Remote Access Servers

System Security Plan

Author Name, Title

Contents

1 Introduction **4**
- 1.1 About this document . . . 4
- 1.2 Standards . . . 4
- 1.3 Certifications . . . 4

2 Remote Access Servers **5**
- 2.1 Overview . . . 5
- 2.2 Components . . . 6
  - 2.2.1 Citrix remote access server . . . 6
  - 2.2.2 Windows remote access server . . . 6
  - 2.2.3 SSH remote access server . . . 6

3 Appendix: Standards **10**
- 3.1 Simple Standard #1 . . . 10
  - 3.1.1 Families . . . 10
  - 3.1.2 Controls . . . 10
- 3.2 NIST SP 800-53 Revision 4 . . . 10
  - 3.2.1 Families . . . 10
  - 3.2.2 Controls . . . 11

List of Tables

3.1 Control families for Simple Standard #1 10
3.2 Control families for NIST SP 800-53 Revision 4 10

List of Figures

2.1 High-level diagram of Remote Access System 5
2.2 Placeholder for CMDB report 7
2.3 SSHGuard blocks offender IPs 8

Chapter 1

Introduction

1.1 About this document

A System Security Plan (SSP) is a document to describe security controls in use on an information system and their implementation. An SSP provides:

- Narrative of security control implementation
- Description of components and services
- System data flows and authorization boundaries

1.2 Standards

This SSP draws from these standards:

- Simple Standard #1
- NIST SP 800-53 Revision 4

The full copy of each standard is included in the appendix.

1.3 Certifications

A certification is a logical grouping of controls that are of interest to a given subject. A particular certification does not necessarily target all controls from a standard, nor does a particular certification need to draw from a single standard.

This SSP addresses these certifications:

- Low side
  - NIST-800-53-r4 control AC-2 (5)
- High side
  - NIST-800-53-r4 control AC-2 (5)
  - S1 control 2.1
  - S1 control 9.5

Chapter 2

Remote Access Servers

2.1 Overview

My Example Organization, Inc. (MyEO) classifies remote access servers as *jump hosts* or *bastion hosts*. The organization recognizes the following definitions when necessary to distinguish between the two classes of remote access server.

Jump host

Allows access between *internal* domains with different trust levels.

For example, MyEO uses jump hosts to restrict access between corporate desktop environments and server environments within organization datacenters.

Bastion host

Allows access into corporate environments from *external* domains.

For example, MyEO uses bastion hosts to restrict access from the public Internet.

Here is a high-level diagram of the remote access system.

Figure 2.1: High-level diagram of Remote Access System

2.2 Components

2.2.1 Citrix remote access server

Citrix remote access servers enable employees to remotely access a subset of MyEO systems. Remote access is only available via VPN with multi-factor authentication.

The organization has not yet documented attestations for this component.

2.2.2 Windows remote access server

Windows remote access servers enable employees to remotely access a subset of MyEO systems. Remote access is only available via VPN with multi-factor authentication.

The organization has not yet documented attestations for this component.

2.2.3 SSH remote access server

SSH remote access servers enable employees to remotely access a subset of MyEO systems. Remote access requires multi-factor authentication but does not require VPN.

The organization offers the following attestations for this component.

2.2.3.1 Terminate inactive ssh sessions after 15 minutes

Status	Date verified	Satisfies
complete	2020-05-01	• S1 control 9.5 • NIST-800-53-r4 control AC-12 • NIST-800-53-r4 control AC-2 (5)

MyEO uses configuration management to configure sshd to terminate idle (inactive) sessions after 900 seconds (15 minutes).

The specific settings for sshd include:

```
# Request a response
# from the client through the encrypted channel
# if no data has been received from the client within this many seconds.
ClientAliveInterval 300

# Terminate the session
# if the client has not responded in this many ClientAliveIntervals.
ClientAliveCountMax 3
```

MyEO verifies the configuration through its central management database (CMDB), which is updated via daily automation. The automation runs a job on each host and collects the configuration as it actually exists on the host to populate the CMDB. Job automation triggers an alert if any host fails to respond to the collection.

The following screenshot of the CMDB report shows that 100% of systems have the idle timeout set to the specified configuration:

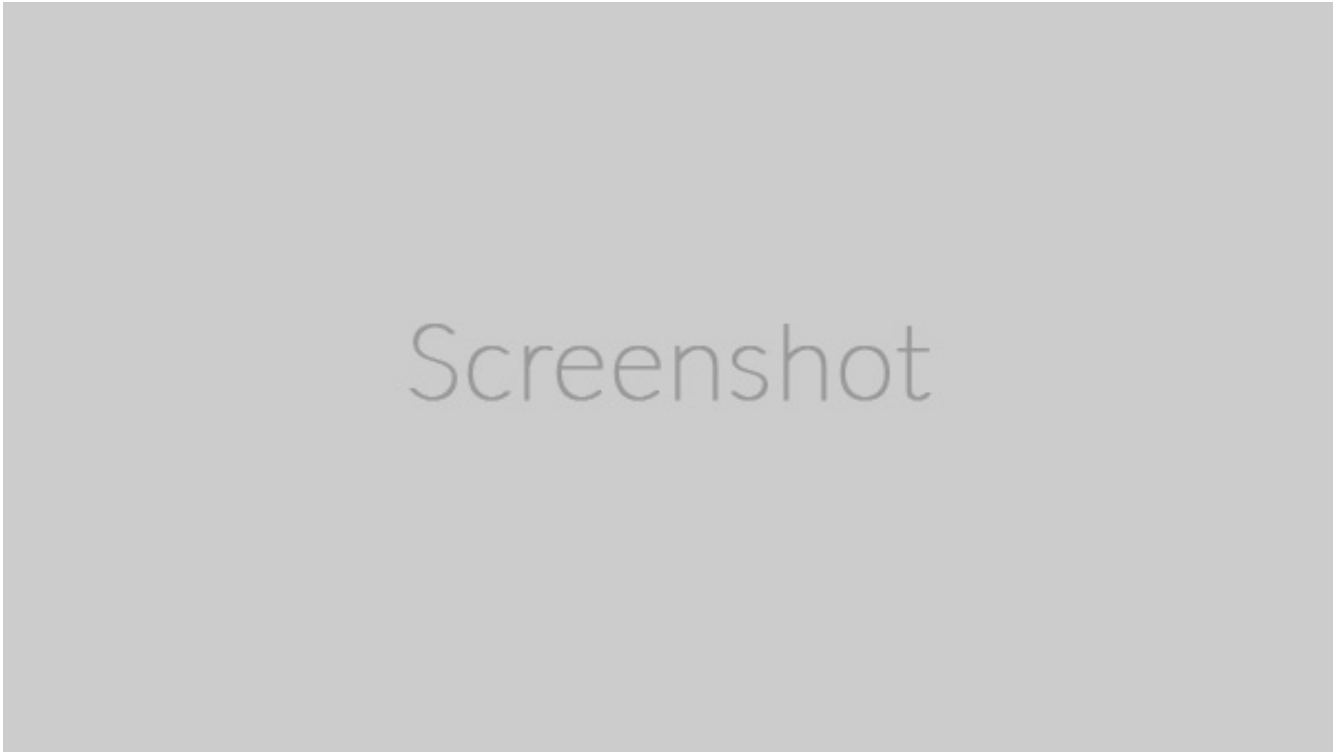

Figure 2.2: Placeholder for CMDB report

References:

- sshd config in organization puppet source control
- sshd_config(5)

2.2.3.2 Monitor and block unsuccessful logon attempts

Status	Date verified	Satisfies
complete	2020-05-01	• NIST-800-53-r4 control AC-7 • NIST-800-53-r4 control AC-17 (1) • NIST-800-53-r4 control SI-4

MyEO uses configuration management to install and configure `sshguard` on bastion hosts to continuously aggregate system logs, monitor unsuccessful logon attempts, and block repeat offenders. The tool adds offenders to a *DROP* rule on the host firewall. The DROP rule prevents the offender from establishing any type of connection to the bastion for the configured amount of time.

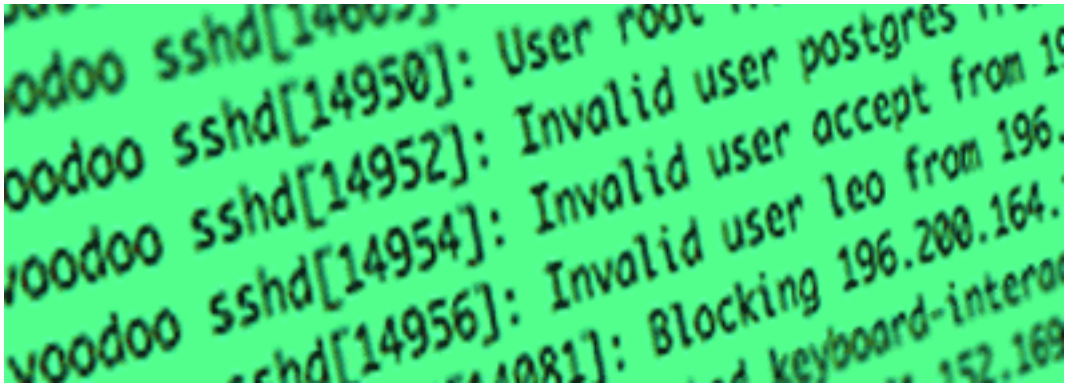

Figure 2.3: SSHGuard blocks offender IPs

The following output shows a tiny portion of blocked offenders for a single ssh bastion.

```
Chain sshguard (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       37.139.4.138         0.0.0.0/0
    4   240 DROP       all  --  *      *       211.213.198.139      0.0.0.0/0
   10   600 DROP       all  --  *      *       49.235.229.211       0.0.0.0/0
   24  1440 DROP       all  --  *      *       104.131.231.109      0.0.0.0/0
   44  2640 DROP       all  --  *      *       139.199.18.200       0.0.0.0/0
   35  2028 DROP       all  --  *      *       49.234.50.247        0.0.0.0/0
   80  4800 DROP       all  --  *      *       125.124.147.117      0.0.0.0/0
  136  8160 DROP       all  --  *      *       51.77.220.183        0.0.0.0/0
  116  6960 DROP       all  --  *      *       103.218.242.102      0.0.0.0/0
  149  8212 DROP       all  --  *      *       101.231.124.6        0.0.0.0/0
   52  3056 DROP       all  --  *      *       175.24.67.124        0.0.0.0/0
  152  9120 DROP       all  --  *      *       118.24.208.67        0.0.0.0/0
   80  4800 DROP       all  --  *      *       170.239.47.251       0.0.0.0/0
   52  3120 DROP       all  --  *      *       167.71.63.63         0.0.0.0/0
  152  9072 DROP       all  --  *      *       154.8.141.3          0.0.0.0/0
   80  4800 DROP       all  --  *      *       188.173.97.144       0.0.0.0/0
  172 10320 DROP       all  --  *      *       46.8.158.66          0.0.0.0/0
  173 10308 DROP       all  --  *      *       165.22.215.70        0.0.0.0/0
  176 10560 DROP       all  --  *      *       117.33.253.49        0.0.0.0/0
   15   836 DROP       all  --  *      *       209.182.237.202      0.0.0.0/0
   44  2640 DROP       all  --  *      *       45.162.4.175         0.0.0.0/0
  104  6240 DROP       all  --  *      *       77.65.17.2           0.0.0.0/0
  104  6240 DROP       all  --  *      *       62.148.142.202       0.0.0.0/0
   71  4260 DROP       all  --  *      *       200.14.32.101        0.0.0.0/0
   92  5520 DROP       all  --  *      *       139.59.46.243        0.0.0.0/0
   38  2280 DROP       all  --  *      *       150.109.62.167       0.0.0.0/0
  148  8808 DROP       all  --  *      *       118.25.152.169       0.0.0.0/0
  180 10800 DROP       all  --  *      *       192.144.136.109      0.0.0.0/0
   96  5760 DROP       all  --  *      *       52.130.92.196        0.0.0.0/0
   58  3416 DROP       all  --  *      *       49.234.27.90         0.0.0.0/0
```

References:

- sshguard config in organization source control

- sshguard

Chapter 3

Appendix: Standards

3.1 Simple Standard #1

3.1.1 Families

Simple Standard #1 categorizes controls into logical groups called families.

Table 3.1: Control families for Simple Standard #1

Family abbreviation	Family name
2	Observability
9	Session management

3.1.2 Controls

3.1.2.1 Control 2.1: Central audit facility

The information system sends security events from every source system to a central facility for analysis.

3.1.2.2 Control 9.5: Idle timeout

The information system must disconnect sessions after 15 minutes of inactivity.

3.2 NIST SP 800-53 Revision 4

3.2.1 Families

NIST SP 800-53 Revision 4 categorizes controls into logical groups called families.

Table 3.2: Control families for NIST SP 800-53 Revision 4

Family abbreviation	Family name
AC	Access Control
AU	Audit and Accountability

Family abbreviation	Family name
AT	Awareness and Training
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PS	Personnel Security
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
RA	Risk Assessment
CA	Security Assessment and Authorization
SC	System and Communications Protection
SI	System and Information Integrity
SA	System and Services Acquisition

3.2.2 Controls

3.2.2.1 Control AC-1: 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; and

b. Reviews and updates the current:

    1. Access control policy [Assignment: organization-defined frequency]; and
    2. Access control procedures [Assignment: organization-defined frequency].

3.2.2.2 Control AC-2: Account Management

The organization:

a. Identifies and selects 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. 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.

3.2.2.3 Control AC-2 (1): Automated System Account Management

The organization employs automated mechanisms to support the management of information system accounts.

3.2.2.4 Control AC-2 (2): Removal Of Temporary / Emergency Accounts

The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

3.2.2.5 Control AC-2 (3): Disable Inactive Accounts

The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

3.2.2.6 Control AC-2 (4): Automated Audit Actions

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

3.2.2.7 Control AC-2 (5): Inactivity Logout

The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].

3.2.2.8 Control AC-2 (6): Dynamic Privilege Management

The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities].

3.2.2.9 Control AC-2 (7): Role-Based Schemes

The organization: (7)(a). Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (7)(b). Monitors privileged role assignments; and (7)(c). Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.

3.2.2.10 Control AC-2 (8): Dynamic Account Creation

The information system creates [Assignment: organization-defined information system accounts] dynamically.

