Federal Public Key Infrastructure (FPKI)

Security Controls Profile of Special Publication 800-53A

Assessment Guidance for Security Controls in PKI Systems

Version 1.0
April 18, 2011

Revision History

Document Version	Document Date	Revision Details
v1.0	18 April 2011	Approved version for publication.

Acknowledgements

This publication was developed by the Certificate Policy Working Group (CPWG) with representatives from various federal agencies and non-federal organizations in an effort to produce a unified Federal Public Key Infrastructure security control profile. The Federal Public Key Infrastructure Policy Authority wishes to acknowledge and thank the members of the CPWG for their dedicated efforts.

In addition to the above acknowledgment, a special note of thanks goes to Judith Spencer (General Services Administration, FPKIPA Chair), Ron Ross (National Institute of Standards and Technology), Matt King (Protiviti Government Services), Charles Froehlich (ManTech, CPWG Chair), Larry Frank (Booz Allen), and Dave Silver (Protiviti Government Services) for their exceptional contributions to the direction, content, and presentation of this document.

NIST SP 800-53A FPKI Security Controls Profile – Assessment Guidance to Security Controls in PKI Systems

This document is a Profile of National Institute of Standards and Technology Special Publication (NIST SP) 800-53A. The Profile scopes NIST SP 800-53, providing specific guidance for assessing Federal Public Key Infrastructure (PKI) Systems against security controls required by the *Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53, FPKI Security Controls for PKI Systems*. The Profile excludes NIST SP 800-53 security controls (in whole or in part) and control enhancements (in whole or in part) that do not apply to PKI Systems. Where necessary, guidance has been modified to be relevant to PKI Systems. As a result, this Profile is a complete assessment tool that an Assessor can use to evaluate a PKI system.

Questions about this Profile should be directed to FPKI.Webmaster@gsa.gov

.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-1	**ACCESS CONTROL POLICY AND PROCEDURES**
AC-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents access control policy;* *(ii) the organization access control policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;* *(iv) the organization develops and formally documents access control procedures;* *(v) the organization access control procedures facilitate implementation of the access control policy and associated access controls; and* *(vi) the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access control responsibilities].
AC-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of access control policy reviews/updates;* *(ii) the organization reviews/updates access control policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of access control procedure reviews/updates; and* *(iv) the organization reviews/updates access control procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access control responsibilities].

AC-1(PKI)	ACCESS CONTROL POLICY AND PROCEDURES
AC-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Access Control policy, Access Control policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, and frequency of review/update.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-2	**ACCOUNT MANAGEMENT**
AC-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages information system accounts, including;* - *group, guest, temporary, anonymous accounts are not permitted;* - *identifying authorized users of the information system and specifying access privileges;* - *requiring appropriate approvals for requests to establish accounts;* - *establishing, activating, modifying, disabling, and removing accounts;* - *notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;* - *deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and* - *granting access to the system based on:* - *a valid access authorization;* - *intended system usage; and* - *other attributes as required by the organization or associated missions/business functions; and* *(ii) the organization defines the frequency of information system account reviews; and* *(iii) the organization reviews information system accounts in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities].

AC-2(3)	ACCOUNT MANAGEMENT
AC-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines in a time period after which the information system disables inactive accounts; and* *(ii) the information system automatically disables inactive accounts after organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Test**: [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(4)	ACCOUNT MANAGEMENT
AC-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system automatically audits:* - *account creation;* - *modification;* - *disabling; and* - *termination actions; and* *(ii) the information system notifies, as required, appropriate individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Test**: [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(5)	ACCOUNT MANAGEMENT
AC-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization monitors for atypical usage of information system accounts; and* *(ii) the organization reports atypical usage to designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities].

AC-2(7)	ACCOUNT MANAGEMENT
AC-2(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and* *(ii) the organization tracks and monitors privileged role assignments.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities].

