup | CP-9 (3) |
| Control: Information System Backup  The organization stores backup copies of [Assignment: organization-defined 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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Backup | CP-9 (5) |
| Control: Information System Backup  The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].  Supplemental Guidance  Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.  Related control: None.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Recovery and Reconstitution | CP-10 |
| Control: Information System Recovery and Reconstitution  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.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Recovery and Reconstitution | CP-10 (2) |
| Control: Information System Recovery and Reconstitution  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.  Related control: None.  References: Federal Continuity Directive 1; NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 7.47 | Information System Recovery and Reconstitution | CP-10 (4) |
| Control: Information System Recovery and Reconstitution  The organization provides the capability to restore information system components within [Assignment: 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.  References: NIST Special Publication 800-34. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 8.0 Identification and Authentication (IA)

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication Policy and Procedures | IA-1 |
| Control: Identification and Authentication Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (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 [Assignment: organization-defined frequency]; and (2) Identification and authentication procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal 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.  References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication Policy and Procedures | IA-1 (DHS-1.6.d) |
| Control: Identification and Authentication Policy and Procedures  Components shall accept and be able to verify Personal Identity Verification (PIV) credentials issued by other Federal agencies as proof of identity.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication Policy and Procedures | IA-1 (DHS-3.14.7.a) |
| Control: Identification and Authentication Policy and Procedures  For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.  Related controls: IA-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication Policy and Procedures | IA-1 (DHS-3.14.7.c) |
| Control: Identification and Authentication Policy and Procedures  Components shall implement the technical requirements described in NIST SP 800-63, Electronic Authentication Guideline, at the appropriate assurance level for those systems with e-authentication requirements.  Related controls: IA-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication Policy and Procedures | IA-1 (DHS-3.14.7.f) |
| Control: Identification and Authentication Policy and Procedures  Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 |
| Control: Identification and Authentication (Organizational Users)  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. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.  Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.  Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (1) |
| Control: Identification and Authentication (Organizational Users)  The information system implements multifactor authentication for network access to privileged accounts.  Supplemental Guidance  None.  Related control: AC-6.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (2) |
| Control: Identification and Authentication (Organizational Users)  The information system implements multifactor authentication for network access to non-privileged accounts.  Supplemental Guidance  None.  Related control: None.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (3) |
| Control: Identification and Authentication (Organizational Users)  The information system implements multifactor authentication for local access to privileged accounts.  Supplemental Guidance  None.  Related control: AC-6.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (4) |
| Control: Identification and Authentication (Organizational Users)  The information system implements multifactor authentication for local access to non-privileged accounts.  Supplemental Guidance  None.  Related control: None.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (8) |
| Control: Identification and Authentication (Organizational Users)  The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.  Supplemental Guidance  Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.  Related control: None.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (9) |
| Control: Identification and Authentication (Organizational Users)  The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.  Supplemental Guidance  Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.  Related control: None.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (11) |
| Control: Identification and Authentication (Organizational Users)  The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].  Supplemental Guidance  For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users.  Related control: AC-6.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (12) |
| Control: Identification and Authentication (Organizational Users)  The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.  Supplemental Guidance  This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.  Related controls: AU-2, PE-3, SA-4.  References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Organizational Users) | IA-2 (DHS-5.1.d) |
| Control: Identification and Authentication (Organizational Users)  Department of Homeland Security (DHS) users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user’s identity.  Related control: IA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Device Identification and Authentication | IA-3 |
| Control: Device Identification and Authentication  The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.  Supplemental Guidance  Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability.  Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identifier Management | IA-4 |
| Control: Identifier Management  The organization manages information system identifiers by:  (a) Receiving authorization from [Assignment: organization-defined personnel or roles] 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 [Assignment: organization-defined time period]; and (e) Disabling the identifier after [Assignment: organization-defined time period 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.  References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Management | IA-5 |
| Control: Authenticator Management  The organization manages information system authenticators by:  (a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; (b) Establishing initial authenticator content for authenticators defined by the organization; (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; (d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; (e) Changing default content of authenticators prior to information system installation; (f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; (g) Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; (h) Protecting authenticator content from unauthorized disclosure and modification; (i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and (j) Changing authenticators for group/role accounts when membership to those accounts changes.  Supplemental Guidance  Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.  Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.  References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Management | IA-5 (1) |
| Control: Authenticator Management  The information system, for password-based authentication:  (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (c) Stores and transmits only encrypted representations of passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [Assignment: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.  Supplemental Guidance  This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords.  Related control: IA-6.  References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Management | IA-5 (2) |
| Control: Authenticator Management  The information system, for PKI-based authentication:  (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.  Supplemental Guidance  Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing.  Related control: IA-6.  References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Management | IA-5 (3) |
| Control: Authenticator Management  The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].  Supplemental Guidance  None.  Related control: None.  References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Management | IA-5 (11) |
| Control: Authenticator Management  The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].  Supplemental Guidance  Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.  Related control: None.  References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Management | IA-5 (DHS-5.1.e) |
| Control: Authenticator Management  All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.  Related control: IA-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Authenticator Feedback | IA-6 |
| Control: Authenticator Feedback  The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.  Supplemental Guidance  The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.  Related control: PE-18.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Cryptographic Module Authentication | IA-7 |
| Control: Cryptographic Module Authentication  The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.  Supplemental Guidance  Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.  Related controls: SC-12, SC-13.  References: FIPS Publication 140; Web: csrc.nist.gov/groups/STM/cmvp/index.html | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Non-Organizational Users) | IA-8 |
| Control: Identification and Authentication (Non-Organizational Users)  The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).  Supplemental Guidance  Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users.  Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.  References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) |
| Control: Identification and Authentication (Non-Organizational Users)  The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.  Supplemental Guidance  This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.  Related controls: AU-2, PE-3, SA-4.  References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Non-Organizational Users) | IA-8 (2) |
| Control: Identification and Authentication (Non-Organizational Users)  The information system accepts only FICAM-approved third-party credentials.  Supplemental Guidance  This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.  Related control: AU-2.  References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Non-Organizational Users) | IA-8 (3) |
| Control: Identification and Authentication (Non-Organizational Users)  The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.  Supplemental Guidance  This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program.  Related control: SA-4.  References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Non-Organizational Users) | IA-8 (4) |
| Control: Identification and Authentication (Non-Organizational Users)  The information system conforms to FICAM-issued profiles.  Supplemental Guidance  This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).  Related control: SA-4.  References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 8.47 | Identification and Authentication (Non-Organizational Users) | IA-8 (DHS-1.5.4.c) |
| Control: Identification and Authentication (Non-Organizational Users)  Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO.  Related control: PS-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 9.0 Incident Response (IR)

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Policy and Procedures | IR-1 |
| Control: Incident Response Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and  (b) Reviews and updates the current:  (1) Incident response policy [Assignment: organization-defined frequency]; and (2) Incident response procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-61, 800-83, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Training | IR-2 |
| Control: Incident Response Training  The organization provides incident response training to information system users consistent with assigned roles and responsibilities:  (a) Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; (b) When required by information system changes; and (c) [Assignment: organization-defined frequency] thereafter.  Supplemental Guidance  Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.  Related controls: AT-3, CP-3, IR-8.  References: NIST Special Publications 800-16, 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Training | IR-2 (1) |
| Control: Incident Response Training  The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.  Supplemental Guidance  None.  Related control: None.  References: NIST Special Publications 800-16, 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Training | IR-2 (2) |
| Control: Incident Response Training  The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.  Supplemental Guidance  None.  Related control: None.  References: NIST Special Publications 800-16, 800-50. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Testing | IR-3 |
| Control: Incident Response Testing and Exercises  The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.  Supplemental Guidance  Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.  Related controls: CP-4, IR-8.  References: NIST Special Publications 800-84, 800-115. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Testing | IR-3 (2) |
| Control: Incident Response Testing and Exercises  The organization coordinates incident response testing with organizational elements responsible for related plans.  Supplemental Guidance  Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.  Related control: None.  References: NIST Special Publications 800-84, 800-115. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Handling | IR-4 |
| Control: Incident Handling  The organization:  (a) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; (b) Coordinates incident handling activities with contingency planning activities; and (c) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.  Supplemental Guidance  Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).  Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.  References: Executive Order 13587; NIST Special Publication 800-61. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Handling | IR-4 (1) |
| Control: Incident Handling  The organization employs automated mechanisms to support the incident handling process.  Supplemental Guidance  Automated mechanisms supporting incident handling processes include, for example, online incident management systems.  Related control: None.  References: Executive Order 13587; NIST Special Publication 800-61. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Handling | IR-4 (4) |
| Control: Incident Handling  The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.  Supplemental Guidance  Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.  Related control: None.  References: Executive Order 13587; NIST Special Publication 800-61. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Monitoring | IR-5 |
| Control: Incident Monitoring  The organization tracks and documents information system security incidents.  Supplemental Guidance  Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.  Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.  References: NIST Special Publication 800-61. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Monitoring | IR-5 (1) |
| Control: Incident Monitoring  The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.  Supplemental Guidance  Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents.  Related controls: AU-7, IR-4.  References: NIST Special Publication 800-61. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Reporting | IR-6 |
| Control: Incident Reporting  The organization:  (a) Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and (b) Reports security incident information to [Assignment: organization-defined authorities].  Supplemental Guidance  The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.  Related controls: IR-4, IR-5, IR-8.  References: NIST Special Publication 800-61: Web: www.us-cert.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Reporting | IR-6 (1) |
| Control: Incident Reporting  The organization employs automated mechanisms to assist in the reporting of security incidents.  Supplemental Guidance  None.  Related control: IR-7.  References: NIST Special Publication 800-61: Web: www.us-cert.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Assistance | IR-7 |
| Control: Incident Response Assistance  The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.  Supplemental Guidance  Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.  Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Assistance | IR-7 (1) |
| Control: Incident Response Assistance  The organization employs automated mechanisms to increase the availability of incident response-related information and support.  Supplemental Guidance  Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 9.47 | Incident Response Plan | IR-8 |
| Control: Incident Response Plan  The organization: (a) Develops an incident response plan that:  (1) Provides the organization with a roadmap for implementing its incident response capability; (2) Describes the structure and organization of the incident response capability; (3) Provides a high-level approach for how the incident response capability fits into the overall organization; (4) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; (5) Defines reportable incidents; (6) Provides metrics for measuring the incident response capability within the organization; (7) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and (8) Is reviewed and approved by [Assignment: organization-defined personnel or roles];  (b) Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; (c) Reviews the incident response plan [Assignment: organization-defined frequency]; (d) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; (e) Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and (f) Protects the incident response plan from unauthorized disclosure and modification.  Supplemental Guidance  It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.  Related controls: MP-2, MP-4, MP-5.  References: NIST Special Publication 800-61. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 10.0 Maintenance (MA)