3.2.2.11 Control AC-2 (9): Restrictions On Use Of Shared / Group Accounts

The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].

3.2.2.12 Control AC-2 (10): Shared / Group Account Credential Termination

The information system terminates shared/group account credentials when members leave the group.

3.2.2.13 Control AC-2 (11): Usage Conditions

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

3.2.2.14 Control AC-2 (12): Account Monitoring / Atypical Usage

The organization: (12)(a). Monitors information system accounts for [Assignment: organization-defined atypical usage]; and (12)(b). Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].

3.2.2.15 Control AC-2 (13): Disable Accounts For High-Risk Individuals

The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.

3.2.2.16 Control AC-3: Access Enforcement

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

3.2.2.17 Control AC-3 (1): Restricted Access To Privileged Functions

[Withdrawn: Incorporated into AC-6].

3.2.2.18 Control AC-3 (2): Dual Authorization

The information system enforces dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].

3.2.2.19 Control AC-3 (3): Mandatory Access Control

The information system enforces [Assignment: organization-defined mandatory access control policy] over all subjects and objects where the policy: (3)(a). Is uniformly enforced across all subjects and objects within the boundary of the information system; (3)(b). Specifies that a subject that has been granted access to information is constrained from doing any of the following; (3)(b)(1). Passing the information to unauthorized subjects or objects; (3)(b)(2). Granting its privileges to other subjects; (3)(b)(3). Changing one or more security attributes on subjects, objects, the information system, or information system components; (3)(b)(4). Choosing the security attributes and attribute values to be associated with newly created or modified objects; or (3)(b)(5). Changing the rules governing access control; and (3)(c). Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges (i.e., they are trusted subjects)] such that they are not limited by some or all of the above constraints.

3.2.2.20 Control AC-3 (4): Discretionary Access Control

The information system enforces [Assignment: organization-defined discretionary access control policy] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following: (4)(a). Pass the information to any other subjects or objects; (4)(b). Grant its privileges to other subjects; (4)(c). Change security attributes on subjects, objects, the information system, or the information system's components; (4)(d). Choose the security attributes to be associated with newly created or revised objects; or (4)(e). Change the rules governing access control.

3.2.2.21 Control AC-3 (5): Security-Relevant Information

The information system prevents access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.

3.2.2.22 Control AC-3 (6): Protection Of User And System Information

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

3.2.2.23 Control AC-3 (7): Role-Based Access Control

The information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [Assignment: organization-defined roles and users authorized to assume such roles].

3.2.2.24 Control AC-3 (8): Revocation Of Access Authorizations

The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].

3.2.2.25 Control AC-3 (9): Controlled Release

The information system does not release information outside of the established system boundary unless: (9)(a). The receiving [Assignment: organization-defined information system or system component] provides [Assignment: organization-defined security safeguards]; and (9)(b). [Assignment: organization-defined security safeguards] are used to validate the appropriateness of the information designated for release.

3.2.2.26 Control AC-3 (10): Audited Override Of Access Control Mechanisms

The organization employs an audited override of automated access control mechanisms under [Assignment: organization-defined conditions].

3.2.2.27 Control AC-4: 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].

3.2.2.28 Control AC-4 (1): Object Security Attributes

The information system uses [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.

3.2.2.29 Control AC-4 (2): Processing Domains

The information system uses protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.

3.2.2.30 Control AC-4 (3): Dynamic Information Flow Control

The information system enforces dynamic information flow control based on [Assignment: organization-defined policies].

3.2.2.31 Control AC-4 (4): Content Check Encrypted Information

The information system prevents encrypted information from bypassing content-checking mechanisms by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].

3.2.2.32 Control AC-4 (5): Embedded Data Types

The information system enforces [Assignment: organization-defined limitations] on embedding data types within other data types.

3.2.2.33 Control AC-4 (6): Metadata

The information system enforces information flow control based on [Assignment: organization-defined metadata].

3.2.2.34 Control AC-4 (7): One-Way Flow Mechanisms

The information system enforces [Assignment: organization-defined one-way information flows] using hardware mechanisms.

3.2.2.35 Control AC-4 (8): Security Policy Filters

The information system enforces information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows].

3.2.2.36 Control AC-4 (9): Human Reviews

The information system enforces the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].

3.2.2.37 Control AC-4 (10): Enable / Disable Security Policy Filters

The information system provides the capability for privileged administrators to enable/disable [Assignment: organization-defined security policy filters] under the following conditions: [Assignment: organization-defined conditions].

3.2.2.38 Control AC-4 (11): Configuration Of Security Policy Filters

The information system provides the capability for privileged administrators to configure [Assignment: organization-defined security policy filters] to support different security policies.

3.2.2.39 Control AC-4 (12): Data Type Identifiers

The information system, when transferring information between different security domains, uses [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.

3.2.2.40 Control AC-4 (13): Decomposition Into Policy-Relevant Subcomponents

The information system, when transferring information between different security domains, decomposes information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.

3.2.2.41 Control AC-4 (14): Security Policy Filter Constraints

The information system, when transferring information between different security domains, implements [Assignment: organization-defined security policy filters] requiring fully enumerated formats that restrict data structure and content.

3.2.2.42 Control AC-4 (15): Detection Of Unsanctioned Information

The information system, when transferring information between different security domains, examines the information for the presence of [Assignment: organized-defined unsanctioned information] and prohibits the transfer of such information in accordance with the [Assignment: organization-defined security policy].

3.2.2.43 Control AC-4 (16): Information Transfers On Interconnected Systems

[Withdrawn: Incorporated into AC-4].

3.2.2.44 Control AC-4 (17): Domain Authentication

The information system uniquely identifies and authenticates source and destination points by [Selection (one or more): organization, system, application, individual] for information transfer.

3.2.2.45 Control AC-4 (18): Security Attribute Binding

The information system binds security attributes to information using [Assignment: organization-defined binding techniques] to facilitate information flow policy enforcement.

3.2.2.46 Control AC-4 (19): Validation Of Metadata

The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.

3.2.2.47 Control AC-4 (20): Approved Solutions

The organization employs [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.

3.2.2.48 Control AC-4 (21): Physical / Logical Separation Of Information Flows

The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

3.2.2.49 Control AC-4 (22): Access Only

The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

3.2.2.50 Control AC-5: 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.

3.2.2.51 Control AC-6: Least Privilege

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

3.2.2.52 Control AC-6 (1): Authorize Access To Security Functions

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

3.2.2.53 Control AC-6 (2): Non-Privileged Access For Nonsecurity Functions

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 nonsecurity functions.

3.2.2.54 Control AC-6 (3): Network Access To Privileged Commands

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.

3.2.2.55 Control AC-6 (4): Separate Processing Domains

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

3.2.2.56 Control AC-6 (5): Privileged Accounts

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

3.2.2.57 Control AC-6 (6): Privileged Access By Non-Organizational Users

The organization prohibits privileged access to the information system by non-organizational users.

3.2.2.58 Control AC-6 (7): Review Of User Privileges

The organization: (7)(a). Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (7)(b). Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

3.2.2.59 Control AC-6 (8): Privilege Levels For Code Execution

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

3.2.2.60 Control AC-6 (9): Auditing Use Of Privileged Functions

The information system audits the execution of privileged functions.

3.2.2.61 Control AC-6 (10): Prohibit Non-Privileged Users From Executing Privileged Functions

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

3.2.2.62 Control AC-7: 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.

3.2.2.63 Control AC-7 (1): Automatic Account Lock

[Withdrawn: Incorporated into AC-7].

3.2.2.64 Control AC-7 (2): Purge / Wipe Mobile Device

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

3.2.2.65 Control AC-8: 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 system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.

3.2.2.66 Control AC-9: Previous Logon (Access) Notification

The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

3.2.2.67 Control AC-9 (1): Unsuccessful Logons

The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

3.2.2.68 Control AC-9 (2): Successful / Unsuccessful Logons

The information system notifies the user of the number of [Selection: successful logons/accesses; unsuccessful logon/access attempts; both] during [Assignment: organization-defined time period].

3.2.2.69 Control AC-9 (3): Notification Of Account Changes

The information system notifies the user of changes to [Assignment: organization-defined security-related characteristics/parameters of the users account] during [Assignment: organization-defined time period].

3.2.2.70 Control AC-9 (4): Additional Logon Information

The information system notifies the user, upon successful logon (access), of the following additional information: [Assignment: organization-defined information to be included in addition to the date and time of the last logon (access)].

3.2.2.71 Control AC-10: 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].

3.2.2.72 Control AC-11: 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.

3.2.2.73 Control AC-11 (1): Pattern-Hiding Displays

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

3.2.2.74 Control AC-12: Session Termination

The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

3.2.2.75 Control AC-12 (1): User-Initiated Logouts / Message Displays

The information system: (1)(a). Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and (1)(b). Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

3.2.2.76 Control AC-13: Supervision And Review - Access Control

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

3.2.2.77 Control AC-14: 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.

3.2.2.78 Control AC-14 (1): Necessary Uses

[Withdrawn: Incorporated into AC-14].

3.2.2.79 Control AC-15: Automated Marking

[Withdrawn: Incorporated into MP-3].

3.2.2.80 Control AC-16: Security Attributes

The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission; b. Ensures that the security attribute associations are made and retained with the information; c. Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and d. Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.

3.2.2.81 Control AC-16 (1): Dynamic Attribute Association

The information system dynamically associates security attributes with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies] as information is created and combined.

3.2.2.82 Control AC-16 (2): Attribute Value Changes By Authorized Individuals

The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security attributes.

3.2.2.83 Control AC-16 (3): Maintenance Of Attribute Associations By Information System

The information system maintains the association and integrity of [Assignment: organization-defined security attributes] to [Assignment: organization-defined subjects and objects].

3.2.2.84 Control AC-16 (4): Association Of Attributes By Authorized Individuals

The information system supports the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).

3.2.2.85 Control AC-16 (5): Attribute Displays For Output Devices

The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-identified special dissemination, handling, or distribution instructions] using [Assignment: organization-identified human-readable, standard naming conventions].

3.2.2.86 Control AC-16 (6): Maintenance Of Attribute Association By Organization

The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security policies].

3.2.2.87 Control AC-16 (7): Consistent Attribute Interpretation

The organization provides a consistent interpretation of security attributes transmitted between distributed information system components.

3.2.2.88 Control AC-16 (8): Association Techniques / Technologies

The information system implements [Assignment: organization-defined techniques or technologies] with [Assignment: organization-defined level of assurance] in associating security attributes to information.

3.2.2.89 Control AC-16 (9): Attribute Reassignment

The organization ensures that security attributes associated with information are reassigned only via re-grading mechanisms validated using [Assignment: organization-defined techniques or procedures].

3.2.2.90 Control AC-16 (10): Attribute Configuration By Authorized Individuals

The information system provides authorized individuals the capability to define or change the type and value of security attributes available for association with subjects and objects.

3.2.2.91 Control AC-17: Remote Access

The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

3.2.2.92 Control AC-17 (1): Automated Monitoring / Control

The information system monitors and controls remote access methods.

3.2.2.93 Control AC-17 (2): Protection Of Confidentiality / Integrity Using Encryption

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

3.2.2.94 Control AC-17 (3): Managed Access Control Points

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

3.2.2.95 Control AC-17 (4): Privileged Commands / Access

The organization: (4)(a). Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (4)(b). Documents the rationale for such access in the security plan for the information system.

3.2.2.96 Control AC-17 (5): Monitoring For Unauthorized Connections

[Withdrawn: Incorporated into SI-4].

3.2.2.97 Control AC-17 (6): Protection Of Information

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

3.2.2.98 Control AC-17 (7): Additional Protection For Security Function Access

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

3.2.2.99 Control AC-17 (8): Disable Nonsecure Network Protocols

[Withdrawn: Incorporated into CM-7].

3.2.2.100 Control AC-17 (9): Disconnect / Disable Access

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period].

3.2.2.101 Control AC-18: 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.

3.2.2.102 Control AC-18 (1): Authentication And Encryption

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

3.2.2.103 Control AC-18 (2): Monitoring Unauthorized Connections

[Withdrawn: Incorporated into SI-4].

3.2.2.104 Control AC-18 (3): Disable Wireless Networking

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

3.2.2.105 Control AC-18 (4): Restrict Configurations By Users

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

3.2.2.106 Control AC-18 (5): Antennas / Transmission Power Levels

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

3.2.2.107 Control AC-19: Access Control For Mobile Devices

The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.

3.2.2.108 Control AC-19 (1): Use Of Writable / Portable Storage Devices

[Withdrawn: Incorporated into MP-7].

3.2.2.109 Control AC-19 (2): Use Of Personally Owned Portable Storage Devices

[Withdrawn: Incorporated into MP-7].

3.2.2.110 Control AC-19 (3): Use Of Portable Storage Devices With No Identifiable Owner

[Withdrawn: Incorporated into MP-7].

3.2.2.111 Control AC-19 (4): Restrictions For Classified Information

The organization: (4)(a). Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and (4)(b). Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information: (4)(b)(1). Connection of unclassified mobile devices to classified information systems is prohibited; (4)(b)(2). Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official; (4)(b)(3). Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and (4)(b)(4). Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed. (4)(c). Restricts the connection of classified mobile devices to classified information systems in accordance with [Assignment: organization-defined security policies].

3.2.2.112 Control AC-19 (5): Full Device / Container-Based Encryption

The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

3.2.2.113 Control AC-20: 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.

3.2.2.114 Control AC-20 (1): Limits On Authorized Use

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (1)(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 (1)(b). Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

3.2.2.115 Control AC-20 (2): Portable Storage Devices

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

3.2.2.116 Control AC-20 (3): Non-Organizationally Owned Systems / Components / Devices

The organization [Selection: restricts; prohibits] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

3.2.2.117 Control AC-20 (4): Network Accessible Storage Devices

The organization prohibits the use of [Assignment: organization-defined network accessible storage devices] in external information systems.

3.2.2.118 Control AC-21: 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.

3.2.2.119 Control AC-21 (1): Automated Decision Support

The information system enforces information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

3.2.2.120 Control AC-21 (2): Information Search And Retrieval

The information system implements information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].

3.2.2.121 Control AC-22: 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.

3.2.2.122 Control AC-23: Data Mining Protection

The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.