AC-2(PKI)	ACCOUNT MANAGEMENT
AC-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms under the control of PKI Trusted Roles identified in the CP to support the management of information system accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Test**: [*SELECT FROM:* Automated mechanisms implementing account management functions].
AC-2(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if at least two-person PKI Trusted Role (identified in the CP) access control is required for access to CA equipment.* **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-3	**ACCESS ENFORCEMENT**
AC-3.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access enforcement policy].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-4	**INFORMATION FLOW ENFORCEMENT**
AC-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems;* *(ii) the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; and* *(iii) the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(PKI)	**INFORMATION FLOW ENFORCEMENT**
AC-4(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization defines the security policy filters that privileged administrators have the capability to configure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, as appropriate, to provide for multi party control where one of the following actions occurs for CAs operating at Medium Assurance or above: • CA key generation; • CA signing key activation; • CA private key backup **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for configuring security policy filters]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].
AC-4(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if the information system requires a privileged administrator to configure all attributes and security policies; and the Administrator must operate in a two- (or more) person control environment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, as appropriate, to provide for multi party control where one of the following actions occurs for CAs operating at Medium Assurance or above: • CA key generation; • CA signing key activation; • CA private key backup **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for configuring security policy filters]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-5	**SEPARATION OF DUTIES**
AC-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;* *(ii) the organization documents separation of duties; and* *(iii) the organization implements separation of duties through assigned information system access authorizations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, as appropriate, for separation of duties of PKI Trusted Roles identified in the CP. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties]. **Test**: [*SELECT FROM:* Automated mechanisms implementing separation of duties policy].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-6	**LEAST PRIVILEGE**
AC-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(2)	**LEAST PRIVILEGE**
AC-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access; and* *(ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions; and* *(iii) the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(5)	**LEAST PRIVILEGE**
AC-6(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits authorization to super user accounts on the information system to designated system administration personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of system-generated super user accounts; list of system administration personnel; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(PKI)	LEAST PRIVILEGE
AC-6(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; and* *(ii) the organization explicitly authorizes access to CA and RA security and audit functions, configurations, and logs only to specifically designated Trusted Roles as specified in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of security functions and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].
AC-6(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits access to the information system by users not designated as Trusted Roles of the PKI System.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, as appropriate, for separation of duties of PKI Trusted Roles identified in the CP to include the following enhancements: • The organization limits authorization to super user accounts on the information system to designated system administration Trusted Role • The organization prohibits access to the information system by users not designated as Trusted Roles of the PKI System **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-7	**UNSUCCESSFUL LOGIN ATTEMPTS**
AC-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occur;* *(ii) the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;* *(iii) the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:* − *lock out the account/node for a specified time period;* − *lock out the account/note until released by an administrator; or* − *delay the next login prompt according to organization-defined delay algorithm;* *(iv) the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded; and* *(v) the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures for the predetermined number of failed login attempts. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for unsuccessful login attempts].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-8	**SYSTEM USE NOTIFICATION**
AC-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization approves the information system use notification message or banner to be displayed by the information system before granting access to the system;* *(ii) the information system displays the approved 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:* - *users are accessing a U.S. Government information system;* - *system usage may be monitored, recorded, and subject to audit;* - *unauthorized use of the system is prohibited and subject to criminal and civil penalties; and* - *use of the system indicates consent to monitoring and recording; and* *(iii) the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding system use notification. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for system use notification].
AC-8.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;* *(ii) the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and* *(iii) the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding system use notification. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for system use notification].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-10	**CONCURRENT SESSION CONTROL**
AC-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum number of concurrent sessions to be allowed for each system account; and* *(ii) the information system limits the number of concurrent sessions for each system account to the organization-defined number of sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for concurrent session control].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-11	**SESSION LOCK**
AC-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of user inactivity after which the information system initiates a session lock;* *(ii) the information system initiates a session lock after the organization-defined time period of inactivity or upon receiving a request from a user;* *(iii) the information system retains the session lock until the user reestablishes access using established identification and authentication procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for session lock].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-14	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**
AC-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies specific user actions that can be performed on the information system without identification or authentication; and* *(ii) the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, which specify permitted actions that can be performed without identification and authentication, and any circumstances, limitations, or requirements on such actions.

AC-14(1)	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**
AC-14(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, which specify permitted actions that can be performed without identification and authentication, and any circumstances, limitations, or requirements on such actions.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-17	**REMOTE ACCESS**
AC-17.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization documents allowed methods of remote access to the information system;* *(ii) the organization establishes usage restrictions and implementation guidance for each allowed remote access method;* *(iii) the organization monitors for unauthorized remote access to the information system;* *(iv) the organization authorizes remote access to the information system prior to connection; and* *(v) the organization enforces requirements for remote connections to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with remote access authorization, monitoring, and control responsibilities]. **Test**: [*SELECT FROM:* Remote access methods for the information system].

AC-17(1)	REMOTE ACCESS
AC-17(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for remote access].

AC-17(2)	REMOTE ACCESS
AC-17(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses cryptography to protect the confidentiality and integrity of remote access sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing cryptographic protections for remote access].

AC-17(3)	REMOTE ACCESS
AC-17(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a limited number of managed access control points for remote access to the information system; and* *(ii) the information system routes all remote accesses through managed access control points.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for remote access].

AC-17(4)	REMOTE ACCESS
AC-17(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and* *(ii) the organization documents the rationale for such access in the security plan for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records].

AC-17(5)	REMOTE ACCESS
AC-17(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of monitoring for unauthorized remote connections to the information system;* *(ii) the organization monitors for unauthorized remote connections to the information system in accordance with the organization-defined frequency;* *(iii) the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and* *(iv) the organization takes organization-defined appropriate action(s) if an unauthorized connection is discovered.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for monitoring remote connections to the information system].

AC-17(7)	REMOTE ACCESS
AC-17(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions and security-relevant information that can be accessed using remote sessions;* *(ii) the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;* *(iii) the organization employs organization-defined additional security measures for remote sessions used to access organization-defined security functions and security-relevant information; and* *(iv) the organization audits remote sessions for accessing organization-defined security functions and security-relevant information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for remote access].

AC-17(8)	REMOTE ACCESS
AC-17(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the networking protocols within the information system deemed to be nonsecure; and* *(ii) the organization disables the organization-defined networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; security plan; list of networking protocols deemed to be non-secure; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms disabling networking protocols deemed to be non-secure].

AC-17(PKI)	REMOTE ACCESS
AC-17(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if remote access devices for administration of Certification Authorities require the same physical and logical controls as the CA itself.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures for the above control requirements and evidence that remote access devices for administration of Certification Authorities require the same physical and logical controls as the CA itself.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-18	**WIRELESS ACCESS**
AC-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for wireless access;* *(ii) the organization monitors for unauthorized wireless access to the information system;* *(iii) the organization authorizes wireless access to the information system prior to connection; and* *(iv) the organization enforces requirements for wireless connections to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system]. **Test**: [*SELECT FROM:* Wireless access usage and restrictions].

AC-18(1)	WIRELESS ACCESS
AC-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects wireless access to the system using authentication and encryption.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for wireless access to the information system].