|  |  |  |
| --- | --- | --- |
| 10.47 | System Maintenance Policy and Procedures | MA-1 |
| Control: System Maintenance Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and  (b) Reviews and updates the current:  (1) System maintenance policy [Assignment: organization-defined frequency]; and (2) System maintenance procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Controlled Maintenance | MA-2 |
| Control: Controlled Maintenance  The organization:  (a) Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; (e) Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and (f) Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.  Supplemental Guidance  This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.  Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Controlled Maintenance | MA-2 (2) |
| Control: Controlled Maintenance  The organization:  (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.  Supplemental Guidance  None.  Related controls: CA-7, MA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Maintenance Tools | MA-3 |
| Control: Maintenance Tools  The organization approves, controls, and monitors information system maintenance tools.  Supplemental Guidance  This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch.  Related controls: MA-2, MA-5, MP-6.  References: NIST Special Publication 800-88. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Maintenance Tools | MA-3 (1) |
| Control: Maintenance Tools  The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.  Supplemental Guidance  If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.  Related control: SI-7.  References: NIST Special Publication 800-88. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Maintenance Tools | MA-3 (2) |
| Control: Maintenance Tools  The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.  Supplemental Guidance  If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.  Related control: SI-3.  References: NIST Special Publication 800-88. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Maintenance Tools | MA-3 (3) |
| Control: Maintenance Tools  The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:  (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.  Supplemental Guidance  Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.  Related control: None.  References: NIST Special Publication 800-88. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Nonlocal Maintenance | MA-4 |
| Control: Non-Local Maintenance  The organization:  (a) Approves and monitors nonlocal maintenance and diagnostic activities; (b) Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; (c) Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; (d) Maintains records for nonlocal maintenance and diagnostic activities; and (e) Terminates session and network connections when nonlocal maintenance is completed.  Supplemental Guidance  Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.  Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.  References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Nonlocal Maintenance | MA-4 (2) |
| Control: Non-Local Maintenance  The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.  Supplemental Guidance  None.  Related control: None.  References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Nonlocal Maintenance | MA-4 (3) |
| Control: Non-Local Maintenance  The organization:  (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or  (b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.  Supplemental Guidance  Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.   Related controls: MA-3, SA-12, SI-3, SI-7.  References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Nonlocal Maintenance | MA-4 (DHS-5.4.4.c) |
| Control: Non-Local Maintenance  Components shall encrypt remote maintenance paths to the firewalls and PEPs.   Related controls: MA-4 and SC-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Maintenance Personnel | MA-5 |
| Control: Maintenance Personnel  The organization:  (a) Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; (b) Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and (c) Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.  Supplemental Guidance  This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.  Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Maintenance Personnel | MA-5 (1) |
| Control: Maintenance Personnel  The organization:  (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:  (1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;  (2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and  (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.  Supplemental Guidance  This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems.  Related controls: MP-6, PL-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 10.47 | Timely Maintenance | MA-6 |
| Control: Timely Maintenance  The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.  Supplemental Guidance  Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.  Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 11.0 Media Protection (MP)

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Protection Policy and Procedures | MP-1 |
| Control: Media Protection Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and  (b) Reviews and updates the current:  (1) Media protection policy [Assignment: organization-defined frequency]; and (2) Media protection procedures [Assignment: organization-defined frequency].  Supplemental Guidance   This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Protection Policy and Procedures | MP-1 (DHS-3.14.5.b) |
| Control: Media Protection Policy and Procedures  If PII and Sensitive PII can be physically removed from an information system (e.g., printouts, CDs), the Security Plan (SP) shall document the specific procedures, training, and accountability measures in place to ensure that remote use of the data does not bypass the protections provided by the encryption.  Related controls: MP-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Protection Policy and Procedures | MP-1 (DHS-4.3.1.g) |
| Control: Media Protection Policy and Procedures  Users shall ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.  Related Control: SI-12.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Protection Policy and Procedures | MP-1 (DHS-5.4.1.d) |
| Control: Media Protection Policy and Procedures  Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the Security Plan.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Protection Policy and Procedures | MP-1 (DHS-5.6.c) |
| Control: Media Protection Policy and Procedures  System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.  Related controls: AC-20 and SI-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Access | MP-2 |
| Control: Media Access  The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals].  Supplemental Guidance  Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.   Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.  References: FIPS Publication 199; NIST Special Publication 800-111. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Marking | MP-3 |
| Control: Media Marking  The organization:  (a) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and (b) Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].  Supplemental Guidance  The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.  Related controls: AC-16, PL-2, RA-3.  References: FIPS Publication 199. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Storage | MP-4 |
| Control: Media Storage  The organization:  (a) Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and (b) Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.  Supplemental Guidance  Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.   Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.  References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Protection Policy and Procedures | MP-4 (DHS-3.14.5.f) |
| Control: Media Storage  Ad hoc CREs shall be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Transport | MP-5 |
| Control: Media Transport  The organization:  (a) Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards]; (b) Maintains accountability for information system media during transport outside of controlled areas; (c) Documents activities associated with the transport of information system media; and (d) Restricts the activities associated with the transport of information system media to authorized personnel.  Supplemental Guidance  Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.  Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.  Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.  References: FIPS Publication 199; NIST Special Publication 800-60. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Transport | MP-5 (4) |
| Control: Media Transport  The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.  Supplemental Guidance   This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers).   Related control: MP-2.  References: FIPS Publication 199; NIST Special Publication 800-60. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Transport | MP-5 (DHS-4.11.f) |
| Control: Media Transport  Backup media shall be shipped using an accountable delivery service (e.g. U.S. Postal Service First Class Mail, Federal Express, United Parcel Service) and shall be properly inventoried.  Related Controls: CP-9 and MP-5.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Sanitization | MP-6 |
| Control: Media Sanitization  The organization:  (a) Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and (b) Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.  Supplemental Guidance  This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.  Related controls: MA-2, MA-4, RA-3, SC-4.  References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation\_guidance/media\_destruction\_guidance/index.shtml. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Sanitization | MP-6 (1) |
| Control: Media Sanitization  The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.  Supplemental Guidance  Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal.   Related control: SI-12.  References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation\_guidance/media\_destruction\_guidance/index.shtml. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Sanitization | MP-6 (2) |
| Control: Media Sanitization  The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.  Supplemental Guidance  Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).  Related control: None.  References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation\_guidance/media\_destruction\_guidance/index.shtml. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Sanitization | MP-6 (3) |
| Control: Media Sanitization  The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].  Supplemental Guidance  This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices.   Related control: SI-3  References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation\_guidance/media\_destruction\_guidance/index.shtml. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Use | MP-7 |
| Control: Media Use  The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].  Supplemental Guidance  Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.   Related controls: AC-19, PL-4.  References: FIPS Publication 199; NIST Special Publication 800-111. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Use | MP-7 (1) |
| Control: Prohibit Use Without Owner  The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.  Supplemental Guidance  Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).   Related control: PL-4.  References: FIPS Publication 199; NIST Special Publication 800-111. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Use | MP-7 (DHS-4.3.1.d) |
| Control: USB Drive encryption  All USB drives shall use encryption in compliance with Section 5.5.1 of this Policy Directive.  Related Controls: IA-7 and SC-13.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Use | MP-7 (DHS-4.3.1.e) |
| Control: DHS owned Removable Media  DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). (The respective CISO is the CISO with that system in his or her inventory.)  Related Controls: AC-20, MP-2, and PM-9.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 11.47 | Media Use | MP-7 (DHS-4.3.1.f) |
| Control: Protection of Sensitive Paper and Electronic Outputs  Components shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.  Related Control: MP-1.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 12.0 Physical and Environmental Protection (PE)