3.2.2.123 Control AC-24: Access Control Decisions

The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

3.2.2.124 Control AC-24 (1): Transmit Access Authorization Information

The information system transmits [Assignment: organization-defined access authorization information] using [Assignment: organization-defined security safeguards] to [Assignment: organization-defined information systems] that enforce access control decisions.

3.2.2.125 Control AC-24 (2): No User Or Process Identity

The information system enforces access control decisions based on [Assignment: organization-defined security attributes] that do not include the identity of the user or process acting on behalf of the user.

3.2.2.126 Control AC-25: Reference Monitor

The information system implements a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

3.2.2.127 Control AT-1: 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].

3.2.2.128 Control AT-2: Security Awareness Training

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.

3.2.2.129 Control AT-2 (1): Practical Exercises

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

3.2.2.130 Control AT-2 (2): Insider Threat

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

3.2.2.131 Control AT-3: Role-Based Security Training

The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.

3.2.2.132 Control AT-3 (1): Environmental Controls

The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.

3.2.2.133 Control AT-3 (2): Physical Security Controls

The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.

3.2.2.134 Control AT-3 (3): Practical Exercises

The organization includes practical exercises in security training that reinforce training objectives.

3.2.2.135 Control AT-3 (4): Suspicious Communications And Anomalous System Behavior

The organization provides training to its personnel on [Assignment: organization-defined indicators of malicious code] to recognize suspicious communications and anomalous behavior in organizational information systems.

3.2.2.136 Control AT-4: 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].

3.2.2.137 Control AT-5: Contacts With Security Groups And Associations

[Withdrawn: Incorporated into PM-15].

3.2.2.138 Control AU-1: 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].

3.2.2.139 Control AU-2: Audit Events

The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined 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 auditable events are deemed to be adequate to support after-the-fact investigations of security

incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

3.2.2.140 Control AU-2 (1): Compilation Of Audit Records From Multiple Sources

[Withdrawn: Incorporated into AU-12].

3.2.2.141 Control AU-2 (2): Selection Of Audit Events By Component

[Withdrawn: Incorporated into AU-12].

3.2.2.142 Control AU-2 (3): Reviews And Updates

The organization reviews and updates the audited events [Assignment: organization-defined frequency].

3.2.2.143 Control AU-2 (4): Privileged Functions

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

3.2.2.144 Control AU-3: 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.

3.2.2.145 Control AU-3 (1): Additional Audit Information

The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].

3.2.2.146 Control AU-3 (2): Centralized Management Of Planned Audit Record Content

The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].

3.2.2.147 Control AU-4: Audit Storage Capacity

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

3.2.2.148 Control AU-4 (1): Transfer To Alternate Storage

The information system off-loads audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.

3.2.2.149 Control AU-5: 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)].

3.2.2.150 Control AU-5 (1): Audit Storage Capacity

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.

3.2.2.151 Control AU-5 (2): Real-Time Alerts

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].

3.2.2.152 Control AU-5 (3): Configurable Traffic Volume Thresholds

The information system enforces configurable network communications traffic volume thresholds reflecting limits on auditing capacity and [Selection: rejects; delays] network traffic above those thresholds.

3.2.2.153 Control AU-5 (4): Shutdown On Failure

The information system invokes a [Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available] in the event of [Assignment: organization-defined audit failures], unless an alternate audit capability exists.

3.2.2.154 Control AU-6: 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].

3.2.2.155 Control AU-6 (1): Process Integration

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

3.2.2.156 Control AU-6 (2): Automated Security Alerts

[Withdrawn: Incorporated into SI-4].

3.2.2.157 Control AU-6 (3): Correlate Audit Repositories

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

3.2.2.158 Control AU-6 (4): Central Review And Analysis

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

3.2.2.159 Control AU-6 (5): Integration / Scanning And Monitoring Capabilities

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.

3.2.2.160 Control AU-6 (6): Correlation With Physical Monitoring

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

3.2.2.161 Control AU-6 (7): Permitted Actions

The organization specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information.

3.2.2.162 Control AU-6 (8): Full Text Analysis Of Privileged Commands

The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.

3.2.2.163 Control AU-6 (9): Correlation With Information From Nontechnical Sources

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

3.2.2.164 Control AU-6 (10): Audit Level Adjustment

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

3.2.2.165 Control AU-7: 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.

3.2.2.166 Control AU-7 (1): Automatic Processing

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

3.2.2.167 Control AU-7 (2): Automatic Sort And Search

The information system provides the capability to sort and search audit records for events of interest based on the content of [Assignment: organization-defined audit fields within audit records].

3.2.2.168 Control AU-8: Time Stamps

The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

3.2.2.169 Control AU-8 (1): Synchronization With Authoritative Time Source

The information system: (1)(a). Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (1)(b). Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

3.2.2.170 Control AU-8 (2): Secondary Authoritative Time Source

The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

3.2.2.171 Control AU-9: Protection Of Audit Information

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

3.2.2.172 Control AU-9 (1): Hardware Write-Once Media

The information system writes audit trails to hardware-enforced, write-once media.

3.2.2.173 Control AU-9 (2): Audit Backup On Separate Physical Systems / Components

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.

3.2.2.174 Control AU-9 (3): Cryptographic Protection

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

3.2.2.175 Control AU-9 (4): Access By Subset Of Privileged Users

The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].

3.2.2.176 Control AU-9 (5): Dual Authorization

The organization enforces dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].

3.2.2.177 Control AU-9 (6): Read Only Access

The organization authorizes read-only access to audit information to [Assignment: organization-defined subset of privileged users].

3.2.2.178 Control AU-10: Non-Repudiation

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].

3.2.2.179 Control AU-10 (1): Association Of Identities

The information system: (1)(a). Binds the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; and (1)(b). Provides the means for authorized individuals to determine the identity of the producer of the information.

3.2.2.180 Control AU-10 (2): Validate Binding Of Information Producer Identity

The information system: (2)(a). Validates the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and (2)(b). Performs [Assignment: organization-defined actions] in the event of a validation error.

3.2.2.181 Control AU-10 (3): Chain Of Custody

The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

3.2.2.182 Control AU-10 (4): Validate Binding Of Information Reviewer Identity

The information system: (4)(a). Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [Assignment: organization-defined security domains]; and (4)(b). Performs [Assignment: organization-defined actions] in the event of a validation error.

3.2.2.183 Control AU-10 (5): Digital Signatures

[Withdrawn: Incorporated into SI-7].

3.2.2.184 Control AU-11: 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.

3.2.2.185 Control AU-11 (1): Long-Term Retrieval Capability

The organization employs [Assignment: organization-defined measures] to ensure that long-term audit records generated by the information system can be retrieved.

3.2.2.186 Control AU-12: 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.

3.2.2.187 Control AU-12 (1): System-Wide / Time-Correlated Audit Trail

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 the relationship between time stamps of individual records in the audit trail].

3.2.2.188 Control AU-12 (2): Standardized Formats

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

3.2.2.189 Control AU-12 (3): Changes By Authorized Individuals

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].

3.2.2.190 Control AU-13: Monitoring For Information Disclosure

The organization monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.

3.2.2.191 Control AU-13 (1): Use Of Automated Tools

The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.

3.2.2.192 Control AU-13 (2): Review Of Monitored Sites

The organization reviews the open source information sites being monitored [Assignment: organization-defined frequency].

3.2.2.193 Control AU-14: Session Audit

The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

3.2.2.194 Control AU-14 (1): System Start-Up

The information system initiates session audits at system start-up.

3.2.2.195 Control AU-14 (2): Capture/Record And Log Content

The information system provides the capability for authorized users to capture/record and log content related to a user session.

3.2.2.196 Control AU-14 (3): Remote Viewing / Listening

The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.

3.2.2.197 Control AU-15: Alternate Audit Capability

The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [Assignment: organization-defined alternate audit functionality].

3.2.2.198 Control AU-16: Cross-Organizational Auditing

The organization employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

3.2.2.199 Control AU-16 (1): Identity Preservation

The organization requires that the identity of individuals be preserved in cross-organizational audit trails.

3.2.2.200 Control AU-16 (2): Sharing Of Audit Information

The organization provides cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].

3.2.2.201 Control CA-1: Security Assessment And Authorization Policy 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].

3.2.2.202 Control CA-2: 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].

3.2.2.203 Control CA-2 (1): Independent Assessors

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.

3.2.2.204 Control CA-2 (2): Specialized 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]].

3.2.2.205 Control CA-2 (3): External Organizations

The organization accepts the results of an assessment of [Assignment: organization-defined information system] performed by [Assignment: organization-defined external organization] when the assessment meets [Assignment: organization-defined requirements].

3.2.2.206 Control CA-3: System Interconnections

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].

3.2.2.207 Control CA-3 (1): Unclassified National Security System Connections

The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].

3.2.2.208 Control CA-3 (2): Classified National Security System Connections

The organization prohibits the direct connection of a classified, national security system to an external network without the use of [Assignment: organization-defined boundary protection device].

3.2.2.209 Control CA-3 (3): Unclassified Non-National Security System Connections

The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [Assignment; organization-defined boundary protection device].

3.2.2.210 Control CA-3 (4): Connections To Public Networks

The organization prohibits the direct connection of an [Assignment: organization-defined information system] to a public network.

3.2.2.211 Control CA-3 (5): Restrictions On External 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.

3.2.2.212 Control CA-4: Security Certification

[Withdrawn: Incorporated into CA-2].

3.2.2.213 Control CA-5: 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.

3.2.2.214 Control CA-5 (1): Automation Support For Accuracy / Currency

The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

3.2.2.215 Control CA-6: Security Authorization

The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].

3.2.2.216 Control CA-7: 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].

3.2.2.217 Control CA-7 (1): Independent Assessment

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.

3.2.2.218 Control CA-7 (2): Types Of Assessments

[Withdrawn: Incorporated into CA-2].

3.2.2.219 Control CA-7 (3): Trend Analyses

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

3.2.2.220 Control CA-8: Penetration Testing

The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

3.2.2.221 Control CA-8 (1): Independent Penetration Agent Or Team

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

3.2.2.222 Control CA-8 (2): Red Team Exercises

The organization employs [Assignment: organization-defined red team exercises] to simulate attempts by adversaries to compromise organizational information systems in accordance with [Assignment: organization-defined rules of engagement].

3.2.2.223 Control CA-9: 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.

3.2.2.224 Control CA-9 (1): Security Compliance Checks

The information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.

3.2.2.225 Control CM-1: 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].

3.2.2.226 Control CM-2: Baseline Configuration

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

3.2.2.227 Control CM-2 (1): Reviews And Updates

The organization reviews and updates the baseline configuration of the information system: (1)(a). [Assignment: organization-defined frequency]; (1)(b). When required due to [Assignment organization-defined circumstances]; and (1)(c). As an integral part of information system component installations and upgrades.

3.2.2.228 Control CM-2 (2): Automation Support For Accuracy / Currency

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

3.2.2.229 Control CM-2 (3): Retention Of Previous Configurations

The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.

3.2.2.230 Control CM-2 (4): Unauthorized Software

[Withdrawn: Incorporated into CM-7].

3.2.2.231 Control CM-2 (5): Authorized Software

[Withdrawn: Incorporated into CM-7].

3.2.2.232 Control CM-2 (6): Development And Test Environments

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

3.2.2.233 Control CM-2 (7): Configure Systems, Components, Or Devices For High-Risk Areas

The organization: (7)(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 (7)(b). Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

3.2.2.234 Control CM-3: 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]].

3.2.2.235 Control CM-3 (1): Automated Document / Notification / Prohibition Of Changes

The organization employs automated mechanisms to: (1)(a). Document proposed changes to the information system; (1)(b). Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (1)(c). Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period]; (1)(d). Prohibit changes to the information system until designated approvals are received; (1)(e). Document all changes to the information system; and (1)(f). Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.

3.2.2.236 Control CM-3 (2): Test / Validate / Document Changes

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

3.2.2.237 Control CM-3 (3): Automated Change Implementation

The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.

3.2.2.238 Control CM-3 (4): Security Representative

The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].

3.2.2.239 Control CM-3 (5): Automated Security Response

The information system implements [Assignment: organization-defined security responses] automatically if baseline configurations are changed in an unauthorized manner.

3.2.2.240 Control CM-3 (6): Cryptography Management

The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management.

3.2.2.241 Control CM-4: Security Impact Analysis

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

3.2.2.242 Control CM-4 (1): Separate Test Environments

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.

3.2.2.243 Control CM-4 (2): Verification Of Security Functions

The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

3.2.2.244 Control CM-5: Access Restrictions For Change

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

3.2.2.245 Control CM-5 (1): Automated Access Enforcement / Auditing

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

3.2.2.246 Control CM-5 (2): Review System Changes

The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.

3.2.2.247 Control CM-5 (3): Signed Components

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.

3.2.2.248 Control CM-5 (4): Dual Authorization

The organization enforces dual authorization for implementing changes to [Assignment: organization-defined information system components and system-level information].

3.2.2.249 Control CM-5 (5): Limit Production / Operational Privileges

The organization: (5)(a). Limits privileges to change information system components and system-related information within a production or operational environment; and (5)(b). Reviews and reevaluates privileges [Assignment: organization-defined frequency].

3.2.2.250 Control CM-5 (6): Limit Library Privileges

The organization limits privileges to change software resident within software libraries.

3.2.2.251 Control CM-5 (7): Automatic Implementation Of Security Safeguards

[Withdrawn: Incorporated into SI-7].

3.2.2.252 Control CM-6: 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.

3.2.2.253 Control CM-6 (1): Automated Central Management / Application / Verification

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].

3.2.2.254 Control CM-6 (2): Respond To Unauthorized Changes

The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].

3.2.2.255 Control CM-6 (3): Unauthorized Change Detection

[Withdrawn: Incorporated into SI-7].

3.2.2.256 Control CM-6 (4): Conformance Demonstration

[Withdrawn: Incorporated into CM-4].

3.2.2.257 Control CM-7: 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].

3.2.2.258 Control CM-7 (1): Periodic Review

The organization: (1)(a). Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (1)(b). Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].

3.2.2.259 Control CM-7 (2): Prevent Program Execution

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].

3.2.2.260 Control CM-7 (3): Registration Compliance

The organization ensures compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].