AC-18(2)	WIRELESS ACCESS
AC-18(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of monitoring for unauthorized wireless connections to the information system, including scans for unauthorized wireless access points;* *(ii) the organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, in accordance with organization-defined frequency;* *(iii) the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and* *(iv) the organization takes appropriate action(s) if an unauthorized connection discovered.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel responsible for monitoring wireless connections to the information system]. **Test**: [*SELECT FROM:* Scanning procedures for detecting unauthorized wireless connections and access points].

AC-18(4)	WIRELESS ACCESS
AC-18(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization does not allow users to independently configure wireless networking capabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms preventing independent configuration of wireless networking capabilities].

AC-18(5)	WIRELESS ACCESS
AC-18(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization confines wireless communications to organization-controlled boundaries.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for wireless access to the information system; Wireless connections and access points outside of organizational boundaries using scanning devices.].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-19	**ACCESS CONTROL FOR MOBILE DEVICES**
AC-19.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices;* *(ii) the organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;* *(iii) the organization monitors for unauthorized connections of mobile devices to organizational information systems;* *(iv) the organization enforces requirements for the connection of mobile devices to organizational information systems;* *(v) the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;* *(vi) the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;* *(vii) the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk; and* *(viii) the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel who use portable and mobile devices to access the information system]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(1)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization restricts the use of writable, removable media in organizational information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel who use portable and mobile devices to access the information system]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(2)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits the use of personally owned, removable media in organizational information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(3)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-20	**USE OF EXTERNAL INFORMATION SYSTEMS**
AC-20.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies individuals authorized to:* - *access the information system from the external information systems; and* - *process, store, and/or transmit organization-controlled information using the external information systems; and* *(ii) 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:* - *access the information system from the external information systems; and* - *process, store, and/or transmit organization-controlled information using the external information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems].

AC-20(1)	USE OF EXTERNAL INFORMATION SYSTEMS
AC-20(1).1	**ASSESSMENT OBJECTIVE:** *Determine if 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:* – *can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or* – *has approved information system connection or processing agreements with the organizational entity hosting the external information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external information systems; security plan; information system connection or processing agreements; account management documents; other relevant documents or records].

AC-20(2)	USE OF EXTERNAL INFORMATION SYSTEMS
AC-20(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external information systems; security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records].

AC-20(PKI)	USE OF EXTERNAL INFORMATION SYSTEMS
AC-20(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if downloading/uploading of configuration information from/to the CA is restricted to authorized PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures that limit the use of external information systems to the repositories and CSS only.
AC-20(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if use of external systems to process, store, or transmit information is limited to/from the PKI repositories and CSS.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures that limit the use of external information systems to the repositories and CSS only.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-22	**PUBLICLY ACCESSIBLE CONTENT**
AC-22.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible;* *(ii) the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;* *(iii) the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;* *(iv) the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information;* *(v) the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization-defined frequency; and* *(vi) the organization removes nonpublic information from the publicly accessible organizational information system, if discovered.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures addressing publicly accessible content, and its posting, accessibility, control, and security. **Interview**: [*SELECT FROM:* Organizational personnel responsible for managing publicly accessible information posted on organizational information systems].

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

ASSESSMENT PROCEDURE	
AT-1	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**
AT-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents security awareness and training policy;* *(ii) the organization security awareness and training policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment; and* - *coordination among organizational entities, and compliance;* *(iii) the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;* *(iv) the organization develops and formally documents security awareness and training procedures;* *(v) the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls; and* *(vi) the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures for security awareness and training requirements. **Interview**: [*SELECT FROM:* Organizational personnel with security awareness and training responsibilities].
AT-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of security awareness and training policy reviews/updates;* *(ii) the organization reviews/updates security awareness and training policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of security awareness and training procedure reviews/updates; and* *(iv) the organization reviews/updates security awareness and training procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures for security awareness and training requirements. **Interview**: [*SELECT FROM:* Organizational personnel with security awareness and training responsibilities].

AT-1(PKI)	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AT-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local awareness and training policy, awareness and training policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for role-based security awareness and training policy and procedures for the following: • CA (or RA) security principles and mechanisms; • All PKI software versions in use on the CA (or RA) system; • All PKI duties they are expected to perform; • Disaster recovery and business continuity procedures; and • Stipulations of this policy.

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

ASSESSMENT PROCEDURE	
AT-2	**SECURITY AWARENESS**
AT-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;* *(ii) the organization defines the frequency of refresher security awareness training;* *(iii) the organization provides refresher security awareness training in accordance with the organization-defined frequency;* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures for security awareness training requirements. **Interview**: [*SELECT FROM:* Organizational personnel comprising the general information system user community].

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

ASSESSMENT PROCEDURE	
AT-3	**SECURITY TRAINING**
AT-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;* *(ii) the organization defines the frequency of refresher role-based security-related training;* *(iii) the organization provides refresher role-based security-related training in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant information system security responsibilities].
AT-3(PKI)	**SECURITY TRAINING**
AT-3(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local awareness and training policy, awareness and training policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for role-based security awareness and training policy and procedures for the following: • CA (or RA) security principles and mechanisms; • All PKI software versions in use on the CA (or RA) system; • All PKI duties they are expected to perform; • Disaster recovery and business continuity procedures; and • Stipulations of this policy.