|  |  |  |
| --- | --- | --- |
| 12.47 | Physical and Environmental Protection Policy and Procedures | PE-1 |
| Control: Physical and Environmental Protection Policy and Procedures  The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and  b. Reviews and updates the current:  1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Physical and Environmental Protection Policy and Procedures | PE-1 (DHS-3.3.c) |
| Control: Physical and Environmental Protection Policy and Procedures  Requirements shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background investigations and clearances, and facility security.  Related Control: SA-9.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Physical and Environmental Protection Policy and Procedures | PE-1 (DHS-4.6.2.3.b) |
| Control: Physical and Environmental Protection Policy and Procedures  Functions that transmit or receive video, infrared (IR), or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed.   Related controls: AC-19 and PE-18.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Physical Access Authorizations | PE-2 |
| Control: Physical Access Authorizations  The organization:  a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required.  Supplemental Guidance  This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.   Related controls: PE-3, PE-4, PS-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Physical Access Control | PE-3 |
| Control: Physical Access Control  The organization:  (a) Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by;  (1) Verifying individual access authorizations before granting access to the facility; and (2) Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards];  (b) Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; (c) Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; (d) Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; (e) Secures keys, combinations, and other physical access devices; (f) Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and (g) Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.  Supplemental Guidance  This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.   Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.  References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Physical Access Control | PE-3 (1) |
| Control: Physical Access Control  The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the information system].  Supplemental Guidance  This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers).   Related control: PS-2.  References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Access Control for Transmission Medium | PE-4 |
| Control: Access Control for Transmission Medium  The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].  Supplemental Guidance  Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.  Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.  References: NSTISSI No. 7003. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Access Control for Output Devices | PE-5 |
| Control: Access Control for Output Devices  The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.  Supplemental Guidance  Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, and audio devices are examples of information system output devices.   Related controls: PE-2, PE-3, PE-4, PE-18.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Monitoring Physical Access | PE-6 |
| Control: Monitoring Physical Access  The organization:  a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;  b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and  c. Coordinates results of reviews and investigations with the organizational incident response capability.  Supplemental Guidance:   Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.  Related controls: CA-7, IR-4, IR-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Monitoring Physical Access | PE-6 (1) |
| Control: Monitoring Physical Access  The organization monitors physical intrusion alarms and surveillance equipment.  Supplemental Guidance  None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Monitoring Physical Access | PE-6 (4) |
| Control: Monitoring Physical Access  The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system].  Supplemental Guidance  This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers).  Related controls: PS-2, PS-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Visitor Access Records | PE-8 |
| Control: Access Records  The organization:  a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency].  Supplemental Guidance:   Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Visitor Access Records | PE-8 (1) |
| Control: Access Records  The organization employs automated mechanisms to facilitate the maintenance and review of access visitor records.  Supplemental Guidance  None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Power Equipment and Cabling | PE-9 |
| Control: Power Equipment and Power Cabling  The organization protects power equipment and power cabling for the information system from damage and destruction.  Supplemental Guidance  Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.   Related control: PE-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Emergency Shutoff | PE-10 |
| Control: Emergency Shutoff  The organization:  a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;  b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and,  c. Protects emergency power shutoff capability from unauthorized activation.  Supplemental Guidance  This control applies to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.  Related control: PE-15.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Emergency Power | PE-11 |
| Control: Emergency Power  The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.   Supplemental Guidance  None.  Related controls: AT-3, CP-2, CP-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Emergency Power | PE-11 (1) |
| Control: Emergency Power  The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.  Supplemental Guidance  This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.  Related Controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Emergency Lighting | PE-12 |
| Control: Emergency Lighting  The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.  Supplemental Guidance  This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.   Related controls: CP-2, CP-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Fire Protection | PE-13 |
| Control: Fire Protection  The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.  Supplemental Guidance  This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.  Related Controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Fire Protection | PE-13 (1) |
| Control: Fire Protection  The organization employs fire detection devices/systems for the information system that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.  Supplemental Guidance:   Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.  Related Controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Fire Protection | PE-13 (2) |
| Control: Fire Protection  The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].  Supplemental Guidance  Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.  Related Controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Fire Protection | PE-13 (3) |
| Control: Fire Protection  The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.  Supplemental Guidance  None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Temperature and Humidity Controls | PE-14 |
| Control: Temperature and Humidity Controls  The organization:  (a) Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and, (b) Monitors temperature and humidity levels [Assignment: organization-defined frequency].  Supplemental Guidance  This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.   Related control: AT-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Water Damage Protection | PE-15 |
| Control: Water Damage Protection  The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.  Supplemental Guidance  This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.   Related control: AT-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Water Damage Protection | PE-15 (1) |
| Control: Water Damage Protection  The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [Assignment: organization-defined personnel or roles].  Supplemental Guidance  Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.  Related Controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Delivery and Removal | PE-16 |
| Control: Delivery and Removal  The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.  Supplemental Guidance  Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.  Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Alternate Work Site | PE-17 |
| Control: Alternate Work Site  The organization:  (a) Employs [Assignment: organization-defined security controls] at alternate work sites; (b) Assesses as feasible, the effectiveness of security controls at alternate work sites; and, (c) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.  Supplemental Guidance  Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative.   Related controls: AC-17, CP-7.  References: NIST Special Publication 800-46. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 12.47 | Location of Information System Components | PE-18 |
| Control: Location of Information System Components  The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.  Supplemental Guidance  Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).   Related controls: CP-2, PE-19, RA-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 13.0 Planning (PL)

|  |  |  |
| --- | --- | --- |
| 13.47 | Security Planning Policy and Procedures | PL-1 |
| Control: Security Planning Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and  (b) Reviews and updates the current:  (1) Security planning policy [Assignment: organization-defined frequency]; and (2) Security planning procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-18, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Security Planning Policy and Procedures | PL-1 (DHS-3.14.5.c) |
| Control: Security Planning Policy and Procedures  Systems that, as part of routine business, remove Sensitive PII in the form of a CRE, e.g., routine system-to-system transmissions of data (routine CREs) shall address associated risks in the Security Plan.   Related controls: MP-5.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Security Planning Policy and Procedures | PL-1 (DHS-3.14.7.d) |
| Control: Security Planning Policy and Procedures  Components shall ensure that each Security Plan reflects the e-authentication status of the respective system.   Related control: IA-2 and PL-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | System Security Plan | PL-2 |
| Control: System Security Plan  The organization:  (a) Develops a security plan for the information system that:  (1) Is consistent with the organization’s enterprise architecture; (2) Explicitly defines the authorization boundary for the system; (3) Describes the operational context of the information system in terms of missions and business processes; (4) Provides the security categorization of the information system including supporting rationale; (5) Describes the operational environment for the information system and relationships with or connections to other information systems; (6) Provides an overview of the security requirements for the system; (7) Identifies any relevant overlays, if applicable;  (8) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and (9) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;  (b) Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; (c) Reviews the security plan for the information system [Assignment: organization-defined frequency];  (d) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and (e) Protects the security plan from unauthorized disclosure and modification.  Supplemental Guidance  Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.  Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.  Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.  References: NIST Special Publication 800-18. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | System Security Plan | PL-2 (3) |
| Control: System Security Plan  The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.  Supplemental Guidance  Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.   Related controls: CP-4, IR-4.  References: NIST Special Publication 800-18. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 |
| Control: Rules of Behavior  The organization:  (a) Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; (b) Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; (c) Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and (d) Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.  Supplemental Guidance  This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior.   Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.  References: NIST Publication 800-18. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 (1) |
| Control: Rules of Behavior  The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting information on commercial websites.  Supplemental Guidance  This control enhancement addresses rules of behavior related to the use of social media/networking sites:   (i) when organizational personnel are using such sites for official duties or in the conduct of official business;   (ii) when organizational information is involved in social media/networking transactions; and   (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent the ability to obtain, or infer, non-public organizational information from social media/networking sites (e.g., system account information, personally identifiable information).  Related Controls: None.  References: NIST Publication 800-18. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 (DHS-4.1.2.a) |
| Control: Rules of Behavior  Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a “Consent to Monitor” provision) and that disciplinary actions may result from violations.   Related controls: PL-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 (DHS-4.8.2.a) |
| Control: Rules of Behavior  Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption, for data at rest and in motion. Passwords, tokens and Smart Cards shall not be stored on or with the laptop or other mobile computing device.   Related controls: AC-19, IA-2, and SC-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 (DHS-4.8.2.b) |
| Control: Rules of Behavior  Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities).   Related controls: AC-19 and PL-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 (DHS-4.8.3.a) |
| Control: Rules of Behavior  Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.   Related controls: SA-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Rules of Behavior | PL-4 (DHS-4.8.5.e) |
| Control: Rules of Behavior  DHS users are required to sign rules of behavior prior to being granted system accounts or access to DHS systems or data. The rules of behavior shall contain a “Consent to Monitor” provision and an acknowledgement that the user has no expectation of privacy.   Related control: PL-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 13.47 | Information Security Architecture | PL-8 |
| Control: Information Security Architecture  The organization:  (a) Develops an information security architecture for the information system that:  (1) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; (2) Describes how the information security architecture is integrated into and supports the enterprise architecture; and (3) Describes any information security assumptions about, and dependencies on, external services;  (b) Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and (c) Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.  Supplemental Guidance  This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.  In today’s modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization’s enterprise architecture and information security architecture.  Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 14.0 Personnel Security (PS)

|  |  |  |
| --- | --- | --- |
| 14.47 | Personnel Security Policy and Procedures | PS-1 |
| Control: Personnel Security Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and  (b) Reviews and updates the current:  (1) Personnel security policy [Assignment: organization-defined frequency]; and (2) Personnel security procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Position Risk Designation | PS-2 |
| Control: Position Categorization  The organization:  (a) Assigns a risk designation to all organizational positions; (b) Establishes screening criteria for individuals filling those positions; and (c) Reviews and updates position risk designations [Assignment: organization-defined frequency].  Supplemental Guidance  Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).  Related control: AT-3, PL-2, PS-3.  References: 5 CFR 731.106(a). | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Personnel Screening | PS-3 |
| Control: Personnel Screening  The organization:  (a) Screens individuals prior to authorizing access to the information system; and, (b) Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].  Supplemental Guidance  Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.  Related control: AC-2, IA-4, PE-2, PS-2.  References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Personnel Termination | PS-4 |
| Control: Personnel Termination  The organization, upon termination of individual employment:  (a) Disables information system access within [Assignment: organization-defined time period]; (b) Terminates/revokes any authenticators/credentials associated with the individual; (c) Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; (d) Retrieves all security-related organizational information system-related property; (e) Retains access to organizational information and information systems formerly controlled by terminated individual; and (f) Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].  Supplemental Guidance  Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.  Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Personnel Termination | PS-4 (2) |
| Control: Automated Notification  The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual.  Supplemental Guidance  In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.  Related Controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Personnel Transfer | PS-5 |
| Control: Personnel Transfer  The organization:   (a) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; (b) Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; (c) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and (d) Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].  Supplemental Guidance  This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.  Related controls: AC-2, IA-4, PE-2, PS-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Access Agreements | PS-6 |
| Control: Access Agreements  The organization:  (a) Develops and documents access agreements for organizational information systems; (b) Reviews and updates the access agreements [Assignment: organization-defined frequency]; and (c) Ensures that individuals requiring access to organizational information and information systems:   (1) Sign appropriate access agreements prior to being granted access; and (2) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].  Supplemental Guidance:   Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.   Related control: PL-4, PS-2, PS-3, PS-4, PS-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Third-Party Personnel Security | PS-7 |
| Control: Third-Party Personnel Security  The organization:  (a) Establishes personnel security requirements including security roles and responsibilities for third-party providers; (b) Requires third-party providers to comply with personnel security policies and procedures established by the organization; (c) Documents personnel security requirements; (d) Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and (e) Monitors provider compliance.  Supplemental Guidance  Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.   Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.  References: NIST Special Publication 800-35. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 14.47 | Personnel Sanctions | PS-8 |
| Control: Personnel Sanctions  The organization:  (a) Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and (b) Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.  Supplemental Guidance  Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.  Related controls: PL-4, PS-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 15.0 Risk Assessment (RA)