3.2.2.261 Control CM-7 (4): Unauthorized Software / Blacklisting

The organization: (4)(a). Identifies [Assignment: organization-defined software programs not authorized to execute on the information system]; (4)(b). Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (4)(c). Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].

3.2.2.262 Control CM-7 (5): Authorized Software / Whitelisting

The organization: (5)(a). Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (5)(b). Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (5)(c). Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency].

3.2.2.263 Control CM-8: 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].

3.2.2.264 Control CM-8 (1): Updates During Installations / Removals

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

3.2.2.265 Control CM-8 (2): Automated Maintenance

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

3.2.2.266 Control CM-8 (3): Automated Unauthorized Component Detection

The organization: (3)(a). Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (3)(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]].

3.2.2.267 Control CM-8 (4): Accountability Information

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.

3.2.2.268 Control CM-8 (5): No Duplicate Accounting Of Components

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

3.2.2.269 Control CM-8 (6): Assessed Configurations / Approved Deviations

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

3.2.2.270 Control CM-8 (7): Centralized Repository

The organization provides a centralized repository for the inventory of information system components.

3.2.2.271 Control CM-8 (8): Automated Location Tracking

The organization employs automated mechanisms to support tracking of information system components by geographic location.

3.2.2.272 Control CM-8 (9): Assignment Of Components To Systems

The organization: (9)(a). Assigns [Assignment: organization-defined acquired information system components] to an information system; and (9)(b). Receives an acknowledgement from the information system owner of this assignment.

3.2.2.273 Control CM-9: 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.

3.2.2.274 Control CM-9 (1): Assignment Of Responsibility

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

3.2.2.275 Control CM-10: 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.

3.2.2.276 Control CM-10 (1): Open Source Software

The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].

3.2.2.277 Control CM-11: 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].

3.2.2.278 Control CM-11 (1): Alerts For Unauthorized Installations

The information system alerts [Assignment: organization-defined personnel or roles] when the unauthorized installation of software is detected.

3.2.2.279 Control CM-11 (2): Prohibit Installation Without Privileged Status

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

3.2.2.280 Control CP-1: 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].

3.2.2.281 Control CP-2: 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.

3.2.2.282 Control CP-2 (1): Coordinate With Related Plans

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

3.2.2.283 Control CP-2 (2): Capacity Planning

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

3.2.2.284 Control CP-2 (3): Resume Essential Missions / Business Functions

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

3.2.2.285 Control CP-2 (4): Resume All Missions / Business Functions

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

3.2.2.286 Control CP-2 (5): Continue Essential Missions / Business Functions

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.

3.2.2.287 Control CP-2 (6): Alternate Processing / Storage Site

The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.

3.2.2.288 Control CP-2 (7): Coordinate With External Service Providers

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

3.2.2.289 Control CP-2 (8): Identify Critical Assets

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

3.2.2.290 Control CP-3: 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.

3.2.2.291 Control CP-3 (1): Simulated Events

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

3.2.2.292 Control CP-3 (2): Automated Training Environments

The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.

3.2.2.293 Control CP-4: Contingency Plan Testing

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.

3.2.2.294 Control CP-4 (1): Coordinate With Related Plans

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

3.2.2.295 Control CP-4 (2): Alternate Processing Site

The organization tests the contingency plan at the alternate processing site: (2)(a). To familiarize contingency personnel with the facility and available resources; and (2)(b). To evaluate the capabilities of the alternate processing site to support contingency operations.

3.2.2.296 Control CP-4 (3): Automated Testing

The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

3.2.2.297 Control CP-4 (4): Full Recovery / Reconstitution

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

3.2.2.298 Control CP-5: Contingency Plan Update

[Withdrawn: Incorporated into CP-2].

3.2.2.299 Control CP-6: 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.

3.2.2.300 Control CP-6 (1): Separation From Primary Site

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

3.2.2.301 Control CP-6 (2): Recovery Time / Point Objectives

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

3.2.2.302 Control CP-6 (3): Accessibility

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

3.2.2.303 Control CP-7: 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 those of the primary site.

3.2.2.304 Control CP-7 (1): Separation From Primary Site

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

3.2.2.305 Control CP-7 (2): Accessibility

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

3.2.2.306 Control CP-7 (3): Priority Of Service

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

3.2.2.307 Control CP-7 (4): Preparation For Use

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

3.2.2.308 Control CP-7 (5): Equivalent Information Security Safeguards

[Withdrawn: Incorporated into CP-7].

3.2.2.309 Control CP-7 (6): Inability To Return To Primary Site

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

3.2.2.310 Control CP-8: 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.

3.2.2.311 Control CP-8 (1): Priority Of Service Provisions

The organization: (1)(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 (1)(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.

3.2.2.312 Control CP-8 (2): Single Points Of Failure

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

3.2.2.313 Control CP-8 (3): Separation Of Primary / Alternate Providers

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

3.2.2.314 Control CP-8 (4): Provider Contingency Plan

The organization: (4)(a). Requires primary and alternate telecommunications service providers to have contingency plans; (4)(b). Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and (4)(c). Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency].

3.2.2.315 Control CP-8 (5): Alternate Telecommunication Service Testing

The organization tests alternate telecommunication services [Assignment: organization-defined frequency].

3.2.2.316 Control CP-9: 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.

3.2.2.317 Control CP-9 (1): Testing For Reliability / Integrity

The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.

3.2.2.318 Control CP-9 (2): Test Restoration Using Sampling

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

3.2.2.319 Control CP-9 (3): Separate Storage For Critical Information

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.

3.2.2.320 Control CP-9 (4): Protection From Unauthorized Modification

[Withdrawn: Incorporated into CP-9].

3.2.2.321 Control CP-9 (5): Transfer To Alternate Storage Site

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].

3.2.2.322 Control CP-9 (6): Redundant Secondary System

The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

3.2.2.323 Control CP-9 (7): Dual Authorization

The organization enforces dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].

3.2.2.324 Control CP-10: 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.

3.2.2.325 Control CP-10 (1): Contingency Plan Testing

[Withdrawn: Incorporated into CP-4].

3.2.2.326 Control CP-10 (2): Transaction Recovery

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

3.2.2.327 Control CP-10 (3): Compensating Security Controls

[Withdrawn: Addressed through tailoring procedures].

3.2.2.328 Control CP-10 (4): Restore Within Time Period

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.

3.2.2.329 Control CP-10 (5): Failover Capability

[Withdrawn: Incorporated into SI-13].

3.2.2.330 Control CP-10 (6): Component Protection

The organization protects backup and restoration hardware, firmware, and software.

3.2.2.331 Control CP-11: Alternate Communications Protocols

The information system provides the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

3.2.2.332 Control CP-12: Safe Mode

The information system, when [Assignment: organization-defined conditions] are detected, enters a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

3.2.2.333 Control CP-13: Alternative Security Mechanisms

The organization employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

3.2.2.334 Control IA-1: 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].

3.2.2.335 Control IA-2: Identification And Authentication (Organizational Users)

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

3.2.2.336 Control IA-2 (1): Network Access To Privileged Accounts

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

3.2.2.337 Control IA-2 (2): Network Access To Non-Privileged Accounts

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

3.2.2.338 Control IA-2 (3): Local Access To Privileged Accounts

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

3.2.2.339 Control IA-2 (4): Local Access To Non-Privileged Accounts

The information system implements multifactor authentication for local access to non-privileged accounts.

3.2.2.340 Control IA-2 (5): Group Authentication

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

3.2.2.341 Control IA-2 (6): Network Access To Privileged Accounts - Separate Device

The information system implements multifactor authentication for network access to 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].

3.2.2.342 Control IA-2 (7): Network Access To Non-Privileged Accounts - Separate Device

The information system implements multifactor authentication for network access to 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].

3.2.2.343 Control IA-2 (8): Network Access To Privileged Accounts - Replay Resistant

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

3.2.2.344 Control IA-2 (9): Network Access To Non-Privileged Accounts - Replay Resistant

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

3.2.2.345 Control IA-2 (10): Single Sign-On

The information system provides a single sign-on capability for [Assignment: organization-defined information system accounts and services].

3.2.2.346 Control IA-2 (11): Remote Access - Separate Device

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].

3.2.2.347 Control IA-2 (12): Acceptance Of Piv Credentials

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

3.2.2.348 Control IA-2 (13): Out-Of-Band Authentication

The information system implements [Assignment: organization-defined out-of-band authentication] under [Assignment: organization-defined conditions].

3.2.2.349 Control IA-3: 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.

3.2.2.350 Control IA-3 (1): Cryptographic Bidirectional Authentication

The information system authenticates [Assignment: organization-defined specific devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.

3.2.2.351 Control IA-3 (2): Cryptographic Bidirectional Network Authentication

[Withdrawn: Incorporated into IA-3 (1)].

3.2.2.352 Control IA-3 (3): Dynamic Address Allocation

The organization: (3)(a). Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and (3)(b). Audits lease information when assigned to a device.

3.2.2.353 Control IA-3 (4): Device Attestation

The organization ensures that device identification and authentication based on attestation is handled by [Assignment: organization-defined configuration management process].

3.2.2.354 Control IA-4: 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].

3.2.2.355 Control IA-4 (1): Prohibit Account Identifiers As Public Identifiers

The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.

3.2.2.356 Control IA-4 (2): Supervisor Authorization

The organization requires that the registration process to receive an individual identifier includes supervisor authorization.

3.2.2.357 Control IA-4 (3): Multiple Forms Of Certification

The organization requires multiple forms of certification of individual identification be presented to the registration authority.

3.2.2.358 Control IA-4 (4): Identify User Status

The organization manages individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

3.2.2.359 Control IA-4 (5): Dynamic Management

The information system dynamically manages identifiers.

3.2.2.360 Control IA-4 (6): Cross-Organization Management

The organization coordinates with [Assignment: organization-defined external organizations] for cross-organization management of identifiers.

3.2.2.361 Control IA-4 (7): In-Person Registration

The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority.

3.2.2.362 Control IA-5: 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.

3.2.2.363 Control IA-5 (1): Password-Based Authentication

The information system, for password-based authentication: (1)(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]; (1)(b). Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (1)(c). Stores and transmits only cryptographically-protected passwords; (1)(d). Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; (1)(e). Prohibits password reuse for [Assignment: organization-defined number] generations; and (1)(f). Allows the use of a temporary password for system logons with an immediate change to a permanent password.

3.2.2.364 Control IA-5 (2): Pki-Based Authentication

The information system, for PKI-based authentication: (2)(a). Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (2)(b). Enforces authorized access to the corresponding private key; (2)(c). Maps the authenticated identity to the account of the individual or group; and (2)(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.

3.2.2.365 Control IA-5 (3): In-Person Or Trusted Third-Party Registration

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].

3.2.2.366 Control IA-5 (4): Automated Support For Password Strength Determination

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements].

3.2.2.367 Control IA-5 (5): Change Authenticators Prior To Delivery

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

3.2.2.368 Control IA-5 (6): Protection Of Authenticators

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

3.2.2.369 Control IA-5 (7): No Embedded Unencrypted Static Authenticators

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

3.2.2.370 Control IA-5 (8): Multiple Information System Accounts

The organization implements [Assignment: organization-defined security safeguards] to manage the risk of compromise due to individuals having accounts on multiple information systems.

3.2.2.371 Control IA-5 (9): Cross-Organization Credential Management

The organization coordinates with [Assignment: organization-defined external organizations] for cross-organization management of credentials.

3.2.2.372 Control IA-5 (10): Dynamic Credential Association

The information system dynamically provisions identities.

3.2.2.373 Control IA-5 (11): Hardware Token-Based Authentication

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

3.2.2.374 Control IA-5 (12): Biometric-Based Authentication

The information system, for biometric-based authentication, employs mechanisms that satisfy [Assignment: organization-defined biometric quality requirements].

3.2.2.375 Control IA-5 (13): Expiration Of Cached Authenticators

The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].

3.2.2.376 Control IA-5 (14): Managing Content Of Pki Trust Stores

The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

3.2.2.377 Control IA-5 (15): Ficam-Approved Products And Services

The organization uses only FICAM-approved path discovery and validation products and services.

3.2.2.378 Control IA-6: 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.

3.2.2.379 Control IA-7: 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.

3.2.2.380 Control IA-8: 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).

3.2.2.381 Control IA-8 (1): Acceptance Of Piv Credentials From Other Agencies

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

3.2.2.382 Control IA-8 (2): Acceptance Of Third-Party Credentials

The information system accepts only FICAM-approved third-party credentials.

3.2.2.383 Control IA-8 (3): Use Of Ficam-Approved Products

The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

3.2.2.384 Control IA-8 (4): Use Of Ficam-Issued Profiles

The information system conforms to FICAM-issued profiles.

3.2.2.385 Control IA-8 (5): Acceptance Of Piv-I Credentials

The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.

3.2.2.386 Control IA-9: Service Identification And Authentication

The organization identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].

3.2.2.387 Control IA-9 (1): Information Exchange

The organization ensures that service providers receive, validate, and transmit identification and authentication information.

3.2.2.388 Control IA-9 (2): Transmission Of Decisions

The organization ensures that identification and authentication decisions are transmitted between [Assignment: organization-defined services] consistent with organizational policies.

3.2.2.389 Control IA-10: Adaptive Identification And Authentication

The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

3.2.2.390 Control IA-11: Re-Authentication

The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

3.2.2.391 Control IR-1: 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].

3.2.2.392 Control IR-2: 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.

3.2.2.393 Control IR-2 (1): Simulated Events

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

3.2.2.394 Control IR-2 (2): Automated Training Environments

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

3.2.2.395 Control IR-3: Incident Response Testing

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.

3.2.2.396 Control IR-3 (1): Automated Testing

The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

3.2.2.397 Control IR-3 (2): Coordination With Related Plans

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

3.2.2.398 Control IR-4: 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, and implements the resulting changes accordingly.

3.2.2.399 Control IR-4 (1): Automated Incident Handling Processes

The organization employs automated mechanisms to support the incident handling process.

3.2.2.400 Control IR-4 (2): Dynamic Reconfiguration

The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability.

3.2.2.401 Control IR-4 (3): Continuity Of Operations

The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions.

3.2.2.402 Control IR-4 (4): Information Correlation

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

3.2.2.403 Control IR-4 (5): Automatic Disabling Of Information System

The organization implements a configurable capability to automatically disable the information system if [Assignment: organization-defined security violations] are detected.