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

ASSESSMENT PROCEDURE	
AT-4	**SECURITY TRAINING RECORDS**
AT-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training;* *(ii) the organization defines the time period for retaining individual training records; and* *(iii) the organization retains individual training records in accordance with the organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures for security awareness and training requirements. **Interview**: [*SELECT FROM:* Organizational personnel with security training record retention responsibilities].

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

ASSESSMENT PROCEDURE	
AU-1	**AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**
AU-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents audit and accountability policy;* *(ii) the organization audit and accountability policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;* *(iv) the organization develops and formally documents audit and accountability procedures;* *(v) the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls; and* *(vi) the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with audit and accountability responsibilities].
AU-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of audit and accountability policy reviews/updates;* *(ii) the organization reviews/updates audit and accountability policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of audit and accountability procedure reviews/updates; and* *(iv) the organization reviews/updates audit and accountability procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with audit and accountability responsibilities].

AU-1(PKI)	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
AU-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Audit and Accountability policy, Audit and Accountability policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Audit and Accountability policy and procedures, and frequency of review/update.

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

ASSESSMENT PROCEDURE	
AU-2	**AUDITABLE EVENTS**
AU-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the list of events the information system must be capable of auditing based on a risk assessment and mission/business needs;* *(ii) the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events; and* **(iii)** *the organization defines the subset of auditable events defined in (i) that are to be audited within the information system and the frequency of (or situation requiring) auditing for each identified event.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system auditing of organization-defined auditable events].

AU-2(3)	AUDITABLE EVENTS
AU-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of reviews and updates to the list of organization-defined auditable events; and* *(ii) the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities].

AU-2(4)	AUDITABLE EVENTS
AU-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; information system configuration settings and associated documentation; list of organization-defined auditable events; list of privileged security functions; other relevant documents or records].

AU-2(PKI)	AUDITABLE EVENTS
AU-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the minimum list of auditable events are specified in the PKI Certificate Policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the events audited match the list of auditable events recorded by the system.

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

ASSESSMENT PROCEDURE	
AU-3	**CONTENT OF AUDIT RECORDS**
AU-3.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system produces audit records that contain sufficient information to, at a minimum, establish:* – *what type of event occurred;* – *when (date and time) the event occurred;* – *where the event occurred;* – *the source of the event;* – *the outcome (success or failure) of the event; and* – *the identity of any user/subject associated with the event.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system auditing of auditable events].

AU-3(1)	CONTENT OF AUDIT RECORDS
AU-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject; and* *(ii) the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject].

AU-3(2)	CONTENT OF AUDIT RECORDS
AU-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the information system components for which the content of audit records generated is centrally managed; and* *(ii) the organization centrally manages the content of audit records generated by organization-defined information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing centralized management of audit record content].

AU-3(PKI)	CONTENT OF AUDIT RECORDS
AU-3(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if for enhancement (2), the organization's PKI Program controls and manages the content of audit records generated by the PKI CAs and RAs.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: The organizational personnel responsible for fulfilling the PKI Auditor Trusted Role to verify PKI Program controls and manages the content of audit records generated by the PKI CAs and RAs.

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

ASSESSMENT PROCEDURE	
AU-4	**AUDIT STORAGE CAPACITY**
AU-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization allocates audit record storage capacity; and* *(ii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Audit record storage capacity and related configuration settings].

AU-4(PKI)	**AUDIT STORAGE CAPACITY**
AU-4(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if audit logs for the PKI are backed up and archived prior to overwriting or deletion of the audit log.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify audit logs are backed up or archived prior to overwriting or deletion of the audit log. AND/OR **Interview**: The organizational personnel responsible for fulfilling the PKI Auditor Trusted Role to verify audit logs are backed up or archived prior to overwriting or deletion of the audit log.

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

ASSESSMENT PROCEDURE	
AU-5	**RESPONSE TO AUDIT PROCESSING FAILURES**
AU-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines designated organizational officials to be alerted in the event of an audit processing failure;* *(ii) the information system alerts designated organizational officials in the event of an audit processing failure;* *(iii) the organization defines additional actions to be taken in the event of an audit processing failure; and* *(iv) Takes the following additional actions: the appropriate authority as specified in the CP and CPS shall determine whether to suspend PKI System operation until the problem is remedied* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify that the Administrator (or comparable authority) determines whether to suspend PKI System operation in the event of an audit processing failure. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system response to audit processing failures].

AU-5(1)	RESPONSE TO AUDIT PROCESSING FAILURES
AU-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided; and* *(ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing audit storage limit warnings].

AU-5(2)	RESPONSE TO AUDIT PROCESSING FAILURES
AU-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines audit failure events requiring real-time alerts; and* *(ii) the information system provides a real-time alert when organization-defined audit failure events occur.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing real time audit alerts when organization-defined audit failure events occur].

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

ASSESSMENT PROCEDURE	
AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING**
AU-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system audit record reviews and analyses;* *(ii) the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; and* *(iii) the organization reports findings of inappropriate/unusual activities, to designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Information system audit review, analysis, and reporting capability].
AU-6.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information , intelligence information, or other credible sources of information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].

AU-6(1)	**AUDIT REVIEW, ANALYSIS, AND REPORTING**
AU-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; procedures for investigating and responding to suspicious activities; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities].

AU-6(7)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify permitted actions for each authorized information system process, role, and/or user for audit and accountability are specified.

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

ASSESSMENT PROCEDURE	
AU-7	**AUDIT REDUCTION AND REPORT GENERATION**
AU-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides an audit reduction and report generation capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Audit reduction and report generation capability].