|  |  |  |
| --- | --- | --- |
| 15.47 | Risk Assessment Policy and Procedures | RA-1 |
| Control: Risk Assessment Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and  (b) Reviews and updates the current:  (1) Risk assessment policy [Assignment: organization-defined frequency]; and (2) Risk assessment procedures [Assignment: organization-defined frequency].  Supplemental Guidance:   This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-30,800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Security Categorization | RA-2 |
| Control: Security Categorization  The organization:  (a) Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; (b) Documents the security categorization results (including supporting rationale) in the security plan for the information system; and (c) Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.  Supplemental Guidance  Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.   Related controls: CM-8, MP-4, RA-3, SC-7.  References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Security Categorization | RA-2 (DHS-3.9.a) |
| Control: Security Categorization  Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 controls as tailored specifically to the security objective at the determined impact level in the Attachment M to DHS 4300A, Sensitive Systems Handbook, “Tailoring the NIST 800-53 Security Controls.”   Related controls: PM-10 and RA-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Security Categorization | RA-2 (DHS-3.14.2.e) |
| Control: Security Categorization  For Privacy Sensitive Systems, the confidentiality security objective shall be assigned an impact level of moderate or higher.   Related controls: RA-2.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Risk Assessment | RA-3 |
| Control: Risk Assessment  The organization:  (a) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; (b) Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; (c) Reviews risk assessment results [Assignment: organization-defined frequency]; (d) Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and (e) Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.  Supplemental Guidance  Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.  Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.   Related controls: RA-2, PM-9.  References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: idmanagement.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Vulnerability Scanning | RA-5 |
| Control: Vulnerability Scanning  The organization:  (a) Scans for vulnerabilities in the information system and hosted applications [Assignment:organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; (b) Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:  - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and, - Measuring vulnerability impact;  (c) Analyzes vulnerability scan reports and results from security control assessments; (d) Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and, (e) Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).  Supplemental Guidance  Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example:  (i) scanning for patch levels;  (ii) scanning for functions, ports, protocols, and services that should  not be accessible to users or devices; and  (iii) scanning for improperly configured or incorrectly  operating information flow control mechanisms.   Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).   Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.  References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org, nvd.nist.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Vulnerability Scanning | RA-5 (1) |
| Control: Vulnerability Scanning  The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.  Supplemental Guidance  The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.   Related controls: SI-3, SI-7.  References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org, nvd.nist.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Vulnerability Scanning | RA-5 (2) |
| Control: Vulnerability Scanning  The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].  Supplemental Guidance  None.  Related control: SI-3, SI-5.  References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org, nvd.nist.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Vulnerability Scanning | RA-5 (4) |
| Control: Vulnerability Scanning  The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined corrective actions].  Supplemental Guidance  Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries.  Related control: AU-13.  References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org, nvd.nist.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Vulnerability Scanning | RA-5 (5) |
| Control: Vulnerability Scanning  The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities].  Supplemental Guidance  In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.  Related control: None.  References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org, nvd.nist.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 15.47 | Vulnerability Scanning | RA-5 (DHS-4.8.4.d) |
| Control: Vulnerability Scanning  Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.   Related controls: CM-3 and RA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 16.0 System and Services Acquisition (SA)

|  |  |  |
| --- | --- | --- |
| 16.47 | System and Services Acquisition Policy and Procedures | SA-1 |
| Control: System and Services Acquisition Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and  (b) Reviews and updates the current:  (1) System and services acquisition policy [Assignment: organization-defined frequency]; and (2) System and services acquisition procedures [Assignment: organization-defined frequency].  Supplemental Guidance:   This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | System and Services Acquisition Policy and Procedures | SA-1 (DHS-3.1.g) |
| Control: System and Services Acquisition Policy and Procedures  Component CISOs/ISSMs shall ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference model (TRM) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/CISO.   Related controls: PL-1 and PM-1.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | System and Services Acquisition Policy and Procedures | SA-1 (DHS-3.2.g) |
| Control: System and Services Acquisition Policy and Procedures  Procurements for services and products involving facility or system access control shall be in accordance with DHS guidance regarding HSPD-12 implementation.  Related Control: None.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | System and Services Acquisition Policy and Procedures | SA-1 (DHS-3.3.a) |
| Control: System and Services Acquisition Policy and Procedures  All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.  Related Control: SA-4.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | System and Services Acquisition Policy and Procedures | SA-1 (DHS-3.3.b) |
| Control: System and Services Acquisition Policy and Procedures  Contractor information system services and operations shall adhere to all applicable DHS information security policies.  Related Control: SA-9.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Allocation of Resources | SA-2 |
| Control: Allocation of Resources  The organization:  (a) Determines information security requirements for the information system or information system service in mission/business process planning; (b) Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and (c) Establishes a discrete line item for information security in organizational programming and budgeting documentation.  Supplemental Guidance  Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.   Related controls: PM-3, PM-11.  References: NIST Special Publication 800-65. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | System Development Life Cycle | SA-3 |
| Control: Life Cycle Support  The organization:  (a) Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; (b) Defines and documents information security roles and responsibilities throughout the system development life cycle; (c) Identifies individuals having information security roles and responsibilities; and (d) Integrates the organizational information security risk management process into system development life cycle activities.  Supplemental Guidance  A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.  Related controls: AT-3, PM-7, SA-8.  References: NIST Special Publications 800-37, 800-64. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | System Development Life Cycle | SA-3 (DHS-3.6.c) |
| Control: Life Cycle Support  The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority to another DHS employee in writing. This authority shall not be delegated to contractor personnel.   Related control: RA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 |
| Control: Acquisitions  The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:   (a) Security functional requirements; (b) Security strength requirements; (c) Security assurance requirements; (d) Security-related documentation requirements; (e) Requirements for protecting security-related documentation; (f) Description of the information system development environment and environment in which the system is intended to operate; and (g) Acceptance criteria.  Supplemental Guidance  Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include:   (i) development processes, procedures, practices, and methodologies; and   (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.   Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.  Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.  References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 (1) |
| Control: Acquisitions  The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.  Supplemental Guidance  Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.  Related control: SA-5.  References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 (2) |
| Control: Acquisitions  The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].  Supplemental Guidance  Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system.   Related control: SA-5.  References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 (9) |
| Control: Acquisitions  The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.  Supplemental Guidance  The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.   Related controls: CM-7, SA-9.  References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 (10) |
| Control: Acquisitions  The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.  Supplemental Guidance  None.  Related controls: IA-2; IA-8.  References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 (DHS-3.14.7.g) |
| Control: Acquisitions  All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.   Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Acquisition Process | SA-4 (DHS-5.7.b) |
| Control: Acquisitions  Strong preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following:   - The NIST FIPS validation program  - The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program  - The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement   Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Information System Documentation | SA-5 |
| Control: Information System Documentation  The organization:  (a) Obtains administrator documentation for the information system, system component, or information system service that describes:  (1) Secure configuration, installation, and operation of the system, component, or service;  (2) Effective use and maintenance of security functions/mechanisms; and (3) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;  (b) Obtains user documentation for the information system, system component, or information system service that describes:   (1) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; (2) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and (3) User responsibilities in maintaining the security of the system, component, or service;  (c) Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response; (d) Protects documentation as required, in accordance with the risk management strategy; and (e) Distributes documentation to [Assignment: organization-defined personnel or roles].  Supplemental Guidance  This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.  Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Security Engineering Principles | SA-8 |
| Control: Security Engineering Principles  The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.  Supplemental Guidance  Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example:   (i) developing layered protections;  (ii) establishing sound security policy, architecture, and controls as the foundation for design;  (iii) incorporating security requirements into the system development life cycle;  (iv) delineating physical and logical security boundaries;  (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and  (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.   Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.  References: NIST Special Publication 800-27. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | External Information System Services | SA-9 |
| Control: External Information System Services  The organization:  (a) Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; (b) Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and (c) Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.  Supplemental Guidance  External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that external providers processing, storing, or transmitting federal information or operating information systems on behalf of the federal government meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.   Related control: CA-3, IR-7, PS-7.  References: NIST Special Publication 800-35. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | External Information System Services | SA-9 (2) |
| Control: External Information System Services  The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.  Supplemental Guidance  Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.   Related control: CM-7.  References: NIST Special Publication 800-35. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Developer Configuration Management | SA-10 |
| Control: Developer Configuration Management  The organization requires the developer of the information system, system component, or information system service to:  (a) Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; (b) Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; (c) Implement only organization-approved changes to the information system; (d) Document approved changes to the system, component, or service and the potential security impacts of such changes; and (e) Track security flaws and flaw resolution within the system, component, or service.  Supplemental Guidance  This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.  Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.  References: NIST Special Publication 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Developer Security Testing and Evaluation | SA-11 |
| Control: Developer Security Testing and Evaluation  The organization requires the developer of the information system, system component, or information system service to:  (a) Create and implement a security assessment plan that provides for security testing and evaluation:  (1) At the depth of [Selection (one or more): security-related functional properties; securityrelated externally visible interfaces; high-level design; low-level design; implementation representation (source code/hardware schematics)]; and (2) At the rigor of [Selection: showing; demonstrating; rigorously demonstrating];   (b) Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined breadth/depth]; (c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; (d) Implement a verifiable flaw remediation process; and (e) Correct flaws identified during security testing/evaluation.  Supplemental Guidance  Developmental security testing/evaluation occurs at all post‐design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.  Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.  References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Supply Chain Protection | SA-12 |
| Control: Supply Chain Protection  The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.  Supplemental Guidance  Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.  Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.  References: NIST Special Publication 800-161; NIST Interagency Report 7622. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Supply Chain Protection | SA-12 (DHS-5.8.a) |
| Control: Supply Chain Protection  Business Impact Assessments (BIA) shall be used to determine the level of risk introduced to the system by the IT supply chain and whether the IT supply chain threat introduces sufficient risk to require the implementation of countermeasures.  Related Control: SA-12.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Supply Chain Protection | SA-12 (DHS-5.8.b) |
| Control: Supply Chain Protection  To protect against the supply chain threat, Components shall implement appropriate countermeasures, commensurate with the level of risk determined by the BIA.  Related Control: SA-12.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Development Process, Standards, and Tools | SA-15 |
| Control: Development Process, Standards, and Tools  The organization:  (a) Requires the developer of the information system, system component, or information system service to follow a documented development process that:  (1) Explicitly addresses security requirements; (2) Identifies the standards and tools used in the development process; (3) Documents the specific tool options and tool configurations used in the development process; and (4) Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and   (b) Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].  Supplemental Guidance  Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.   Related controls: SA-3, SA-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Developer-Provided Training | SA-16 |
| Control: Developer-Provided Training  The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.  Supplemental Guidance  This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer selftraining to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.  Related controls: AT-2, AT-3, SA-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 16.47 | Developer Security Architecture and Design | SA-17 |
| Control: Developer Security Architecture and Design  The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:  (a) Is consistent with and supportive of the security architecture established within the enterprise architecture; (b) Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and (c) Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.  Supplemental Guidance  This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization’s enterprise architecture and information security architecture.   Related controls: PL-8, PM-7, SA-3, SA-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 17.0 System and Communications Protection (SC)