3.2.2.404 Control IR-4 (6): Insider Threats - Specific Capabilities

The organization implements incident handling capability for insider threats.

3.2.2.405 Control IR-4 (7): Insider Threats - Intra-Organization Coordination

The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].

3.2.2.406 Control IR-4 (8): Correlation With External Organizations

The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.

3.2.2.407 Control IR-4 (9): Dynamic Response Capability

The organization employs [Assignment: organization-defined dynamic response capabilities] to effectively respond to security incidents.

3.2.2.408 Control IR-4 (10): Supply Chain Coordination

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

3.2.2.409 Control IR-5: Incident Monitoring

The organization tracks and documents information system security incidents.

3.2.2.410 Control IR-5 (1): Automated Tracking / Data Collection / Analysis

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

3.2.2.411 Control IR-6: 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].

3.2.2.412 Control IR-6 (1): Automated Reporting

The organization employs automated mechanisms to assist in the reporting of security incidents.

3.2.2.413 Control IR-6 (2): Vulnerabilities Related To Incidents

The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].

3.2.2.414 Control IR-6 (3): Coordination With Supply Chain

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

3.2.2.415 Control IR-7: 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.

3.2.2.416 Control IR-7 (1): Automation Support For Availability Of Information / Support

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

3.2.2.417 Control IR-7 (2): Coordination With External Providers

The organization: (2)(a). Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (2)(b). Identifies organizational incident response team members to the external providers.

3.2.2.418 Control IR-8: 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.

3.2.2.419 Control IR-9: Information Spillage Response

The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [Assignment: organization-defined actions].

3.2.2.420 Control IR-9 (1): Responsible Personnel

The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.

3.2.2.421 Control IR-9 (2): Training

The organization provides information spillage response training [Assignment: organization-defined frequency].

3.2.2.422 Control IR-9 (3): Post-Spill Operations

The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

3.2.2.423 Control IR-9 (4): Exposure To Unauthorized Personnel

The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.

3.2.2.424 Control IR-10: Integrated Information Security Analysis Team

The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

3.2.2.425 Control MA-1: 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].

3.2.2.426 Control MA-2: 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.

3.2.2.427 Control MA-2 (1): Record Content

[Withdrawn: Incorporated into MA-2].

3.2.2.428 Control MA-2 (2): Automated Maintenance Activities

The organization: (2)(a). Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (2)(b). Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

3.2.2.429 Control MA-3: Maintenance Tools

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

3.2.2.430 Control MA-3 (1): Inspect Tools

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

3.2.2.431 Control MA-3 (2): Inspect Media

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

3.2.2.432 Control MA-3 (3): Prevent Unauthorized Removal

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (3)(a). Verifying that there is no organizational information contained on the equipment; (3)(b). Sanitizing or destroying the equipment; (3)(c). Retaining the equipment within the facility; or (3)(d). Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.

3.2.2.433 Control MA-3 (4): Restricted Tool Use

The information system restricts the use of maintenance tools to authorized personnel only.

3.2.2.434 Control MA-4: Nonlocal 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.

3.2.2.435 Control MA-4 (1): Auditing And Review

The organization: (1)(a). Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events]; and (1)(b). Reviews the records of the maintenance and diagnostic sessions.

3.2.2.436 Control MA-4 (2): Document Nonlocal Maintenance

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

3.2.2.437 Control MA-4 (3): Comparable Security / Sanitization

The organization: (3)(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 (3)(b). Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

3.2.2.438 Control MA-4 (4): Authentication / Separation Of Maintenance Sessions

The organization protects nonlocal maintenance sessions by: (4)(a). Employing [Assignment: organization-defined authenticators that are replay resistant]; and (4)(b). Separating the maintenance sessions from other network sessions with the information system by either: (4)(b)(1). Physically separated communications paths; or (4)(b)(2). Logically separated communications paths based upon encryption.

3.2.2.439 Control MA-4 (5): Approvals And Notifications

The organization: (5)(a). Requires the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; and (5)(b). Notifies [Assignment: organization-defined personnel or roles] of the date and time of planned nonlocal maintenance.

3.2.2.440 Control MA-4 (6): Cryptographic Protection

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

3.2.2.441 Control MA-4 (7): Remote Disconnect Verification

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

3.2.2.442 Control MA-5: 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.

3.2.2.443 Control MA-5 (1): Individuals Without Appropriate Access

The organization: (1)(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)(a)(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; (1)(a)(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 (1)(b). Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

3.2.2.444 Control MA-5 (2): Security Clearances For Classified Systems

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

3.2.2.445 Control MA-5 (3): Citizenship Requirements For Classified Systems

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.

3.2.2.446 Control MA-5 (4): Foreign Nationals

The organization ensures that: (4)(a). Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and (4)(b). Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.

3.2.2.447 Control MA-5 (5): Nonsystem-Related Maintenance

The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorizations.

3.2.2.448 Control MA-6: 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.

3.2.2.449 Control MA-6 (1): Preventive Maintenance

The organization performs preventive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals].

3.2.2.450 Control MA-6 (2): Predictive Maintenance

The organization performs predictive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals].

3.2.2.451 Control MA-6 (3): Automated Support For Predictive Maintenance

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

3.2.2.452 Control MP-1: 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].

3.2.2.453 Control MP-2: Media Access

The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

3.2.2.454 Control MP-2 (1): Automated Restricted Access

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

3.2.2.455 Control MP-2 (2): Cryptographic Protection

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

3.2.2.456 Control MP-3: 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].

3.2.2.457 Control MP-4: 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.

3.2.2.458 Control MP-4 (1): Cryptographic Protection

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

3.2.2.459 Control MP-4 (2): Automated Restricted Access

The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

3.2.2.460 Control MP-5: 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.

3.2.2.461 Control MP-5 (1): Protection Outside Of Controlled Areas

[Withdrawn: Incorporated into MP-5].

3.2.2.462 Control MP-5 (2): Documentation Of Activities

[Withdrawn: Incorporated into MP-5].

3.2.2.463 Control MP-5 (3): Custodians

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

3.2.2.464 Control MP-5 (4): Cryptographic Protection

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

3.2.2.465 Control MP-6: 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.

3.2.2.466 Control MP-6 (1): Review / Approve / Track / Document / Verify

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

3.2.2.467 Control MP-6 (2): Equipment Testing

The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.

3.2.2.468 Control MP-6 (3): Nondestructive Techniques

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

3.2.2.469 Control MP-6 (4): Controlled Unclassified Information

[Withdrawn: Incorporated into MP-6].

3.2.2.470 Control MP-6 (5): Classified Information

[Withdrawn: Incorporated into MP-6].

3.2.2.471 Control MP-6 (6): Media Destruction

[Withdrawn: Incorporated into MP-6].

3.2.2.472 Control MP-6 (7): Dual Authorization

The organization enforces dual authorization for the sanitization of [Assignment: organization-defined information system media].

3.2.2.473 Control MP-6 (8): Remote Purging / Wiping Of Information

The organization provides the capability to purge/wipe information from [Assignment: organization-defined information systems, system components, or devices] either remotely or under the following conditions: [Assignment: organization-defined conditions].

3.2.2.474 Control MP-7: 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].

3.2.2.475 Control MP-7 (1): Prohibit Use Without Owner

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

3.2.2.476 Control MP-7 (2): Prohibit Use Of Sanitization-Resistant Media

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

3.2.2.477 Control MP-8: Media Downgrading

The organization: a. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization-defined strength and integrity]; b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identifies [Assignment: organization-defined information system media requiring downgrading]; and d. Downgrades the identified information system media using the established process.

3.2.2.478 Control MP-8 (1): Documentation Of Process

The organization documents information system media downgrading actions.

3.2.2.479 Control MP-8 (2): Equipment Testing

The organization employs [Assignment: organization-defined tests] of downgrading equipment and procedures to verify correct performance [Assignment: organization-defined frequency].

3.2.2.480 Control MP-8 (3): Controlled Unclassified Information

The organization downgrades information system media containing [Assignment: organization-defined Controlled Unclassified Information (CUI)] prior to public release in accordance with applicable federal and organizational standards and policies.

3.2.2.481 Control MP-8 (4): Classified Information

The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies.

3.2.2.482 Control PE-1: 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].

3.2.2.483 Control PE-2: 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.

3.2.2.484 Control PE-2 (1): Access By Position / Role

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

3.2.2.485 Control PE-2 (2): Two Forms Of Identification

The organization requires two forms of identification from [Assignment: organization-defined list of acceptable forms of identification] for visitor access to the facility where the information system resides.

3.2.2.486 Control PE-2 (3): Restrict Unescorted Access

The organization restricts unescorted access to the facility where the information system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined credentials]].

3.2.2.487 Control PE-3: 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.

3.2.2.488 Control PE-3 (1): Information System Access

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].

3.2.2.489 Control PE-3 (2): Facility / Information System Boundaries

The organization performs security checks [Assignment: organization-defined frequency] at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.

3.2.2.490 Control PE-3 (3): Continuous Guards / Alarms / Monitoring

The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

3.2.2.491 Control PE-3 (4): Lockable Casings

The organization uses lockable physical casings to protect [Assignment: organization-defined information system components] from unauthorized physical access.

3.2.2.492 Control PE-3 (5): Tamper Protection

The organization employs [Assignment: organization-defined security safeguards] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the information system.

3.2.2.493 Control PE-3 (6): Facility Penetration Testing

The organization employs a penetration testing process that includes [Assignment: organization-defined frequency], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

3.2.2.494 Control PE-4: 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].

3.2.2.495 Control PE-5: Access Control For Output Devices

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

3.2.2.496 Control PE-5 (1): Access To Output By Authorized Individuals

The organization: (1)(a). Controls physical access to output from [Assignment: organization-defined output devices]; and (1)(b). Ensures that only authorized individuals receive output from the device.

3.2.2.497 Control PE-5 (2): Access To Output By Individual Identity

The information system: (2)(a). Controls physical access to output from [Assignment: organization-defined output devices]; and (2)(b). Links individual identity to receipt of the output from the device.

3.2.2.498 Control PE-5 (3): Marking Output Devices

The organization marks [Assignment: organization-defined information system output devices] indicating the appropriate security marking of the information permitted to be output from the device.

3.2.2.499 Control PE-6: 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.

3.2.2.500 Control PE-6 (1): Intrusion Alarms / Surveillance Equipment

The organization monitors physical intrusion alarms and surveillance equipment.

3.2.2.501 Control PE-6 (2): Automated Intrusion Recognition / Responses

The organization employs automated mechanisms to recognize [Assignment: organization-defined classes/types of intrusions] and initiate [Assignment: organization-defined response actions].

3.2.2.502 Control PE-6 (3): Video Surveillance

The organization employs video surveillance of [Assignment: organization-defined operational areas] and retains video recordings for [Assignment: organization-defined time period].

3.2.2.503 Control PE-6 (4): Monitoring Physical Access To Information Systems

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].

3.2.2.504 Control PE-7: Visitor Control

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

3.2.2.505 Control PE-8: Visitor 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].

3.2.2.506 Control PE-8 (1): Automated Records Maintenance / Review

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

3.2.2.507 Control PE-8 (2): Physical Access Records

[Withdrawn: Incorporated into PE-2].

3.2.2.508 Control PE-9: Power Equipment And Cabling

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

3.2.2.509 Control PE-9 (1): Redundant Cabling

The organization employs redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].

3.2.2.510 Control PE-9 (2): Automatic Voltage Controls

The organization employs automatic voltage controls for [Assignment: organization-defined critical information system components].

3.2.2.511 Control PE-10: 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.

3.2.2.512 Control PE-10 (1): Accidental / Unauthorized Activation

[Withdrawn: Incorporated into PE-10].

3.2.2.513 Control PE-11: 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.

3.2.2.514 Control PE-11 (1): Long-Term Alternate Power Supply - Minimal Operational Capability

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.

3.2.2.515 Control PE-11 (2): Long-Term Alternate Power Supply - Self-Contained

The organization provides a long-term alternate power supply for the information system that is: (2)(a). Self-contained; (2)(b). Not reliant on external power generation; and (2)(c). Capable of maintaining [Selection: minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source.

3.2.2.516 Control PE-12: 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.

3.2.2.517 Control PE-12 (1): Essential Missions / Business Functions

The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

3.2.2.518 Control PE-13: 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.

3.2.2.519 Control PE-13 (1): Detection Devices / Systems

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.

3.2.2.520 Control PE-13 (2): Suppression Devices / Systems

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].

3.2.2.521 Control PE-13 (3): Automatic Fire Suppression

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

3.2.2.522 Control PE-13 (4): Inspections

The organization ensures that the facility undergoes [Assignment: organization-defined frequency] inspections by authorized and qualified inspectors and resolves identified deficiencies within [Assignment: organization-defined time period].

3.2.2.523 Control PE-14: 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].

3.2.2.524 Control PE-14 (1): Automatic Controls

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

3.2.2.525 Control PE-14 (2): Monitoring With Alarms / Notifications

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

3.2.2.526 Control PE-15: Water Damage Protection

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

3.2.2.527 Control PE-15 (1): Automation Support

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].

3.2.2.528 Control PE-16: 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.

3.2.2.529 Control PE-17: 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.

3.2.2.530 Control PE-18: 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.

3.2.2.531 Control PE-18 (1): Facility Site

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

3.2.2.532 Control PE-19: Information Leakage

The organization protects the information system from information leakage due to electromagnetic signals emanations.

3.2.2.533 Control PE-19 (1): National Emissions / Tempest Policies And Procedures

The organization ensures that information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.

3.2.2.534 Control PE-20: Asset Monitoring And Tracking

The organization: a. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

3.2.2.535 Control PL-1: 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].

3.2.2.536 Control PL-2: 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 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.

3.2.2.537 Control PL-2 (1): Concept Of Operations

[Withdrawn: Incorporated into PL-7].

3.2.2.538 Control PL-2 (2): Functional Architecture

[Withdrawn: Incorporated into PL-8].

3.2.2.539 Control PL-2 (3): Plan / Coordinate With Other Organizational Entities

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.

3.2.2.540 Control PL-3: System Security Plan Update

[Withdrawn: Incorporated into PL-2].