AU-7(1)	AUDIT REDUCTION AND REPORT GENERATION
AU-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Audit reduction and report generation capability].

AU-7(PKI)	AUDIT REDUCTION AND REPORT GENERATION
AU-7(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if audit reduction and report generation tools are only used under the control of* PKI *Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: The organizational personnel responsible for fulfilling a PKI Trusted Role identified in the CP to verify audit reduction and report generation tools are only used under the control of Trusted Roles.

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

ASSESSMENT PROCEDURE	
AU-8	**TIME STAMPS**
AU-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses internal system clocks to generate time stamps for audit records.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures addressing time stamp generation; security plan(s); information system design documentation and configuration settings; and associated relevant documents and records. **Test**: [*SELECT FROM:* Automated mechanisms implementing time stamp generation].

AU-8(1)	**TIME STAMPS**
AU-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of internal clock synchronization for the information system;* *(ii) the organization defines the authoritative time source for internal clock synchronization; and* *(iii) the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures addressing time stamp generation; security plan(s); information system design documentation and configuration settings; and associated relevant documents and records. **Test**: [*SELECT FROM:* Automated mechanisms implementing internal information system clock synchronization].

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

ASSESSMENT PROCEDURE	
AU-9	**PROTECTION OF AUDIT INFORMATION**
AU-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects audit information and audit tools from unauthorized:* – *access;* – *modification; and* – *deletion.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures addressing the recording, retrieval, handling, and archival of audit records. **Test**: [*SELECT FROM:* Automated mechanisms implementing audit information protection].

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

ASSESSMENT PROCEDURE	
AU-10	**NON-REPUDIATION**
AU-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects against an individual falsely denying having performed a particular action.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures regarding the implementation of PKI as a technology to provide for technical non-repudiation. **Test**: [*SELECT FROM:* Automated mechanisms implementing non-repudiation capability].

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

ASSESSMENT PROCEDURE	
AU-11	**AUDIT RECORD RETENTION**
AU-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the retention period for audit records;* *(ii) the retention period for audit records is consistent with the records retention policy; and* *(iii) The organization retains audit records onsite for 2 months or until reviewed and archives audit records for 10 years and 6 months to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures addressing the recording, retrieval, handling, and archival of audit records. **Interview**: The organizational personnel responsible for fulfilling the PKI Auditor Trusted Role to verify the organization retains audit records onsite for 2 months or until reviewed and archives audit records for 10 years and 6 months. **Interview:** The organizational personnel responsible for fulfilling the PKI Auditor Trusted Role to verify the organization retains audit records onsite for 2 months or until reviewed and archives audit records for a period of time specified in the Certificate Policy (CP) and Certification Practices Statement (CPS).

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

ASSESSMENT PROCEDURE	
AU-12	**AUDIT GENERATION**
AU-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;* *(ii) the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;* *(iii) the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and* *(iv) the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3..* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures addressing the recording, retrieval, handling, and archival of audit records. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit record generation responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing audit record generation capability].

AU-12(1)	AUDIT GENERATION
AU-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system produces a system-wide (logical or physical) audit trail of information system audit records;* *(ii) the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail;* *(iii) the information system compiles audit records from organization-defined information system components into the system-wide audit trail;* *(iv) the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail; and* *(v) the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) audit and accountability policy and procedures addressing the recording, retrieval, handling, and archival of audit records. **Test**: [*SELECT FROM:* Automated mechanisms implementing audit record generation capability].

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

ASSESSMENT PROCEDURE	
CA-1	**SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES**
CA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents security assessment and authorization policy;* *(ii) the organization security assessment and authorization policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities;* *(iv) the organization develops and formally documents security assessment and authorization procedures;* *(v) the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and* *(vi) the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policies and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment and authorization responsibilities].
CA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of security assessment and authorization policy reviews/updates;* *(ii) the organization reviews/updates security assessment and authorization policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of security assessment and authorization procedure reviews/updates; and* *(iv) the organization reviews/updates security assessment and authorization procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policies and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment and authorization responsibilities].

CA-1(PKI)	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES
CA-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Security Assessment and Authorization policy, access control Security Assessment and Authorization are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Security Assessment and Authorization policy and procedures, and frequency of review/update.

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

ASSESSMENT PROCEDURE	
CA-2	**SECURITY ASSESSMENTS**
CA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a security assessment plan for the information system; and* *(ii) the security assessment plan describes the scope of the assessment including:* - *security controls and control enhancements under assessment;* - *assessment procedures to be used to determine security control effectiveness; and* - *assessment environment, assessment team, and assessment roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Security Assessment and Authorization policy and procedures; third-party PKI Compliance Audit requirements; and frequency of assessment and compliance audit review/update.
CA-2.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;* *(ii) the organization assesses the security controls in the information system at the organization-defined frequency;* *(iii) the organization produces a security assessment report that documents the results of the security control assessment; and* *(iv) the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Security Assessment and Authorization policy and procedures; third-party PKI Compliance Audit requirements; and frequency of assessment and compliance audit review/update. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

CA-2(1)	SECURITY ASSESSMENTS
CA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Security Assessment and Authorization policy and procedures; third-party PKI Compliance Audit requirements; and frequency of assessment and compliance audit review/update. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

CA-2(2)	SECURITY ASSESSMENTS
CA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *the forms of security testing to be included in security control assessments, selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing;* - *the frequency for conducting each form of security testing;* - *whether the security testing will be announced or unannounced; and* *(ii) the organization conducts security control assessments using organization-defined forms of testing in accordance with organization-defined frequency and assessment techniques established for each form of testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Security Assessment and Authorization policy and procedures; third-party PKI Compliance Audit requirements; and frequency of assessment and compliance audit review/update. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

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

ASSESSMENT PROCEDURE	
CA-3	**INFORMATION SYSTEM CONNECTIONS**
CA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);* *(ii) the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;* *(iii) the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and* *(iv) the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the interconnection of PKI CA and RA systems to both internal and external information systems. **Interview**: [*SELECT FROM:* Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements].