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 |
| Control: System and Communications Protection Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and  (b) Reviews and updates the current:  (1) System and communications protection policy [Assignment: organization-defined frequency]; and (2) System and communications protection procedures [Assignment: organization-defined frequency].  Supplemental Guidance  This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal 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.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-3.17.a) |
| Control: System and Communications Protection Policy and Procedures  For those Components whose systems collect, process, or store Protected Health Information (PHI), they shall ensure that the stored information is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-4.4.1.a) |
| Control: System and Communications Protection Policy and Procedures  Components shall provide adequate physical and information security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST Special Publication (SP) 800-24, PBX Vulnerability Analysis, for guidance on detecting and fixing vulnerabilities in PBX systems.)  Related Control: None.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-4.5.2.a) |
| Control: System and Communications Protection Policy and Procedures  Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.   Related controls: SC-1, SC-7, SC-8, and SC-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-4.5.3.b) |
| Control: System and Communications Protection Policy and Procedures  Components shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.   Related controls: SC-8 and SC-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-5.5.2.t) |
| Control: System and Communications Protection Policy and Procedures  Commercial applications or appliances used by DHS that require the use of PKI certificates shall obtain those certificates from the DHS Principal CA or a DHS Component Internal Use NPE CA, as appropriate.  Commercial applications or appliances, that require the use of a proprietary CA implemented as an internal feature, shall not be acquired or used, unless prior concurrence by the DHS PKIMA and approval by the DHS PKIPA are obtained.  Related controls: SC-17.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-5.5.3.j) |
| Control: System and Communications Protection Policy and Procedures  Every human subscriber shall read, understand, and sign a “DHS PKI Human Subscriber Acknowledgement of Responsibilities” as a pre-condition for receiving certificates from a DHS CA. Signed PKI Human Subscriber Agreements shall be maintained by the DHS PKI Registrar.  Related controls: SC-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | System and Communications Protection Policy and Procedures | SC-1 (DHS-5.7.a) |
| Control: System and Communications Protection Policy and Procedures  Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (COTS) IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.   Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Application Partitioning | SC-2 |
| Control: Application Partitioning  The information system separates user functionality (including user interface services) from information system management functionality.  Supplemental Guidance  Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.   Related controls: SA-4, SA-8, SC-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Security Function Isolation | SC-3 |
| Control: Security Function Isolation  The information system isolates security functions from nonsecurity functions.  Supplemental Guidance  The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception.   Related controls: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Information in Shared Resources | SC-4 |
| Control: Information in Shared Resources  The information system prevents unauthorized and unintended information transfer via shared system resources.  Supplemental Guidance  This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address:   (i) information remanence which refers to residual representation of data that has been nominally erased or removed;   (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or   (iii) components within information systems for which there are only single users/roles.   Related controls: AC-3, AC-4, MP-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Denial of Service Protection | SC-5 |
| Control: Denial-of-Service Protection  The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].  Supplemental Guidance  A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.  Related controls: SC-6, SC-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Denial of Service Protection | SC-5 (DHS-4.6.1.c) |
| Control: Denial-of-Service Protection  Components shall identify countermeasures to denial-of-service attacks and complete a risk based evaluation prior to approving the use of a wireless PED.   Related controls: AC-19, PM-9, and SC-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 |
| Control: Boundary Protection  The information system:  (a) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; (b) Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and (c) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.  Supplemental Guidance  Managed interfaces include, for example, gateways, routers, firewalls, guards, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.   Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (3) |
| Control: Boundary Protection  The organization limits the number of external network connections to the information system.  Supplemental Guidance  Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.  Related control: None.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (4) |
| Control: Boundary Protection  The organization:  (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.  Supplemental Guidance  None.  Related control: SC-8.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (5) |
| Control: Boundary Protection  The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).  Supplemental Guidance  This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.  Related control: None.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (7) |
| Control: Boundary Protection  The information system, in conjunction with a remote device, prevents the device from  simultaneously establishing non-remote connections with the system and communicating via  some other connection to resources in external networks.  Supplemental Guidance  This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.  Related control: None.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (8) |
| Control: Boundary Protection  The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.  Supplemental Guidance  External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.  Related controls: AC-3, AU-2.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (18) |
| Control: Boundary Protection  The information system fails securely in the event of an operational failure of a boundary protection device.   Supplemental Guidance  Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.   Related controls: CP-2, SC-24.  References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (21) |
| Control: Boundary Protection  The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization defined missions and/or business functions].  Supplemental Guidance  Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys.   Related controls: CA-9, SC-3.   References: FIPS Publication 199; NIST Special Publications 800-41, 800-77. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (DHS-5.4.4.h) |
| Control: Boundary Protection  Components shall determine protocols and services permitted through their Component-level PEPs. Components may restrict traffic sources and destinations at their Component-level PEPs.   Related controls: SC-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (DHS-5.4.5.a) |
| Control: Boundary Protection  Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPs. The PSTN shall not be connected to OneNet at any time.   Related controls: SC-7.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Boundary Protection | SC-7 (DHS-5.4.5.b) |
| Control: Boundary Protection  Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.   Related controls: CM-7, SC-7, SC-8, and SC-9.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Transmission Confidentiality and Integrity | SC-8 |
| Control: Transmission Integrity  The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.  Supplemental Guidance  This control applies to both internal and external networks. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.   Related controls: AC-17, PE-4.  References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Transmission Confidentiality and Integrity | SC-8 (1) |
| Control: Transmission Integrity  The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards] .  Supplemental Guidance  Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.   Related control: SC-13.  References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; NSTISSI No. 7003. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Network Disconnect | SC-10 |
| Control: Network Disconnect  The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.  Supplemental Guidance  This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 |
| Control: Cryptographic Key Establishment and Management  The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].  Supplemental Guidance  Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.   Related controls: SC-13, SC-17.  References: NIST Special Publications 800-56, 800-57. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 (1) |
| Control: Cryptographic Key Establishment and Management  The organization maintains availability of information in the event of the loss of cryptographic keys by users.  Supplemental Guidance  Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).  Related control: None.  References: NIST Special Publications 800-56, 800-57. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 (DHS-4.6.b) |
| Control: Cryptographic Key Establishment and Management  Components using Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.   Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 (DHS-5.5.3.a) |
| Control: Cryptographic Key Establishment and Management  A single public/private key pair must not be used by a human subscriber for both encryption and digital signature.  Related control: SC-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 (DHS-5.5.3.b) |
| Control: Cryptographic Key Establishment and Management  A single public/private key pair must not be used by an NPE for both encryption and digital signature, whenever their separate use is supported by the protocols native to the NPE.  Related control: SC-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 (DHS-5.5.3.c) |
| Control: Cryptographic Key Establishment and Management  A authorized human sponsor shall represent each role, group, code-signer, system, application and device subscriber when the subscriber applies for one or more certificates from a DHS CA.   Related controls: SC-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Key Establishment and Management | SC-12 (DHS-5.5.3.i) |
| Control: Cryptographic Key Establishment and Management  Subscriber private keys shall not be used by more than one entity, with the following exceptions:   • Authorized members of a Group Subscriber, may use the Group’s private keys.   • Multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared.   Related controls: SC-12.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Protection | SC-13 |
| Control: Use of Cryptography  The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.  Supplemental Guidance  Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified information, the protection of Controlled Unclassified Information, the provision of digital signatures, and the enforcement of logical separation of information within an information system when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).   Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.  References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL, WWW.CNSS.GOV. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Protection | SC-13 (DHS-5.4.6.k) |
| Control: Use of Cryptography  When sending email containing any unencrypted sensitive information, particularly sensitive PII, users should use caution. When sending such information outside the dhs.gov domain, users shall ensure that the information is encrypted.  Related Control: None.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Protection | SC-13 (DHS-5.5.1.a) |
| Control: Use of Cryptography  Systems requiring encryption shall comply with the following methods:  - Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2 (Note: The use of triple DES [3DES] and FIPS 140-1 is no longer permitted.) - NSA Type 2 or Type 1 encryption   Related controls: IA-7 and SC-13.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Protection | SC-13 (DHS-5.5.1.c) |
| Control: Use of Cryptography  Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their use.   Related controls: IA-7 and SC-13.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Protection | SC-13 (DHS-5.5.2.v) |
| Control: Use of Cryptography  Commercial products used by DHS and applications developed by DHS that enable the use of PKI shall at a minimum support the following cryptographic algorithms and associated key sizes:  - SHA 1 - SHA 256 - RSA with 1024 Bit keys - RSA with 2048 bit keys - AES 128 - AES 256   Related Control: SC-17.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Cryptographic Protection | SC-13 (DHS-5.7.d) |
| Control: Use of Cryptography  Components shall use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography.  Related controls: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Collaborative Computing Devices | SC-15 |
| Control: Collaborative Computing Devices  The information system:  (a) Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and (b) Provides an explicit indication of use to users physically present at the devices.  Supplemental Guidance  Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.  Related control: AC-21.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Collaborative Computing Devices | SC-15 (DHS-4.5.3.a) |
| Control: Collaborative Computing Devices  Components shall implement controls to ensure that only authorized individuals are able to participate in each video conference.   Related controls: AC-3 and PE-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Collaborative Computing Devices | SC-15 (DHS-4.5.3.b) |
| Control: Collaborative Computing Devices  Components shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.  Related Control: SC-8 and SC-9.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Collaborative Computing Devices | SC-15 (DHS-4.5.3.c) |
| Control: Collaborative Computing Devices  Video teleconferencing equipment and software shall be disabled when not in use.   Related controls: AC-3 and PE-3.   References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Public Key Infrastructure Certificates | SC-17 |
| Control: Public Key Infrastructure Certificates  The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.  Supplemental Guidance  For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.  Related control: SC-12.   References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Mobile Code | SC-18 |
| Control: Mobile Code  The organization:  (a) Defines acceptable and unacceptable mobile code and mobile code technologies; (b) Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and (c) Authorizes, monitors, and controls the use of mobile code within the information system.  Supplemental Guidance  Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.   Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.  References: NIST Special Publication 800-28; DOD Instruction 8552.01. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Voice Over Internet Protocol | SC-19 |
| Control: Voice Over Internet Protocol  The organization:  (a) Establishes usage restrictions and implementation guidance for Voice over Internet Protocol(VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and, (b) Authorizes, monitors, and controls the use of VoIP within the information system.  Supplemental Guidance  None.  Related controls: CM-6, SC-7, SC-15.  References: NIST Special Publication 800-58. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Secure Name / Address Resolution Service (Authoritative Source) | SC-20 |
| Control: Secure Name/Address Resolution Service (Authoritative Source)  The information system:   (a) Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and (b) Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.   Supplemental Guidance   This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.   Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.  References: OMB Memorandum 08-23; NIST Special Publication 800-81. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Secure Name / Address Resolution Service (Authoritative Source) | SC-20 (DHS-5.4.3.k) |
| Control: Secure Name/Address Resolution Service (Authoritative Source)  All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.   Related controls: SC-20, SC-21, and SC-22.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | SC-21 |
| Control: Secure Name/Address Resolution Service (Recursive or Caching Resolver)  The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.  Supplemental Guidance  Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.   Related controls: SC-20, SC-22.  References: NIST Special Publication 800-81. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Architecture and Provisioning for Name/Address Resolution Service | SC-22 |
| Control: Architecture and Provisioning for Name/Address Resolution Service  The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.  Supplemental Guidance  Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).   Related controls: SC-2, SC-20, SC-21, SC-24.  References: NIST Special Publication 800-81. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Session Authenticity | SC-23 |
| Control: Session Authenticity  The information system protects the authenticity of communications sessions.  Supplemental Guidance  This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.   Related controls: SC-8, SC-10, SC-11.  References: NIST Special Publications 800-52, 800-77, 800-95. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Fail in Known State | SC-24 |
| Control: Fail in Known State  The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.  Supplemental Guidance  Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.  Related controls: CP-2, CP-10, CP-12, SC-7, SC-22.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Protection of Information at Rest | SC-28 |
| Control: Protection of Information at Rest  The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].  Supplemental Guidance  This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.   Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.  References: NIST Special Publications 800-56, 800-57, 800-111. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Protection of Information at Rest | SC-28 (DHS-5.2.g) |
| Control: Protection of Information at Rest  Components and Programs shall ensure that all data-at-rest, particularly in cloud or other virtual environments, preserves its identification and access requirements (anyone with access to data storage containing more than one type of information must have specific access authorization for every type of data in the data storage.  Related Control: None.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 17.47 | Process Isolation | SC-39 |
| Control: Process Isolation  The information system maintains a separate execution domain for each executing process.  Supplemental Guidance  Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.  Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 18.0 System and Information Integrity (SI)