3.2.2.541 Control PL-4: 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 re-sign when the rules of behavior are revised/updated.

3.2.2.542 Control PL-4 (1): Social Media And Networking Restrictions

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

3.2.2.543 Control PL-5: Privacy Impact Assessment

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

3.2.2.544 Control PL-6: Security-Related Activity Planning

[Withdrawn: Incorporated into PL-2].

3.2.2.545 Control PL-7: Security Concept Of Operations

The organization: a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and b. Reviews and updates the CONOPS [Assignment: organization-defined frequency].

3.2.2.546 Control PL-8: 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.

3.2.2.547 Control PL-8 (1): Defense-In-Depth

The organization designs its security architecture using a defense-in-depth approach that: (1)(a). Allocates [Assignment: organization-defined security safeguards] to [Assignment: organization-defined locations and architectural layers]; and (1)(b). Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

3.2.2.548 Control PL-8 (2): Supplier Diversity

The organization requires that [Assignment: organization-defined security safeguards] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.

3.2.2.549 Control PL-9: Central Management

The organization centrally manages [Assignment: organization-defined security controls and related processes].

3.2.2.550 Control PM-1: 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.

3.2.2.551 Control PM-2: 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.

3.2.2.552 Control PM-3: 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.

3.2.2.553 Control PM-4: 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.

3.2.2.554 Control PM-5: Information System Inventory

The organization develops and maintains an inventory of its information systems.

3.2.2.555 Control PM-6: Information Security Measures Of Performance

The organization develops, monitors, and reports on the results of information security measures of performance.

3.2.2.556 Control PM-7: 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.

3.2.2.557 Control PM-8: Critical Infrastructure Plan

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

3.2.2.558 Control PM-9: 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.

3.2.2.559 Control PM-10: 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.

3.2.2.560 Control PM-11: 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 organi-

zations, 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.

3.2.2.561 Control PM-12: Insider Threat Program

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

3.2.2.562 Control PM-13: Information Security Workforce

The organization establishes an information security workforce development and improvement program.

3.2.2.563 Control PM-14: 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.

3.2.2.564 Control PM-15: 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.

3.2.2.565 Control PM-16: Threat Awareness Program

The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

3.2.2.566 Control PS-1: 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].

3.2.2.567 Control PS-2: Position Risk Designation

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].

3.2.2.568 Control PS-3: 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].

3.2.2.569 Control PS-3 (1): Classified Information

The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

3.2.2.570 Control PS-3 (2): Formal Indoctrination

The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.

3.2.2.571 Control PS-3 (3): Information With Special Protection Measures

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (3)(a). Have valid access authorizations that are demonstrated by assigned official government duties; and (3)(b). Satisfy [Assignment: organization-defined additional personnel screening criteria].

3.2.2.572 Control PS-4: 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].

3.2.2.573 Control PS-4 (1): Post-Employment Requirements

The organization: (1)(a). Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and (1)(b). Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

3.2.2.574 Control PS-4 (2): Automated Notification

The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual.

3.2.2.575 Control PS-5: 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].

3.2.2.576 Control PS-6: 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].

3.2.2.577 Control PS-6 (1): Information Requiring Special Protection

[Withdrawn: Incorporated into PS-3].

3.2.2.578 Control PS-6 (2): Classified Information Requiring Special Protection

The organization ensures that access to classified information requiring special protection is granted only to individuals who: (2)(a). Have a valid access authorization that is demonstrated by assigned official government duties; (2)(b). Satisfy associated personnel security criteria; and (2)(c). Have read, understood, and signed a nondisclosure agreement.

3.2.2.579 Control PS-6 (3): Post-Employment Requirements

The organization: (3)(a). Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information; and (3)(b). Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

3.2.2.580 Control PS-7: 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.

3.2.2.581 Control PS-8: 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.

3.2.2.582 Control RA-1: 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].

3.2.2.583 Control RA-2: 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 authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

3.2.2.584 Control RA-3: 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.

3.2.2.585 Control RA-4: Risk Assessment Update

[Withdrawn: Incorporated into RA-3].

3.2.2.586 Control RA-5: 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 facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1.

Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [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).

3.2.2.587 Control RA-5 (1): Update Tool Capability

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

3.2.2.588 Control RA-5 (2): Update By Frequency / Prior To New Scan / When Identified

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].

3.2.2.589 Control RA-5 (3): Breadth / Depth Of Coverage

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

3.2.2.590 Control RA-5 (4): Discoverable Information

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined corrective actions].

3.2.2.591 Control RA-5 (5): Privileged Access

The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities].

3.2.2.592 Control RA-5 (6): Automated Trend Analyses

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

3.2.2.593 Control RA-5 (7): Automated Detection And Notification Of Unauthorized Components

[Withdrawn: Incorporated into CM-8].

3.2.2.594 Control RA-5 (8): Review Historic Audit Logs

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

3.2.2.595 Control RA-5 (9): Penetration Testing And Analyses

[Withdrawn: Incorporated into CA-8].

3.2.2.596 Control RA-5 (10): Correlate Scanning Information

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

3.2.2.597 Control RA-6: Technical Surveillance Countermeasures Survey

The organization employs a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]].

3.2.2.598 Control SA-1: 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].

3.2.2.599 Control SA-2: 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.

3.2.2.600 Control SA-3: System Development Life Cycle

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.

3.2.2.601 Control SA-4: Acquisition Process

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.

3.2.2.602 Control SA-4 (1): Functional Properties Of Security Controls

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

3.2.2.603 Control SA-4 (2): Design / Implementation Information For Security Controls

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [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].

3.2.2.604 Control SA-4 (3): Development Methods / Techniques / Practices

The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes].

3.2.2.605 Control SA-4 (4): Assignment Of Components To Systems

[Withdrawn: Incorporated into CM-8 (9)].

3.2.2.606 Control SA-4 (5): System / Component / Service Configurations

The organization requires the developer of the information system, system component, or information system service to: (5)(a). Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and (5)(b). Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

3.2.2.607 Control SA-4 (6): Use Of Information Assurance Products

The organization: (6)(a). Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and (6)(b). Ensures that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

3.2.2.608 Control SA-4 (7): Niap-Approved Protection Profiles

The organization: (7)(a). Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated

against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and (7)(b). Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

3.2.2.609 Control SA-4 (8): Continuous Monitoring Plan

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [Assignment: organization-defined level of detail].

3.2.2.610 Control SA-4 (9): Functions / Ports / Protocols / Services In Use

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

3.2.2.611 Control SA-4 (10): Use Of Approved Piv Products

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

3.2.2.612 Control SA-5: 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 takes [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].

3.2.2.613 Control SA-5 (1): Functional Properties Of Security Controls

[Withdrawn: Incorporated into SA-4 (1)].

3.2.2.614 Control SA-5 (2): Security-Relevant External System Interfaces

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

3.2.2.615 Control SA-5 (3): High-Level Design

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

3.2.2.616 Control SA-5 (4): Low-Level Design

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

3.2.2.617 Control SA-5 (5): Source Code

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

3.2.2.618 Control SA-6: Software Usage Restrictions

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

3.2.2.619 Control SA-7: User-Installed Software

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

3.2.2.620 Control SA-8: Security Engineering Principles

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

3.2.2.621 Control SA-9: 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.

3.2.2.622 Control SA-9 (1): Risk Assessments / Organizational Approvals

The organization: (1)(a). Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (1)(b). Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

3.2.2.623 Control SA-9 (2): Identification Of Functions / Ports / Protocols / 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.

3.2.2.624 Control SA-9 (3): Establish / Maintain Trust Relationship With Providers

The organization establishes, documents, and maintains trust relationships with external service providers based on [Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships].

3.2.2.625 Control SA-9 (4): Consistent Interests Of Consumers And Providers

The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests.

3.2.2.626 Control SA-9 (5): Processing, Storage, And Service Location

The organization restricts the location of [Selection (one or more): information processing; information/data; information system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

3.2.2.627 Control SA-10: 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 system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

3.2.2.628 Control SA-10 (1): Software / Firmware Integrity Verification

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

3.2.2.629 Control SA-10 (2): Alternative Configuration Management Processes

The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

3.2.2.630 Control SA-10 (3): Hardware Integrity Verification

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

3.2.2.631 Control SA-10 (4): Trusted Generation

The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

3.2.2.632 Control SA-10 (5): Mapping Integrity For Version Control

The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

3.2.2.633 Control SA-10 (6): Trusted Distribution

The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

3.2.2.634 Control SA-11: 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; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.

3.2.2.635 Control SA-11 (1): Static Code Analysis

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

3.2.2.636 Control SA-11 (2): Threat And Vulnerability Analyses

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

3.2.2.637 Control SA-11 (3): Independent Verification Of Assessment Plans / Evidence

The organization: (3)(a). Requires an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and (3)(b). Ensures that the independent agent is either provided with sufficient information to complete the verification process or granted the authority to obtain such information.

3.2.2.638 Control SA-11 (4): Manual Code Reviews

The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques].

3.2.2.639 Control SA-11 (5): Penetration Testing

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

3.2.2.640 Control SA-11 (6): Attack Surface Reviews

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

3.2.2.641 Control SA-11 (7): Verify Scope Of Testing / Evaluation

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

3.2.2.642 Control SA-11 (8): Dynamic Code Analysis

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

3.2.2.643 Control SA-12: 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.

3.2.2.644 Control SA-12 (1): Acquisition Strategies / Tools / Methods

The organization employs [Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods] for the purchase of the information system, system component, or information system service from suppliers.

3.2.2.645 Control SA-12 (2): Supplier Reviews

The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.

3.2.2.646 Control SA-12 (3): Trusted Shipping And Warehousing

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

3.2.2.647 Control SA-12 (4): Diversity Of Suppliers

[Withdrawn: Incorporated into SA-12 (13)].

3.2.2.648 Control SA-12 (5): Limitation Of Harm

The organization employs [Assignment: organization-defined security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain.

3.2.2.649 Control SA-12 (6): Minimizing Procurement Time

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

3.2.2.650 Control SA-12 (7): Assessments Prior To Selection / Acceptance / Update

The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update.

3.2.2.651 Control SA-12 (8): Use Of All-Source Intelligence

The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.

3.2.2.652 Control SA-12 (9): Operations Security

The organization employs [Assignment: organization-defined Operations Security (OPSEC) safeguards] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

3.2.2.653 Control SA-12 (10): Validate As Genuine And Not Altered

The organization employs [Assignment: organization-defined security safeguards] to validate that the information system or system component received is genuine and has not been altered.

3.2.2.654 Control SA-12 (11): Penetration Testing / Analysis Of Elements, Processes, And Actors

The organization employs [Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing] of [Assignment: organization-defined supply chain elements, processes, and actors] associated with the information system, system component, or information system service.

3.2.2.655 Control SA-12 (12): Inter-Organizational Agreements

The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service.

3.2.2.656 Control SA-12 (13): Critical Information System Components

The organization employs [Assignment: organization-defined security safeguards] to ensure an adequate supply of [Assignment: organization-defined critical information system components].

3.2.2.657 Control SA-12 (14): Identity And Traceability

The organization establishes and retains unique identification of [Assignment: organization-defined supply chain elements, processes, and actors] for the information system, system component, or information system service.

3.2.2.658 Control SA-12 (15): Processes To Address Weaknesses Or Deficiencies

The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

3.2.2.659 Control SA-13: Trustworthiness

The organization: a. Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and b. Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.

3.2.2.660 Control SA-14: Criticality Analysis

The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].

3.2.2.661 Control SA-14 (1): Critical Components With No Viable Alternative Sourcing

[Withdrawn: Incorporated into SA-20].

3.2.2.662 Control SA-15: 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].

3.2.2.663 Control SA-15 (1): Quality Metrics

The organization requires the developer of the information system, system component, or information system service to: (1)(a). Define quality metrics at the beginning of the development process; and (1)(b). Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].

3.2.2.664 Control SA-15 (2): Security Tracking Tools

The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

3.2.2.665 Control SA-15 (3): Criticality Analysis

The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle].

3.2.2.666 Control SA-15 (4): Threat Modeling / Vulnerability Analysis

The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [Assignment: organization-defined breadth/depth] that: (4)(a). Uses [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; (4)(b). Employs [Assignment: organization-defined tools and methods]; and (4)(c). Produces evidence that meets [Assignment: organization-defined acceptance criteria].

3.2.2.667 Control SA-15 (5): Attack Surface Reduction

The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [Assignment: organization-defined thresholds].

3.2.2.668 Control SA-15 (6): Continuous Improvement

The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

3.2.2.669 Control SA-15 (7): Automated Vulnerability Analysis

The organization requires the developer of the information system, system component, or information system service to: (7)(a). Perform an automated vulnerability analysis using [Assignment: organization-defined tools]; (7)(b). Determine the exploitation potential for discovered vulnerabilities; (7)(c). Determine potential risk mitigations for delivered vulnerabilities; and (7)(d). Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].

3.2.2.670 Control SA-15 (8): Reuse Of Threat / Vulnerability Information

The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

3.2.2.671 Control SA-15 (9): Use Of Live Data

The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.

3.2.2.672 Control SA-15 (10): Incident Response Plan

The organization requires the developer of the information system, system component, or information system service to provide an incident response plan.

3.2.2.673 Control SA-15 (11): Archive Information System / Component

The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.

3.2.2.674 Control SA-16: 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.

3.2.2.675 Control SA-17: 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 organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

3.2.2.676 Control SA-17 (1): Formal Policy Model

The organization requires the developer of the information system, system component, or information system service to: (1)(a). Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security policy] to be enforced; and (1)(b). Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

3.2.2.677 Control SA-17 (2): Security-Relevant Components

The organization requires the developer of the information system, system component, or information system service to: (2)(a). Define security-relevant hardware, software, and firmware; and (2)(b). Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

3.2.2.678 Control SA-17 (3): Formal Correspondence

The organization requires the developer of the information system, system component, or information system service to: (3)(a). Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (3)(b). Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model; (3)(c). Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (3)(d). Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and (3)(e). Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

3.2.2.679 Control SA-17 (4): Informal Correspondence

The organization requires the developer of the information system, system component, or information system service to: (4)(a). Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (4)(b). Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model; (4)(c). Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (4)(d). Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and (4)(e). Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

3.2.2.680 Control SA-17 (5): Conceptually Simple Design

The organization requires the developer of the information system, system component, or information system service to: (5)(a). Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and (5)(b). Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

3.2.2.681 Control SA-17 (6): Structure For Testing

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.