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

ASSESSMENT PROCEDURE	
CA-5	**PLAN OF ACTION AND MILESTONES**
CA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a plan of action and milestones for the information system;* *(ii) the plan of action and milestones documents 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;* *(iii) the organization defines the frequency of plan of action and milestone updates; and* *(iv) the organization updates the plan of action and milestones at an organization-defined frequency with findings from:* - *security controls assessments;* - *security impact analyses; and* - *continuous monitoring activities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with plan of action and milestones development and implementation responsibilities].

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

ASSESSMENT PROCEDURE	
CA-6	**SECURITY AUTHORIZATION**
CA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assigns a senior-level executive or manager to the role of authorizing official for the information system;* *(ii) the authorizing official authorizes the information system for processing before commencing operations;* *(iii) the organization defines the frequency of security authorization updates; and* *(iv) the organization updates the security authorization in accordance with an organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security authorization responsibilities].

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

ASSESSMENT PROCEDURE	
CA-7	**CONTINUOUS MONITORING**
CA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a continuous monitoring strategy and program;* *(ii) the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;* *(iii) the organization defines organizational officials to whom the security state of the information system should be reported; and* *(iv) the organization implements a continuous monitoring program that includes:* - *a configuration management process for the information system and its constituent components;* - *a determination of the security impact of changes to the information system and environment of operation;* - *ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and* - *reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities].

CA-7(PKI)	**CONTINUOUS MONITORING**
CA-7(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the Continuous Monitoring function is under the control of the PKI System Trusted Roles as defined in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify any continuous Monitoring functions are under the control of the PKI System Trusted Roles as defined in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-1	**CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**
CM-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents configuration management policy;* *(ii) the organization configuration management policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities;* *(iv) the organization develops and formally documents configuration management procedures;* *(v) the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; and* *(vi) the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management and control responsibilities].
CM-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of configuration management policy reviews/updates;* *(ii) the organization reviews/updates configuration management policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of configuration management procedure reviews/updates; and* *(iv) the organization reviews/updates configuration management procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management and control responsibilities].

CM-1(PKI)	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
CM-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Configuration Management policy, Configuration Management are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Configuration Management policy and procedures, and frequency of review/update.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-2	**BASELINE CONFIGURATION**
CM-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents a baseline configuration of the information system and* *(ii) the organization maintains, under configuration control, a current baseline configuration of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records].

CM-2(1)	BASELINE CONFIGURATION
CM-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *the frequency of reviews and updates to the baseline configuration of the information system; and* - *the circumstances that require reviews and updates to the baseline configuration of the information system; and* *(ii) the organization reviews and updates the baseline configuration of the information system* - *in accordance with the organization-defined frequency;* - *when required due to organization-defined circumstances; and* - *as an integral part of information system component installations and upgrades.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].

CM-2(3)	BASELINE CONFIGURATION
CM-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; historical copies of baseline configurations; other relevant documents or records].

CM-2(5)	BASELINE CONFIGURATION
CM-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and maintains a list of software programs authorized to execute on the information system; and* *(ii) the organization employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records].

CM-2(6)	BASELINE CONFIGURATION
CM-2(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing baseline configuration environments].

CM-2(PKI)	BASELINE CONFIGURATION
CM-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the PKI CA hardware, software, and middleware are dedicated to performing one task: the CA.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The baseline configuration documentation to ensure PKI CA hardware and software shall be dedicated to performing one task: the CA and that there shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.
CM-2(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine that no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The baseline configuration documentation to ensure PKI CA hardware and software shall be dedicated to performing one task: the CA and that there shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.
CM-2(PKI).3	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.* *(PKI Enhancement): Any automated mechanisms employed by the organization to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system shall be under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records]. **Interview**: The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify: 1. Any automated mechanisms employed by the organization to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system shall be under the control of PKI Trusted Roles 2. The PKI CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation **Test**: [*SELECT FROM:* Automated mechanisms implementing baseline configuration maintenance].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-3	**CONFIGURATION CHANGE CONTROL**
CM-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization determines the types of changes to the information system that are configuration controlled;* *(ii) the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses;* *(iii) the organization documents approved configuration-controlled changes to the system;* *(iv) the organization retains and reviews records of configuration-controlled changes to the system;* *(v) the organization audits activities associated with configuration-controlled changes to the system;* *(vi) the organization defines:* - *the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities;* - *the frequency with which the configuration change control element convenes; and/or;* - *configuration change conditions that prompt the configuration change control element to convene.* *(vii) the organization coordinates and provides oversight for configuration change control activities through the organization-defined configuration change control element that convenes at the organization-defined frequency and/or for any organization-defined configuration change conditions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].

CM-3(1)	CONFIGURATION CHANGE CONTROL
CM-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period after which approvals that have not been received for proposed changes to the information system are highlighted; and* *(ii) the organization employs automated mechanisms to:* - *document proposed changes to the information system;* - *notify designated approval authorities;* - *highlight approvals that have not been received by the organization-defined time period;* - *inhibit change until designated approvals are received; and* - *document completed changes to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing configuration change control].