|  |  |  |
| --- | --- | --- |
| 18.47 | System and Information Integrity Policy and Procedures | SI-1 |
| Control: System and Information Integrity Policy and Procedures  The organization:  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  (1) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and  (b) Reviews and updates the current:  (1) System and information integrity policy [Assignment: organization-defined frequency]; and (2) System and information integrity procedures [Assignment: organization-defined frequency].  Supplemental Guidance:   This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal 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: None.  References: NIST Special Publications 800-12, 800-100. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | System and Information Integrity Policy and Procedures | SI-1 (DHS-5.4.2.a) |
| Control: System and Information Integrity Policy and Procedures  Components shall provide continuous monitoring of their networks for security events, or outsource this requirement to the DHS Security Operations Center (SOC). Monitoring includes interception and disclosure as to the extent necessary for rendering service or to protect Department or Component rights or property. Here rights refers to ownership or entitlements or to property or information as in intellectual property. Service observation or random monitoring shall not be used except for mechanical or service quality control checks in accordance with the Electronic Communications Privacy Act.  Related controls: SI-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | System and Information Integrity Policy and Procedures | SI-1 (DHS-5.4.5.c) |
| Control: System and Information Integrity Policy and Procedures  Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment.   [Note: When the technology becomes available and code can be vetted for security, the policy will be “Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS systems.”]   Related controls: SC-18.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | System and Information Integrity Policy and Procedures | SI-1 (DHS-5.4.6.h) |
| Control: System and Information Integrity Policy and Procedures  The DHS email gateway Steward shall provide email monitoring for spam at the gateway.   Related control: SI-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Flaw Remediation | SI-2 |
| Control: Flaw Remediation  The organization:  (a) Identifies, reports, and corrects information system flaws; (b) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; (c) Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and (d) Incorporates flaw remediation into the organizational configuration management process.  Supplemental Guidance:   Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.   Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.  References: NIST Special Publications 800-40, 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Flaw Remediation | SI-2 (1) |
| Control: Flaw Remediation  The organization centrally manages the flaw remediation process.  Supplemental Guidance  Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.  Related control: None.  References: NIST Special Publications 800-40, 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Flaw Remediation | SI-2 (2) |
| Control: Flaw Remediation  The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.  Supplemental Guidance  None.  Related controls: CM-6, SI-4.  References: NIST Special Publications 800-40, 800-128. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Malicious Code Protection | SI-3 |
| Control: Malicious Code Protection  The organization:  (a) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; (b) Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; (c) Configures malicious code protection mechanisms to:  (1) Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and (2) [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and,  (d) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.  Supplemental Guidance:   Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.   Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.  References: NIST Special Publication 800-83. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Malicious Code Protection | SI-3 (1) |
| Control: Malicious Code Protection  The organization centrally manages malicious code protection mechanisms.  Supplemental Guidance  Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls.  Related controls: AU-2, SI-8.  References: NIST Special Publication 800-83. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Malicious Code Protection | SI-3 (2) |
| Control: Malicious Code Protection  The information system automatically updates malicious code protection mechanisms.  Supplemental Guidance:   Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.   Related control: SI-8.  References: NIST Special Publication 800-83. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Malicious Code Protection | SI-3 (10) |
| Control: Malicious Code Protection  The organization:  (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of malicious code; and (b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.  Supplemental Guidance  The application of selected malicious code analysis tools and techniques provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates more effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code.  Related control: None.  References: NIST Special Publication 800-83. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Malicious Code Protection | SI-3 (DHS-5.4.6.g) |
| Control: Malicious Code Protection  The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.   Related control: SI-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Information System Monitoring | SI-4 |
| Control: Information System Monitoring  The organization:  (a) Monitors the information system to detect:  (1) Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and (2) Unauthorized local, network, and remote connections;  (b) Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; (c) Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; (d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; (e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; (f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and (g) Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].  Supplemental Guidance  Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.  Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.  References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Information System Monitoring | SI-4 (2) |
| Control: Information System Monitoring  The organization employs automated tools to support near real-time analysis of events.  Supplemental Guidance:   Automated tools include, for example, host-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.  Related control: None.  References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Information System Monitoring | SI-4 (4) |
| Control: Information System Monitoring  The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.  Supplemental Guidance  Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.  Related Controls: None  References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Information System Monitoring | SI-4 (5) |
| Control: Information System Monitoring  The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].  Supplemental Guidance  Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers.   Related controls: AU-5, PE-6.  References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Security Alerts, Advisories, and Directives | SI-5 |
| Control: Security Alerts, Advisories, and Directives  The organization:  (a) Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; (b) Generates internal security alerts, advisories, and directives as deemed necessary; (c) Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and (d) Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.  Supplemental Guidance:   The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.   Related control: SI-2  References: NIST Special Publication 800-40. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Security Alerts, Advisories, and Directives | SI-5 (1) |
| Control: Security Alerts, Advisories, and Directives  The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.  Supplemental Guidance  The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information system level.  Related Controls: None.  References: NIST Special Publication 800-40. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Security Function Verification | SI-6 |
| Control: Security Functionality Verification  The information system:  (a) Verifies the correct operation of [Assignment: organization-defined security functions]; (b) Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; (c) Notifies [Assignment: organization-defined personnel or roles] of failed automated security tests; and (d) [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.  Supplemental Guidance  Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.   Related controls: CA-7, CM-6.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 |
| Control: Software and Information Integrity  The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].  Supplemental Guidance  Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.   Related controls: SA-12, SC-8, SC-13, SI-3.  References: NIST Special Publications 800-147, 800-155. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 (1) |
| Control: Software and Information Integrity  The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].  Supplemental Guidance  Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.  Related control: None.  References: NIST Special Publications 800-147, 800-155. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 (2) |
| Control: Software and Information Integrity  The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.  Supplemental Guidance  The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.  Related Controls: None.  References: NIST Special Publications 800-147, 800-155. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 (5) |
| Control: Software and Information Integrity  The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.  Supplemental Guidance  Organizations may define different integrity checking and anomaly responses:   (i) by type of information (e.g., firmware, software, user data);  (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or  (iii) a combination of both.   Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.  Related control: None.  References: NIST Special Publications 800-147, 800-155. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 (7) |
| Control: Software and Information Integrity  The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.  Supplemental Guidance  This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.  Related controls: IR-4, IR-5, SI-4.  References: NIST Special Publications 800-147, 800-155. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 (14) |
| Control: Software and Information Integrity  The organization:  (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and (b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.  Supplemental Guidance  This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations.  Related control: SA-5.  References: NIST Special Publications 800-147, 800-155. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Software, Firmware, and Information Integrity | SI-7 (DHS-5.1.1.e) |
| Control: Software and Information Integrity  Components shall prohibit passwords from being embedded in scripts or source code.  Related Control: IA-5.  Reference: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Spam Protection | SI-8 |
| Control: Spam Protection  The organization:  (a) Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and (b) Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.  Supplemental Guidance  Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.   Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.  References: NIST Special Publication 800-45. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Spam Protection | SI-8 (1) |
| Control: Spam Protection  The organization centrally manages spam protection mechanisms.  Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.  Related controls: AU-3, SI-2, SI-7.  References: NIST Special Publication 800-45. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Spam Protection | SI-8 (2) |
| Control: Spam Protection  The information system automatically updates spam protection mechanisms.  Supplemental Guidance  None.  Related controls: None.  References: NIST Special Publication 800-45. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Information Input Validation | SI-10 |
| Control: Information Input Validation  The information system checks the validity of [Assignment: organization-defined information inputs].  Supplemental Guidance  Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Error Handling | SI-11 |
| Control: Error Handling  The information system:  (a) Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and (b) Reveals error messages only to [Assignment: organization-defined personnel or roles].  Supplemental Guidance  Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.   Related controls: AU-2, AU-3, SC-31.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Information Handling and Retention | SI-12 |
| Control: Information Output Handling and Retention  The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.  Supplemental Guidance  Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.   Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 18.47 | Memory Protection | SI-16 |
| Control: Memory Protection  The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.  Supplemental Guidance  Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.  Related controls: AC-25, SC-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 19.0 Program Management (PM)