3.2.2.682 Control SA-17 (7): Structure For Least Privilege

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

3.2.2.683 Control SA-18: Tamper Resistance And Detection

The organization implements a tamper protection program for the information system, system component, or information system service.

3.2.2.684 Control SA-18 (1): Multiple Phases Of Sdlc

The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

3.2.2.685 Control SA-18 (2): Inspection Of Information Systems, Components, Or Devices

The organization inspects [Assignment: organization-defined information systems, system components, or devices] [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering.

3.2.2.686 Control SA-19: Component Authenticity

The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

3.2.2.687 Control SA-19 (1): Anti-Counterfeit Training

The organization trains [Assignment: organization-defined personnel or roles] to detect counterfeit information system components (including hardware, software, and firmware).

3.2.2.688 Control SA-19 (2): Configuration Control For Component Service / Repair

The organization maintains configuration control over [Assignment: organization-defined information system components] awaiting service/repair and serviced/repaired components awaiting return to service.

3.2.2.689 Control SA-19 (3): Component Disposal

The organization disposes of information system components using [Assignment: organization-defined techniques and methods].

3.2.2.690 Control SA-19 (4): Anti-Counterfeit Scanning

The organization scans for counterfeit information system components [Assignment: organization-defined frequency].

3.2.2.691 Control SA-20: Customized Development Of Critical Components

The organization re-implements or custom develops [Assignment: organization-defined critical information system components].

3.2.2.692 Control SA-21: Developer Screening

The organization requires that the developer of [Assignment: organization-defined information system, system component, or information system service]: a. Have appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and b. Satisfy [Assignment: organization-defined additional personnel screening criteria].

3.2.2.693 Control SA-21 (1): Validation Of Screening

The organization requires the developer of the information system, system component, or information system service take [Assignment: organization-defined actions] to ensure that the required access authorizations and screening criteria are satisfied.

3.2.2.694 Control SA-22: Unsupported System Components

The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

3.2.2.695 Control SA-22 (1): Alternative Sources For Continued Support

The organization provides [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]] for unsupported information system components.

3.2.2.696 Control SC-1: 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].

3.2.2.697 Control SC-2: Application Partitioning

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

3.2.2.698 Control SC-2 (1): Interfaces For Non-Privileged Users

The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.

3.2.2.699 Control SC-3: Security Function Isolation

The information system isolates security functions from nonsecurity functions.

3.2.2.700 Control SC-3 (1): Hardware Separation

The information system utilizes underlying hardware separation mechanisms to implement security function isolation.

3.2.2.701 Control SC-3 (2): Access / Flow Control Functions

The information system isolates security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

3.2.2.702 Control SC-3 (3): Minimize Nonsecurity Functionality

The organization minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

3.2.2.703 Control SC-3 (4): Module Coupling And Cohesiveness

The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

3.2.2.704 Control SC-3 (5): Layered Structures

The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

3.2.2.705 Control SC-4: Information In Shared Resources

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

3.2.2.706 Control SC-4 (1): Security Levels

[Withdrawn: Incorporated into SC-4].

3.2.2.707 Control SC-4 (2): Periods Processing

The information system prevents unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.

3.2.2.708 Control SC-5: 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 references to sources for such information] by employing [Assignment: organization-defined security safeguards].

3.2.2.709 Control SC-5 (1): Restrict Internal Users

The information system restricts the ability of individuals to launch [Assignment: organization-defined denial of service attacks] against other information systems.

3.2.2.710 Control SC-5 (2): Excess Capacity / Bandwidth / Redundancy

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

3.2.2.711 Control SC-5 (3): Detection / Monitoring

The organization: (3)(a). Employs [Assignment: organization-defined monitoring tools] to detect indicators of denial of service attacks against the information system; and (3)(b). Monitors [Assignment: organization-defined information system resources] to determine if sufficient resources exist to prevent effective denial of service attacks.

3.2.2.712 Control SC-6: Resource Availability

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

3.2.2.713 Control SC-7: 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.

3.2.2.714 Control SC-7 (1): Physically Separated Subnetworks

[Withdrawn: Incorporated into SC-7].

3.2.2.715 Control SC-7 (2): Public Access

[Withdrawn: Incorporated into SC-7].

3.2.2.716 Control SC-7 (3): Access Points

The organization limits the number of external network connections to the information system.

3.2.2.717 Control SC-7 (4): External Telecommunications Services

The organization: (4)(a). Implements a managed interface for each external telecommunication service; (4)(b). Establishes a traffic flow policy for each managed interface; (4)(c). Protects the confidentiality and integrity of the information being transmitted across each interface; (4)(d). Documents each exception to the traffic flow policy with a supporting mission/business need

and duration of that need; and (4)(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.

3.2.2.718 Control SC-7 (5): Deny By Default / Allow By Exception

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

3.2.2.719 Control SC-7 (6): Response To Recognized Failures

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

3.2.2.720 Control SC-7 (7): Prevent Split Tunneling For Remote Devices

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

3.2.2.721 Control SC-7 (8): Route Traffic To Authenticated Proxy Servers

The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

3.2.2.722 Control SC-7 (9): Restrict Threatening Outgoing Communications Traffic

The information system: (9)(a). Detects and denies outgoing communications traffic posing a threat to external information systems; and (9)(b). Audits the identity of internal users associated with denied communications.

3.2.2.723 Control SC-7 (10): Prevent Unauthorized Exfiltration

The organization prevents the unauthorized exfiltration of information across managed interfaces.

3.2.2.724 Control SC-7 (11): Restrict Incoming Communications Traffic

The information system only allows incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

3.2.2.725 Control SC-7 (12): Host-Based Protection

The organization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system components].

3.2.2.726 Control SC-7 (13): Isolation Of Security Tools / Mechanisms / Support Components

The organization isolates [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

3.2.2.727 Control SC-7 (14): Protects Against Unauthorized Physical Connections

The organization protects against unauthorized physical connections at [Assignment: organization-defined managed interfaces].

3.2.2.728 Control SC-7 (15): Route Privileged Network Accesses

The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

3.2.2.729 Control SC-7 (16): Prevent Discovery Of Components / Devices

The information system prevents discovery of specific system components composing a managed interface.

3.2.2.730 Control SC-7 (17): Automated Enforcement Of Protocol Formats

The information system enforces adherence to protocol formats.

3.2.2.731 Control SC-7 (18): Fail Secure

The information system fails securely in the event of an operational failure of a boundary protection device.

3.2.2.732 Control SC-7 (19): Blocks Communication From Non-Organizationally Configured Hosts

The information system blocks both inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

3.2.2.733 Control SC-7 (20): Dynamic Isolation / Segregation

The information system provides the capability to dynamically isolate/segregate [Assignment: organization-defined information system components] from other components of the system.

3.2.2.734 Control SC-7 (21): Isolation Of Information System Components

The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].

3.2.2.735 Control SC-7 (22): Separate Subnets For Connecting To Different Security Domains

The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.

3.2.2.736 Control SC-7 (23): Disable Sender Feedback On Protocol Validation Failure

The information system disables feedback to senders on protocol format validation failure.

3.2.2.737 Control SC-8: Transmission Confidentiality And Integrity

The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

3.2.2.738 Control SC-8 (1): Cryptographic Or Alternate Physical Protection

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].

3.2.2.739 Control SC-8 (2): Pre / Post Transmission Handling

The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.

3.2.2.740 Control SC-8 (3): Cryptographic Protection For Message Externals

The information system implements cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].

3.2.2.741 Control SC-8 (4): Conceal / Randomize Communications

The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].

3.2.2.742 Control SC-9: Transmission Confidentiality

[Withdrawn: Incorporated into SC-8].

3.2.2.743 Control SC-10: 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.

3.2.2.744 Control SC-11: Trusted Path

The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].

3.2.2.745 Control SC-11 (1): Logical Isolation

The information system provides a trusted communications path that is logically isolated and distinguishable from other paths.

3.2.2.746 Control SC-12: 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].

3.2.2.747 Control SC-12 (1): Availability

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

3.2.2.748 Control SC-12 (2): Symmetric Keys

The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.

3.2.2.749 Control SC-12 (3): Asymmetric Keys

The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].

3.2.2.750 Control SC-12 (4): Pki Certificates

[Withdrawn: Incorporated into SC-12].

3.2.2.751 Control SC-12 (5): Pki Certificates / Hardware Tokens

[Withdrawn: Incorporated into SC-12].

3.2.2.752 Control SC-13: Cryptographic Protection

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.

3.2.2.753 Control SC-13 (1): Fips-Validated Cryptography

[Withdrawn: Incorporated into SC-13].

3.2.2.754 Control SC-13 (2): Nsa-Approved Cryptography

[Withdrawn: Incorporated into SC-13].

3.2.2.755 Control SC-13 (3): Individuals Without Formal Access Approvals

[Withdrawn: Incorporated into SC-13].

3.2.2.756 Control SC-13 (4): Digital Signatures

[Withdrawn: Incorporated into SC-13].

3.2.2.757 Control SC-14: Public Access Protections

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

3.2.2.758 Control SC-15: 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.

3.2.2.759 Control SC-15 (1): Physical Disconnect

The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

3.2.2.760 Control SC-15 (2): Blocking Inbound / Outbound Communications Traffic

[Withdrawn: Incorporated into SC-7].

3.2.2.761 Control SC-15 (3): Disabling / Removal In Secure Work Areas

The organization disables or removes collaborative computing devices from [Assignment: organization-defined information systems or information system components] in [Assignment: organization-defined secure work areas].

3.2.2.762 Control SC-15 (4): Explicitly Indicate Current Participants

The information system provides an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].

3.2.2.763 Control SC-16: Transmission Of Security Attributes

The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.

3.2.2.764 Control SC-16 (1): Integrity Validation

The information system validates the integrity of transmitted security attributes.

3.2.2.765 Control SC-17: 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.

3.2.2.766 Control SC-18: 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.

3.2.2.767 Control SC-18 (1): Identify Unacceptable Code / Take Corrective Actions

The information system identifies [Assignment: organization-defined unacceptable mobile code] and takes [Assignment: organization-defined corrective actions].

3.2.2.768 Control SC-18 (2): Acquisition / Development / Use

The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code requirements].

3.2.2.769 Control SC-18 (3): Prevent Downloading / Execution

The information system prevents the download and execution of [Assignment: organization-defined unacceptable mobile code].

3.2.2.770 Control SC-18 (4): Prevent Automatic Execution

The information system prevents the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforces [Assignment: organization-defined actions] prior to executing the code.

3.2.2.771 Control SC-18 (5): Allow Execution Only In Confined Environments

The organization allows execution of permitted mobile code only in confined virtual machine environments.

3.2.2.772 Control SC-19: 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.

3.2.2.773 Control SC-20: Secure Name / Address Resolution Service (Authoritative Source)

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

3.2.2.774 Control SC-20 (1): Child Subspaces

[Withdrawn: Incorporated into SC-20].

3.2.2.775 Control SC-20 (2): Data Origin / Integrity

The information system provides data origin and integrity protection artifacts for internal name/address resolution queries.

3.2.2.776 Control SC-21: 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.

3.2.2.777 Control SC-21 (1): Data Origin / Integrity

[Withdrawn: Incorporated into SC-21].

3.2.2.778 Control SC-22: 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.

3.2.2.779 Control SC-23: Session Authenticity

The information system protects the authenticity of communications sessions.

3.2.2.780 Control SC-23 (1): Invalidate Session Identifiers At Logout

The information system invalidates session identifiers upon user logout or other session termination.

3.2.2.781 Control SC-23 (2): User-Initiated Logouts / Message Displays

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

3.2.2.782 Control SC-23 (3): Unique Session Identifiers With Randomization

The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session identifiers that are system-generated.

3.2.2.783 Control SC-23 (4): Unique Session Identifiers With Randomization

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

3.2.2.784 Control SC-23 (5): Allowed Certificate Authorities

The information system only allows the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.

3.2.2.785 Control SC-24: 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.

3.2.2.786 Control SC-25: Thin Nodes

The organization employs [Assignment: organization-defined information system components] with minimal functionality and information storage.

3.2.2.787 Control SC-26: Honeypots

The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

3.2.2.788 Control SC-26 (1): Detection Of Malicious Code

[Withdrawn: Incorporated into SC-35].

3.2.2.789 Control SC-27: Platform-Independent Applications

The information system includes: [Assignment: organization-defined platform-independent applications].

3.2.2.790 Control SC-28: Protection Of Information At Rest

The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].

3.2.2.791 Control SC-28 (1): Cryptographic Protection

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [Assignment: organization-defined information system components].

3.2.2.792 Control SC-28 (2): Off-Line Storage

The organization removes from online storage and stores off-line in a secure location [Assignment: organization-defined information].

3.2.2.793 Control SC-29: Heterogeneity

The organization employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.

3.2.2.794 Control SC-29 (1): Virtualization Techniques

The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].

3.2.2.795 Control SC-30: Concealment And Misdirection

The organization employs [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined information systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries.

3.2.2.796 Control SC-30 (1): Virtualization Techniques

[Withdrawn: Incorporated into SC-29 (1)].

3.2.2.797 Control SC-30 (2): Randomness

The organization employs [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.

3.2.2.798 Control SC-30 (3): Change Processing / Storage Locations

The organization changes the location of [Assignment: organization-defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]; at random time intervals]].

3.2.2.799 Control SC-30 (4): Misleading Information

The organization employs realistic, but misleading information in [Assignment: organization-defined information system components] with regard to its security state or posture.

3.2.2.800 Control SC-30 (5): Concealment Of System Components

The organization employs [Assignment: organization-defined techniques] to hide or conceal [Assignment: organization-defined information system components].

3.2.2.801 Control SC-31: Covert Channel Analysis

The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b. Estimates the maximum bandwidth of those channels.

3.2.2.802 Control SC-31 (1): Test Covert Channels For Exploitability

The organization tests a subset of the identified covert channels to determine which channels are exploitable.

3.2.2.803 Control SC-31 (2): Maximum Bandwidth

The organization reduces the maximum bandwidth for identified covert [Selection (one or more); storage; timing] channels to [Assignment: organization-defined values].