CM-3(2)	CONFIGURATION CHANGE CONTROL
CM-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].
CM-3(PKI)	**CONFIGURATION CHANGE CONTROL**
CM-3(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if any automated mechanisms employed by the organization to implement changes to the current information system baseline and deploys updated baselines across the installed base are under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify: 1. Any automated mechanisms employed by the organization to implement changes to the current information system baseline and deploy updated baselines across the installed base are under the control of PKI Trusted Roles.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-4	**SECURITY IMPACT ANALYSIS**
CM-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements regarding the reliability of hardware, software, and middleware to be installed on the CAs. **Interview:** Trusted Role Administrators, Security Officers, and Officers responsible for receiving and installing hardware, software, and middleware to the CAs.

CM-4(1)	SECURITY IMPACT ANALYSIS
CM-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization analyzes new software in a separate test environment before installation in an operational environment; and* *(ii) the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements regarding the reliability of hardware, software, and middleware to be installed on the CAs. **Interview:** Trusted Role Administrators, Security Officers, and Officers responsible for receiving and installing hardware, software, and middleware to the CAs.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-5	**ACCESS RESTRICTIONS FOR CHANGE**
CM-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities]. **Test**: [*SELECT FROM:* Change control process and associated restrictions for changes to the information system].

CM-5(1)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access restrictions for changes to the information system].

CM-5(2)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for conducting audits of information system changes; and* *(ii) the organization conducts audits of information system changes in accordance with the organization-defined frequency and when indications so warrant to determine whether unauthorized changes have occurred.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records].

CM-5(3)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines critical software programs that the information system will prevent from being installed if such software programs are not signed with a recognized and approved certificate; and* *(ii) the information system prevents the installation of organization-defined critical software programs that are not signed with a certificate that is recognized and approved by the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; list of critical software programs to be prohibited from installation without an approved certificate; information system design documentation; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate].

CM-5(4)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system components and system-level information requiring enforcement of a two-person rule for information system changes; and* *(ii) The organization enforces a two-person rule for changes to CA Systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify multi-person control is required for changes to CA Systems. **Interview**: [*SELECT FROM:* Organizational personnel responsible for enforcing a two-person rule for system changes].

CM-5(PKI)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if all changes to hardware, software, and firmware components and system information directly within a production environment are administered by PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify: 1. Any changes to hardware, software, and firmware components and system information directly within a production environment are under the control of PKI Trusted Roles.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-6	**CONFIGURATION SETTINGS**
CM-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;* *(ii) the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;* *(iii) the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;* *(iv) the organization implements the security configuration settings;* *(v) the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and* *(vi) the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to determine the policy and procedures regarding how configuration settings are established and maintained; and, who is responsible for configuration settings. **Interview:** The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify how PKI-specific configuration settings are established and maintained.

CM-6(PKI)	CONFIGURATION SETTINGS
CM-6(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if configuration settings unique to the CA and RA systems are specified in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS);* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to determine the policy and procedures regarding how configuration settings are established and maintained; and, who is responsible for configuration settings. **Interview:** The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify how PKI-specific configuration settings are established and maintained.
CM-6(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.* *If the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings, this function must be under the control of the PKI System Trusted Roles as defined in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to determine the policy and procedures regarding how configuration settings are established and maintained; and, who is responsible for configuration settings. **Test**: [*SELECT FROM:* Automated mechanisms implementing the centralized management, application, and verification of configuration settings].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-7	**LEAST FUNCTIONALITY**
CM-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines for the information system prohibited or restricted:* - *functions;* - *ports;* - *protocols; and* - *services;* *(ii) the organization configures the information system to provide only essential capabilities; and* *(iii) the organization configures the information system to specifically prohibit or restrict the use of following [Control Assignment: as specified in the PKI CP and CPS]:* - *functions;* - *ports;* - *protocols; and/or* - *services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to determine the CA and RA information systems configuration settings to provide for least functionality. **Test**: [*SELECT FROM:* Information system for disabling or restricting functions, ports, protocols, and services].

CM-7(1)	LEAST FUNCTIONALITY
CM-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system reviews to identify and eliminate unnecessary:* - *functions;* - *ports;* - *protocols; and/or* - *services; and* *(ii) the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary:* - *functions;* - *ports;* - *protocols; and/or* - *services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to determine the CA and RA information systems configuration settings to provide for least functionality. **Interview:** The organizational personnel responsible for fulfilling the PKI Administrator Trusted Role to verify how PKI-specific configuration settings are established and maintained.

CM-7(2)	LEAST FUNCTIONALITY
CM-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and maintains one or more of the following specifications to prevent software program execution on the information system:* - *a list of software programs authorized to execute on the information system;* - *a list of software programs not authorized to execute on the information system; and/or* - *rules authorizing the terms and conditions of software program usage on the information system; and* *(ii) the organization employs automated mechanisms to prevent software program execution on the information system in accordance with the organization-defined specifications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to determine the CA and RA information systems configuration settings to provide for least functionality. **Test:** [*SELECT FROM:* Automated mechanisms preventing software program execution on the information system].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-8	**INFORMATION SYSTEM COMPONENT INVENTORY**
CM-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information deemed necessary to achieve effective property accountability; and* *(ii) the organization develops, documents, and maintains an inventory of information system components that:* - *accurately reflects the current information system;* - *is consistent with the authorization boundary of the information system;* - *is at the level of granularity deemed necessary for tracking and reporting;* - *includes organization-defined information deemed necessary to achieve effective property accountability; and* - *is available for review and audit by designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records].