|  |  |  |
| --- | --- | --- |
| 19.47 | Information Security Program Plan | PM-1 |
| Control: Information Security Program Plan  The organization:  (a) Develops and disseminates an organization-wide information security program plan that:  (1) Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; (2) Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; (3) Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and (4) Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;  (b) Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; (c) Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and (d) Protects the information security program plan from unauthorized disclosure and modification.  Supplemental Guidance  Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.  The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization’s information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.  Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.   Related control: PM-8.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Senior Information Security Officer | PM-2 |
| Control: Senior Information Security Officer  The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.   Supplemental Guidance  The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.  Related control: None.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Information Security Resources | PM-3 |
| Control: Information Security Resources  The organization:  (a) Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; (b) Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and (c) Ensures that information security resources are available for expenditure as planned.  Supplemental Guidance  Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.  Related controls: PM-4, SA-2.  References: NIST Special Publication 800-65. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Plan of Action and Milestones Process | PM-4 |
| Control: Plan of Action and Milestones Process  The organization:  (a) Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:  (1) Are developed and maintained; (2) Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and (3) Are reported in accordance with OMB FISMA reporting requirements.  (b) Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.  Supplemental Guidance  The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.   Related control: CA-5.  References: OMB Memorandum 02-01; NIST Special Publication 800-37. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Information System Inventory | PM-5 |
| Control: Information System Inventory  The organization develops and maintains an inventory of its information systems.   Supplemental Guidance  This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.  Related control: None.  References: Web: www.omb.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Information Security Measures of Performance | PM-6 |
| Control: Information Security Measures of Performance  The organization develops, monitors, and reports on the results of information security measures of performance.  Supplemental Guidance  Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.  Related control: None.  References: NIST Special Publication 800-55. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Enterprise Architecture | PM-7 |
| Control: Enterprise Architecture  The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.    Supplemental Guidance  The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization’s enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization’s mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.   Related controls: PL-2, PL-8, PM-11, RA-2, SA-3.  References: NIST Special Publication 800-39; Web: www.fsam.gov. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Critical Infrastructure Plan | PM-8 |
| Control: Critical Infrastructure Plan  The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.   Supplemental Guidance  Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.   Related controls: PM-1, PM-9, PM-11, RA-3.  References: HSPD 7; National Infrastructure Protection Plan. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Risk Management Strategy | PM-9 |
| Control: Risk Management Strategy  The organization:  (a) Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; (b) Implements the risk management strategy consistently across the organization; and (c) Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.  Supplemental Guidance  An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization’s risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.   Related control: RA-3.  References: NIST Special Publications 800-30, 800-39. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Security Authorization Process | PM-10 |
| Control: Security Authorization Process  The organization:  (a) Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; (b) Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and (c) Fully integrates the security authorization processes into an organization-wide risk management program.  Supplemental Guidance  Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.   Related control: CA-6.   References: NIST Special Publications 800-37, 800-39. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Mission/Business Process Definition | PM-11 |
| Control: Mission/Business Process Definition  The organization:  (a) Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and (b) Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.  Supplemental Guidance  Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization’s information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure.   Related controls: PM-7, PM-8, RA-2.  References: FIPS Publication 199; NIST Special Publication 800-60. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Insider Threat Program | PM-12 |
| Control: Insider Threat Program  The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.  Supplemental Guidance  Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.  Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.  Related controls: AC-6, AT-2, AU-6, AU-7- AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.  References: Executive Order 13587. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Information Security Workforce | PM-13 |
| Control: Information Security Workforce  The organization establishes an information security workforce development and improvement program.  Supplemental Guidance  Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.  Related controls: AT-2, AT-3.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Testing, Training, and Monitoring | PM-14 |
| Control: Testing, Training, and Monitoring  The organization:  (a) Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:  (1) Are developed and maintained; and (2) Continue to be executed in a timely manner;  (b) Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.  Supplemental Guidance  This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.   Related controls: AT-3, CA-7, CP-4, IR-3, SI-4.  References: NIST Special Publications 800-16, 800-37, 800-53A, 800-137. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Contacts with Security and Associations | PM-15 |
| Control: Contacts with Security Groups and Associations  The organization establishes and institutionalizes contact with selected groups and associations within the security community:  (a) To facilitate ongoing security education and training for organizational personnel; (b) To maintain currency with recommended security practices, techniques, and technologies; and (c) To share current security-related information including threats, vulnerabilities, and incidents.  Supplemental Guidance  Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.   Related control: SI-5.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 19.47 | Threat Awareness Program | PM-16 |
| Control: Threat Awareness Program  The organization implements a threat awareness program that includes a cross organization information-sharing capability.  Supplemental Guidance  Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.   Related controls: PM-12, PM-16.  References: None. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 20.0 Privacy

|  |  |  |
| --- | --- | --- |
| 20.47 | Authority to Collect | PRIV-AP-1 |
| Control: Authority to Collect  The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.  Supplemental Guidance  Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.  Related controls: AR-2, DM-1, TR-1, TR-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Purpose Specification | PRIV-AP-2 |
| Control: Purpose Specification  The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.  Supplemental Guidance  Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.  Related controls: AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347). | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Governance and Privacy Program | PRIV-AR-1 |
| Control: Governance and Privacy Program  The organization:  (a) Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; (b) Monitors federal privacy laws and policy for changes that affect the privacy program; (c) Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program; (d) Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; (e) Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and (f) Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].  Supplemental Guidance  The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.  To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.  Related control: None.  References: The Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 07-16; OMB Circular A-130; Federal Enterprise Architecture Security and Privacy Profile. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Impact and Risk Assessment | PRIV-AR-2 |
| Control: Privacy Impact and Risk Assessment  The organization:  (a) Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and (b) Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.  Supplemental Guidance  Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.  Related control: None.  References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Requirements for Contractors and Service Providers | PRIV-AR-3 |
| Control: Privacy Requirements for Contractors and Service Providers  The organization:  (a) Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and (b) Includes privacy requirements in contracts and other acquisition-related documents.  Supplemental Guidance  Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.  Related control: AR-1, AR-5, SA-4.  References: The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Monitoring and Auditing | PRIV-AR-4 |
| Control: Privacy Monitoring and Auditing  The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.  Supplemental Guidance  To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).  Organizations also:  (i) implement technology to audit for the security, appropriate use, and loss of PII;  (ii) perform reviews to ensure physical security of documents containing PII;  (iii) assess contractor compliance with privacy requirements; and  (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.  Related controls: AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Awareness and Training | PRIV-AR-5 |
| Control: Privacy Awareness and Training  The organization:  (a) Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; (b) Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and (c) Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].  Supplemental Guidance  Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIAs) or System of Records Notices (SORNs) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, and Organizations program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training.  Related controls: AR-3, AT-2, AT-3, TR-1.  References: The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Reporting | PRIV-AR-6 |
| Control: Privacy Reporting  The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.  Supplemental Guidance  Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; and (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.  Related control: None.  References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Memoranda 03-22; OMB Circular A-130. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy-Enhanced System Design and Development | PRIV-AR-7 |
| Control: Privacy-Enhanced System Design and Development  The organization designs information systems to support privacy by automating privacy controls.  Supplemental Guidance  To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization’s privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes.  Related controls: AC-6, AR-4, AR-5, DM-2, TR-1.  References: The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Accounting of Disclosures | PRIV-AR-8 |
| Control: Accounting of Disclosures  The organization:  (a) Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:  (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made;  (b) Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and (c) Makes the accounting of disclosures available to the person named in the record upon request.  Supplemental Guidance  The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals.  Related control: IP-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k). | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Data Quality | PRIV-DI-1 |
| Control: Data Quality  The organization:  (a) Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; (b) Collects PII directly from the individual to the greatest extent practicable; (c) Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and (d) Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.  Supplemental Guidance  Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.  When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer’s income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.  Related controls: AP-2, DI-2, DM-1, IP-3, SI-10.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB Memorandum 07-16. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Data Integrity and Data Integrity Board | PRIV-DI-2 |
| Control: Data Integrity and Data Integrity Board  The organization:  (a) Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and, (b) Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.  Supplemental Guidance  Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements.  Related controls: AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2.  References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Minimization of Personally Identifiable Information | PRIV-DM-1 |
| Control: Minimization of Personally Identifiable Information  The organization:  (a) identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;  (b) limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and,  (c) conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.  Supplemental Guidance  Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.  Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.  By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.  Related controls: AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1.  References: The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Data Retention and Disposal | PRIV-DM-2 |
| Control: Data Retention and Disposal  The organization:  (a) retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law;  (b) disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and,  (c) uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).  Supplemental Guidance  NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.  Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization’s records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.  Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media.  Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Minimization of PII Used in Testing, Training, and Research | PRIV-DM-3 |
| Control: Minimization of PII Used in Testing, Training, and Research  The organization:  (a) develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and,  (b) implements controls to protect PII used for testing, training, and research.  Supplemental Guidance: Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.  Related control: None.  References: NIST Special Publication 800-122. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Consent | PRIV-IP-1 |
| Control: Consent  The organization:  (a) Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; (b) Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; (c) Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and (d) Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.  Supplemental Guidance  Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.  Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission’s Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals’ behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization.  Related controls: AC-2, AP-1, TR-1, TR-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-22. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Individual Access | PRIV-IP-2 |
| Control: Individual Access  The organization:  (a) Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; (b) Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; (c) Publishes access procedures in System of Records Notices (SORNs); and (d) Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.  Supplemental Guidance  Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.  Related controls: AR-8, IP-3, TR-1, TR-2.  References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t); OMB Circular A-130. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Redress | PRIV-IP-3 |
| Control: Redress  The organization:  (a) Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and, (b) Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.  Supplemental Guidance  Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.  To provide effective redress, organizations:  (i) provide effective notice of the existence of a PII collection;  (ii) provide plain language explanations of the processes and mechanisms for requesting access to records;  (iii) establish criteria for submitting requests for correction or amendment;  (iv) implement resources to analyze and adjudicate requests;  (v) implement means of correcting or amending data collections; and  (vi) review any decisions that may have been the result of inaccurate information.  Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information.  Related controls: IP-2, TR-1, TR-2, UL-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Complaint Management | PRIV-IP-4 |
| Control: Complaint Management  The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.  Supplemental Guidance  Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.  Related controls: AR-6, IP-3.  References: OMB Circular A-130; OMB Memoranda 07-16, 08-09. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Inventory of Personally Identifiable Information | PRIV-SE-1 |
| Control: Inventory of Personally Identifiable Information  The organization:  (a) Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and  (b) Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.  Supplemental Guidance  The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII.  Related controls: AR-1, AR-4, AR-5, AT-1, DM-1, PM-5, UL-3.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST Special Publications 800-37, 800-122. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Incident Response | PRIV-SE-2 |
| Control: Privacy Incident Response  The organization:  In contrast to the Incident Response (IR) family in Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO.   The plan includes:  (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan;  (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly;  (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks;  (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and  (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials.   Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.  Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1.  Control Enhancements: None.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Privacy Notice | PRIV-TR-1 |
| Control: Privacy Notice  The organization:  (a) Provides effective notice to the public and to individuals regarding:  (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;  (b) Describes:  (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and  (c) Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.  Supplemental Guidance  Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.  The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization’s public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization’s compliance with the public notice provisions of the Privacy Act, the E-Government Act’s PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).124 Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel.  Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | System of Records Notices and Privacy Act Statements | PRIV-TR-2 |
| Control: System of Records Notices and Privacy Act Statements  The organization:  (a) Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);  (b) Keeps SORNs current; and  (c) Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.  Supplemental Guidance  Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as “a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier.” SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys).  Related control: DI-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Dissemination of Privacy Program Information | PRIV-TR-3 |
| Control: Dissemination of Privacy Program Information  The organization:  (a) Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and (b) Ensures that its privacy practices are publicly available through organizational Web sites or otherwise.  Supplemental Guidance  Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.  Related control: AR-6.  References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-23. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Internal Use | PRIV-UL-1 |
| Control: Internal Use  The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.  Supplemental Guidance  Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII.  Related controls: AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1). | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