3.2.2.804 Control SC-31 (3): Measure Bandwidth In Operational Environments

The organization measures the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the information system.

3.2.2.805 Control SC-32: Information System Partitioning

The organization partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].

3.2.2.806 Control SC-33: Transmission Preparation Integrity

[Withdrawn: Incorporated into SC-8].

3.2.2.807 Control SC-34: Non-Modifiable Executable Programs

The information system at [Assignment: organization-defined information system components]:
a. Loads and executes the operating environment from hardware-enforced, read-only media; and
b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.

3.2.2.808 Control SC-34 (1): No Writable Storage

The organization employs [Assignment: organization-defined information system components] with no writeable storage that is persistent across component restart or power on/off.

3.2.2.809 Control SC-34 (2): Integrity Protection / Read-Only Media

The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media.

3.2.2.810 Control SC-34 (3): Hardware-Based Protection

The organization: (3)(a). Employs hardware-based, write-protect for [Assignment: organization-defined information system firmware components]; and (3)(b). Implements specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

3.2.2.811 Control SC-35: Honeyclients

The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

3.2.2.812 Control SC-36: Distributed Processing And Storage

The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.

3.2.2.813 Control SC-36 (1): Polling Techniques

The organization employs polling techniques to identify potential faults, errors, or compromises to [Assignment: organization-defined distributed processing and storage components].

3.2.2.814 Control SC-37: Out-Of-Band Channels

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

3.2.2.815 Control SC-37 (1): Ensure Delivery / Transmission

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

3.2.2.816 Control SC-38: Operations Security

The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.

3.2.2.817 Control SC-39: Process Isolation

The information system maintains a separate execution domain for each executing process.

3.2.2.818 Control SC-39 (1): Hardware Separation

The information system implements underlying hardware separation mechanisms to facilitate process separation.

3.2.2.819 Control SC-39 (2): Thread Isolation

The information system maintains a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].

3.2.2.820 Control SC-40: Wireless Link Protection

The information system protects external and internal [Assignment: organization-defined wireless links] from [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].

3.2.2.821 Control SC-40 (1): Electromagnetic Interference

The information system implements cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.

3.2.2.822 Control SC-40 (2): Reduce Detection Potential

The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].

3.2.2.823 Control SC-40 (3): Imitative Or Manipulative Communications Deception

The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

3.2.2.824 Control SC-40 (4): Signal Parameter Identification

The information system implements cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.

3.2.2.825 Control SC-41: Port And I/O Device Access

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

3.2.2.826 Control SC-42: Sensor Capability And Data

The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].

3.2.2.827 Control SC-42 (1): Reporting To Authorized Individuals Or Roles

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

3.2.2.828 Control SC-42 (2): Authorized Use

The organization employs the following measures: [Assignment: organization-defined measures], so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes.

3.2.2.829 Control SC-42 (3): Prohibit Use Of Devices

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

3.2.2.830 Control SC-43: Usage Restrictions

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

3.2.2.831 Control SC-44: Detonation Chambers

The organization employs a detonation chamber capability within [Assignment: organization-defined information system, system component, or location].

3.2.2.832 Control SI-1: 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].

3.2.2.833 Control SI-2: 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.

3.2.2.834 Control SI-2 (1): Central Management

The organization centrally manages the flaw remediation process.

3.2.2.835 Control SI-2 (2): Automated Flaw Remediation Status

The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.

3.2.2.836 Control SI-2 (3): Time To Remediate Flaws / Benchmarks For Corrective Actions

The organization: (3)(a). Measures the time between flaw identification and flaw remediation; and (3)(b). Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

3.2.2.837 Control SI-2 (4): Automated Patch Management Tools

[Withdrawn: Incorporated into SI-2].

3.2.2.838 Control SI-2 (5): Automatic Software / Firmware Updates

The organization installs [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined information system components].

3.2.2.839 Control SI-2 (6): Removal Of Previous Versions Of Software / Firmware

The organization removes [Assignment: organization-defined software and firmware components] after updated versions have been installed.

3.2.2.840 Control SI-3: 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.

3.2.2.841 Control SI-3 (1): Central Management

The organization centrally manages malicious code protection mechanisms.

3.2.2.842 Control SI-3 (2): Automatic Updates

The information system automatically updates malicious code protection mechanisms.

3.2.2.843 Control SI-3 (3): Non-Privileged Users

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

3.2.2.844 Control SI-3 (4): Updates Only By Privileged Users

The information system updates malicious code protection mechanisms only when directed by a privileged user.

3.2.2.845 Control SI-3 (5): Portable Storage Devices

[Withdrawn: Incorporated into MP-7].

3.2.2.846 Control SI-3 (6): Testing / Verification

The organization: (6)(a). Tests malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing a known benign, non-spreading test case into the information

system; and (6)(b). Verifies that both detection of the test case and associated incident reporting occur.

3.2.2.847 Control SI-3 (7): Nonsignature-Based Detection

The information system implements nonsignature-based malicious code detection mechanisms.

3.2.2.848 Control SI-3 (8): Detect Unauthorized Commands

The information system detects [Assignment: organization-defined unauthorized operating system commands] through the kernel application programming interface at [Assignment: organization-defined information system hardware components] and [Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command].

3.2.2.849 Control SI-3 (9): Authenticate Remote Commands

The information system implements [Assignment: organization-defined security safeguards] to authenticate [Assignment: organization-defined remote commands].

3.2.2.850 Control SI-3 (10): Malicious Code Analysis

The organization: (10)(a). Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of malicious code; and (10)(b). Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

3.2.2.851 Control SI-4: 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: 1. Strategically within the information system to collect organization-determined essential information; and 2. 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]].

3.2.2.852 Control SI-4 (1): System-Wide Intrusion Detection System

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

3.2.2.853 Control SI-4 (2): Automated Tools For Real-Time Analysis

The organization employs automated tools to support near real-time analysis of events.

3.2.2.854 Control SI-4 (3): Automated Tool Integration

The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

3.2.2.855 Control SI-4 (4): Inbound And Outbound Communications Traffic

The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.

3.2.2.856 Control SI-4 (5): System-Generated Alerts

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].

3.2.2.857 Control SI-4 (6): Restrict Non-Privileged Users

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

3.2.2.858 Control SI-4 (7): Automated Response To Suspicious Events

The information system notifies [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events and takes [Assignment: organization-defined least-disruptive actions to terminate suspicious events].

3.2.2.859 Control SI-4 (8): Protection Of Monitoring Information

[Withdrawn: Incorporated into SI-4].

3.2.2.860 Control SI-4 (9): Testing Of Monitoring Tools

The organization tests intrusion-monitoring tools [Assignment: organization-defined frequency].

3.2.2.861 Control SI-4 (10): Visibility Of Encrypted Communications

The organization makes provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined information system monitoring tools].

3.2.2.862 Control SI-4 (11): Analyze Communications Traffic Anomalies

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)] to discover anomalies.

3.2.2.863 Control SI-4 (12): Automated Alerts

The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined activities that trigger alerts].

3.2.2.864 Control SI-4 (13): Analyze Traffic / Event Patterns

The organization: (13)(a). Analyzes communications traffic/event patterns for the information system; (13)(b). Develops profiles representing common traffic patterns and/or events; and (13)(c). Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.

3.2.2.865 Control SI-4 (14): Wireless Intrusion Detection

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

3.2.2.866 Control SI-4 (15): Wireless To Wireline Communications

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

3.2.2.867 Control SI-4 (16): Correlate Monitoring Information

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

3.2.2.868 Control SI-4 (17): Integrated Situational Awareness

The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

3.2.2.869 Control SI-4 (18): Analyze Traffic / Covert Exfiltration

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)] to detect covert exfiltration of information.

3.2.2.870 Control SI-4 (19): Individuals Posing Greater Risk

The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.

3.2.2.871 Control SI-4 (20): Privileged Users

The organization implements [Assignment: organization-defined additional monitoring] of privileged users.

3.2.2.872 Control SI-4 (21): Probationary Periods

The organization implements [Assignment: organization-defined additional monitoring] of individuals during [Assignment: organization-defined probationary period].

3.2.2.873 Control SI-4 (22): Unauthorized Network Services

The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection (one or more): audits; alerts [Assignment: organization-defined personnel or roles]].

3.2.2.874 Control SI-4 (23): Host-Based Devices

The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].

3.2.2.875 Control SI-4 (24): Indicators Of Compromise

The information system discovers, collects, distributes, and uses indicators of compromise.

3.2.2.876 Control SI-5: 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.

3.2.2.877 Control SI-5 (1): Automated Alerts And Advisories

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

3.2.2.878 Control SI-6: Security Function 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 security verification 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.

3.2.2.879 Control SI-6 (1): Notification Of Failed Security Tests

[Withdrawn: Incorporated into SI-6].

3.2.2.880 Control SI-6 (2): Automation Support For Distributed Testing

The information system implements automated mechanisms to support the management of distributed security testing.

3.2.2.881 Control SI-6 (3): Report Verification Results

The organization reports the results of security function verification to [Assignment: organization-defined personnel or roles].

3.2.2.882 Control SI-7: Software, Firmware, And Information Integrity

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

3.2.2.883 Control SI-7 (1): Integrity Checks

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]].

3.2.2.884 Control SI-7 (2): Automated Notifications Of Integrity Violations

The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

3.2.2.885 Control SI-7 (3): Centrally-Managed Integrity Tools

The organization employs centrally managed integrity verification tools.

3.2.2.886 Control SI-7 (4): Tamper-Evident Packaging

[Withdrawn: Incorporated into SA-12].

3.2.2.887 Control SI-7 (5): Automated Response To Integrity Violations

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.

3.2.2.888 Control SI-7 (6): Cryptographic Protection

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

3.2.2.889 Control SI-7 (7): Integration Of Detection And Response

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

3.2.2.890 Control SI-7 (8): Auditing Capability For Significant Events

The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [Selection (one or more): generates an audit record; alerts current user; alerts [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].

3.2.2.891 Control SI-7 (9): Verify Boot Process

The information system verifies the integrity of the boot process of [Assignment: organization-defined devices].

3.2.2.892 Control SI-7 (10): Protection Of Boot Firmware

The information system implements [Assignment: organization-defined security safeguards] to protect the integrity of boot firmware in [Assignment: organization-defined devices].

3.2.2.893 Control SI-7 (11): Confined Environments With Limited Privileges

The organization requires that [Assignment: organization-defined user-installed software] execute in a confined physical or virtual machine environment with limited privileges.

3.2.2.894 Control SI-7 (12): Integrity Verification

The organization requires that the integrity of [Assignment: organization-defined user-installed software] be verified prior to execution.

3.2.2.895 Control SI-7 (13): Code Execution In Protected Environments

The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles].

3.2.2.896 Control SI-7 (14): Binary Or Machine Executable Code

The organization: (14)(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 (14)(b). Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

3.2.2.897 Control SI-7 (15): Code Authentication

The information system implements cryptographic mechanisms to authenticate [Assignment: organization-defined software or firmware components] prior to installation.

3.2.2.898 Control SI-7 (16): Time Limit On Process Execution W/O Supervision

The organization does not allow processes to execute without supervision for more than [Assignment: organization-defined time period].

3.2.2.899 Control SI-8: 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.

3.2.2.900 Control SI-8 (1): Central Management

The organization centrally manages spam protection mechanisms.

3.2.2.901 Control SI-8 (2): Automatic Updates

The information system automatically updates spam protection mechanisms.

3.2.2.902 Control SI-8 (3): Continuous Learning Capability

The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

3.2.2.903 Control SI-9: Information Input Restrictions

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

3.2.2.904 Control SI-10: Information Input Validation

The information system checks the validity of [Assignment: organization-defined information inputs].

3.2.2.905 Control SI-10 (1): Manual Override Capability

The information system: (1)(a). Provides a manual override capability for input validation of [Assignment: organization-defined inputs]; (1)(b). Restricts the use of the manual override capability to only [Assignment: organization-defined authorized individuals]; and (1)(c). Audits the use of the manual override capability.

3.2.2.906 Control SI-10 (2): Review / Resolution Of Errors

The organization ensures that input validation errors are reviewed and resolved within [Assignment: organization-defined time period].

3.2.2.907 Control SI-10 (3): Predictable Behavior

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

3.2.2.908 Control SI-10 (4): Review / Timing Interactions

The organization accounts for timing interactions among information system components in determining appropriate responses for invalid inputs.

3.2.2.909 Control SI-10 (5): Restrict Inputs To Trusted Sources And Approved Formats

The organization restricts the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].

3.2.2.910 Control SI-11: 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].

3.2.2.911 Control SI-12: Information 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.

3.2.2.912 Control SI-13: Predictable Failure Prevention

The organization: a. Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria].

3.2.2.913 Control SI-13 (1): Transferring Component Responsibilities

The organization takes information system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.

3.2.2.914 Control SI-13 (2): Time Limit On Process Execution Without Supervision

[Withdrawn: Incorporated into SI-7 (16)].

3.2.2.915 Control SI-13 (3): Manual Transfer Between Components

The organization manually initiates transfers between active and standby information system components [Assignment: organization-defined frequency] if the mean time to failure exceeds [Assignment: organization-defined time period].

3.2.2.916 Control SI-13 (4): Standby Component Installation / Notification

The organization, if information system component failures are detected: (4)(a). Ensures that the standby components are successfully and transparently installed within [Assignment: organization-defined time period]; and (4)(b). [Selection (one or more): activates [Assignment: organization-defined alarm]; automatically shuts down the information system].

3.2.2.917 Control SI-13 (5): Failover Capability

The organization provides [Selection: real-time; near real-time] [Assignment: organization-defined failover capability] for the information system.

3.2.2.918 Control SI-14: Non-Persistence

The organization implements non-persistent [Assignment: organization-defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].

3.2.2.919 Control SI-14 (1): Refresh From Trusted Sources

The organization ensures that software and data employed during information system component and service refreshes are obtained from [Assignment: organization-defined trusted sources].

3.2.2.920 Control SI-15: Information Output Filtering

The information system validates information output from [Assignment: organization-defined software programs and/or applications] to ensure that the information is consistent with the expected content.

3.2.2.921 Control SI-16: Memory Protection

The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.

3.2.2.922 Control SI-17: Fail-Safe Procedures

The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].