|  |  |  |
| --- | --- | --- |
| 20.47 | Information Sharing with Third Parties | PRIV-UL-2 |
| Control: Information Sharing with Third Parties  The organization:  (a) Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; (b) Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; (c) Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and (d) Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.  Supplemental Guidance  The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.  Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1.  References: The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines. | |
| Status: | |
| Implementation: Not Provided  Responsible Entitles: | |

# 21.0 Plan Approval

We have reviewed the Security Plan for Test\_2015-01-15-1052 and have made the determination that the security requirements and security controls selected for this system are in fact adequate to satisfy the security objectives of confidentiality, integrity, and availability based on the identified security impact level for Test\_2015-01-15-1052

[INFORMATION SYSTEM OWNER] [Date]

{*Insert System Owner signature block*}

[COMPONENT CISO/ISSM] [Date]

{*Insert Component CISO/ISSM signature block*}

[AUTHORIZING OFFICIAL] [Date]

{*Insert Authorizing Official signature block}*

# Acronyms

|  |  |
| --- | --- |
| AC | Access Control |
| AES | Advanced Encryption Standards |
| AO | Authorizing Official |
| ARB | Acquisition Review Board |
| AT | Awareness and Training |
| ATO | Authority to Operate |
| AU | Audit and Accountability |
| BI | Background Investigation |
| BIA | Business Impact Assessment |
| BLSR | Baseline Security Requirements |
| CA | Certificate Authority |
| CA | Certification, Accreditation, and Security Assessments |
| CCB | Change Control Board |
| CFO | Chief Financial Officer |
| CI | Counter-Intelligence |
| C-I-A | Confidentiality, Integrity, and Availability |
| CIO | Chief Information Officer |
| CISID | Chief, Internal Security and Investigations Division |
| CISO | Chief Information Security Officer |
| CM | Configuration Management |
| CMG | Core Management Group |
| CMP | Configuration Management Plan |
| CONOPS | Concept of Operations |
| COOP | Continuity of Operations Planning |
| COOP | Continuity of Operations Plan |
| COTS | Commercial off the Shelf |
| CP | Certificate Policy |
| CP | Contingency Plan |
| CP | Contingency Planning |
| CPIC | Capital Planning and Investment Control |
| CPS | Certificate Practices Statement |
| CRE | Computer-Readable Extract |
| CRL | Certificate Revocation List |
| CSIRC | Computer Security Incident Response Center |
| CUI | Control Unclassified Information |
| DES | Digital Encryption Standards |
| DHS | Department of Homeland Security |
| DNSSE | Domain Name System Security Extensions |
| DoD | Department of Defense |
| DoS | Department of State |
| DoT | Department of Treasury |
| EA | Enterprise Architecture |
| EAB | Enterprise Architecture Board |
| EO | Executive Order |
| EOC | Enterprise Operations Center |
| FBCA | Federal Bridge Certification Authority |
| FDCC | Federal Desktop Core Configuration |
| FICAM | Federal Identity, Credentialing, and Access Management |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| FOUO | For Official Use Only |
| FPKI PA | Federal PKI Policy Authority |
| FTP | File Transfer Protocol |
| FYHSP | Future Years Homeland Security Program |
| GSA | General Services Administration |
| GSS | General Support System |
| HIPAA | Health Insurance Portability and Accountability Act |
| HSAR | Homeland Security Acquisition Regulations |
| HSPD | Homeland Security Presidential Directive |
| HVAC | Heating, Ventilation and Air Conditioning |
| IA | Identification and Authentication |
| IA | Information Assurance |
| IATO | Interim Authority to Operate |
| ICAM | Identity, Credentialing, and Access Management |
| IDS | Intrusion Detection System |
| IOD | Object identifier |
| IR | Infrared Response |
| IR | Incident Response |
| IRB | Investment Review Board |
| ISA | Interconnection Security Agreement |
| ISO | Information Security Office |
| ISSO | Information System Security Officer |
| ISVM | Information System Vulnerability Management |
| IT | Information Technology |
| JWICS | Joint Worldwide Intelligence Communications System |
| LAN | Local Area Network |
| LE | Law Enforcement |
| LMR | Land Mobile Radio |
| MA | Maintenance |
| MA | Major Application |
| MBI | Minimum Background Investigation |
| MBI | Minimum Background Investigation |
| MD | Management Directive |
| MD | Management Directive |
| MMS | Multimedia Messaging Service |
| MMS | Multimedia Messaging Service |
| MP | Media Protection |
| MP | Media Protection |
| NIAP | National Information Assurance Partnership |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NOC | Network Operations Center |
| NSA | National Security Agency |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |
| OIS | Office of Information Security |
| OMB | Office of Management and Budget |
| OPA | Office of Public Affairs |
| OPM | Office of Personnel Management |
| OTAR | Over-The-Air-Rekeying |
| PA | Policy Authority |
| PBX | Private Branch Exchange |
| PCS | Personal Communications Services |
| PDA | Personal Digital Assistant |
| PE | Physical and Environmental Protection |
| PED | Portable Electronic Device |
| PEP | Policy Enforcement Point |
| PHI | Protected Health Information |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PIN | Personal Identity Number |
| PIRT | Privacy Incident Response Team |
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure |
| PKI PA | PKI Policy Authority |
| PKI PM | PKI Management Authority |
| PL | Planning |
| PM | Program Manager |
| PM | Program Manager |
| PNS | Protected Network Services |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| PPOC | Privacy Point of Contact |
| PS | Personnel Security |
| PSTN | Public Switched Telephone Network |
| PTA | Privacy Threshold Analysis |
| RA | Risk Assessment |
| RA | Registration Authority |
| RDP | Remote Desktop Protocol |
| RF | Radio Frequency |
| RFI | Radio Frequency Identification |
| RMS | Risk Management System |
| SA | System and Services Acquisition |
| SA | Security Architecture |
| SAISO | Senior Agency Information Security Officer |
| SAN | Subject Alternative Name |
| SAOP | Senior Agency Official for Privacy |
| SAR | Security Assessment Report |
| SC | System and Communications Protection |
| SCDN | Homeland Secure Data Network |
| SCI | Sensitive Compartmented Information |
| SCO | Chief Security Officer |
| SELC | Systems Engineering Life Cycle |
| SI | System and Information Integrity |
| SLA | Service Level Agreement |
| SMS | Short Message Service |
| SOC | Security Operations Center |
| SOP | Standard Operating Procedure |
| SORN | System of Records Notice |
| SP | Security Plan |
| SP | Special Publication |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| SSP | Shared Service Provider |
| TAF | TrustedAgent FISMA |
| TFPAP | Trust Framework Provider Adoption Process |
| TIC | Trusted Internet Connections |
| TOS | Terms of Service |
| TRM | Technical Reference Model |
| TS | Top Secret |
| US-CERT | United States Computer Emergency Readiness Team |
| USGCB | U.S. Government Configuration Baseline |
| VA | Vulnerability Assessment |
| VAT | Vulnerability Assessment Team |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |
| WPAN | Wireless Personal Area Network |
| WWAN | Wireless Wide Area Network |