CM-8(1)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization updates the inventory of information system components as an integral part of component:* - *installations;* - *removals; and* - *information system updates.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system installation and inventory responsibilities].

CM-8(2)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system component inventory management].

CM-8(3)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of employing automated mechanisms to detect the addition of unauthorized components/devices into the information system;* *(ii) the organization employs automated mechanisms, in accordance with the organization-defined frequency, to detect the addition of unauthorized components/devices into the information system; and* *(iii) the organization disables network access by such components/devices or notifies designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system design documentation; information system inventory records; component installation records; change control records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms for detecting unauthorized components/devices on the information system].

CM-8(4)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes in property accountability information for information system components, a means for identifying by name, position, or role, individuals responsible for administering those components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records].

CM-8(5)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; component installation records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system inventory responsibilities; organizational personnel with responsibilities for defining information system components within the authorization boundary of the system].

CM-8(PKI)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if automated inventory collection mechanisms do not violate the physical access, logical access, and network security requirements defined in the CP and CPS.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy and Certification Practices Statement (CPS) to determine the physical and logical access and network security requirements.

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-9	**CONFIGURATION MANAGEMENT PLAN**
CM-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops, documents, and implements a configuration management plan for the information system that:* – *addresses roles, responsibilities, and configuration management processes and procedures;* – *defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and* – *establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy and Certification Practices Statement (CPS), and any Configuration Management Plan, to determine how the configuration of CA and RA systems is defined and managed throughout the system life cycle.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-1	**CONTINGENCY PLANNING POLICY AND PROCEDURES**
CP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents contingency planning policy;* *(ii) the organization contingency planning policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;* *(iv) the organization develops and formally documents contingency planning procedures;* *(v) the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls; and* *(vi) the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning responsibilities].
CP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of contingency planning policy reviews/updates;* *(ii) the organization reviews/updates contingency planning policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of contingency planning procedure reviews/updates; and* *(iv) the organization reviews/updates contingency planning procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning responsibilities].

CP-1(PKI)	CONTINGENCY PLANNING POLICY AND PROCEDURES
CP-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Contingency Planning policy, Contingency Planning is specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Contingency Planning policy and procedures, and frequency of review/update.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-2	**CONTINGENCY PLAN**
CP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a contingency plan for the information system that:* - *identifies essential missions and business functions and associated contingency requirements;* - *provides recovery objectives, restoration priorities, and metrics;* - *addresses contingency roles, responsibilities, assigned individuals with contact information;* - *addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and* - *addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and* - *is reviewed and approved by designated officials within the organization;* *(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan; and* *(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency planning policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].
CP-2.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization coordinates contingency planning activities with incident handling activities:* *(ii) the organization defines the frequency of contingency plan reviews;* *(iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;* *(iv) the organization revises 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; and* *(v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements as identified in CP-2.1 (ii).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency planning policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities].

ASSESSMENT PROCEDURE	
CP-2(1)	**CONTINGENCY PLAN**
CP-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization coordinates the contingency plan development with other organizational elements responsible for related plans.* **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency planning policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas].

CP-2(2)	CONTINGENCY PLAN
CP-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency planning policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

CP-2(3)	CONTINGENCY PLAN
CP-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for planning the resumption of essential missions and business functions as a result of contingency plan activation; and* *(ii) the organization plans for the resumption of essential missions and business function within organization-defined time period of contingency plan activation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency planning policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-3	**CONTINGENCY TRAINING**
CP-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;* *(ii) the organization defines the frequency of refresher contingency training; and* *(iii) the organization provides refresher training in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency training policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and training responsibilities].

CP-3(1)	CONTINGENCY TRAINING
CP-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization incorporates simulated events into contingency training; and* *(ii) the incorporation of simulated events into contingency training facilitates effective response by personnel in crisis situations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency training policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and training responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-4	**CONTINGENCY PLAN TESTING AND EXERCISES**
CP-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the contingency plan tests and/or exercises to be conducted;* *(ii) the organization defines the frequency of contingency plan tests and/or exercises;* *(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; and* *(iv) the organization reviews the contingency plan test/exercise results and takes corrective actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency testing policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises].

CP-4(1)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency testing policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and testing responsibilities; organizational personnel with responsibilities for related plans].

CP-4(2)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts contingency plan testing/exercises at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency testing policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable.

CP-4(4)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for contingency testing policies and procedures, and the Contingency Plan(s) for PKI CA and RA systems as applicable. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency plan testing and/or exercise responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-6	**ALTERNATE STORAGE SITE**
CP-6.1	**ASSESSMENT OBJECTIVE:** *Determine if :* *(i) the organization establishes an alternate storage site; and* *(ii) the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate storage sites.

CP-6(1)	**ALTERNATE STORAGE SITE**
CP-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies the primary storage site hazards; and* *(ii) the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate storage sites.

CP-6(2)	**ALTERNATE STORAGE SITE**
CP-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate storage site is configured to facilitate recovery operations in accordance with recovery time objectives and recovery point objectives.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate storage sites.

CP-6(3)	ALTERNATE STORAGE SITE
CP-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and* *(ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate storage sites.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-7	**ALTERNATE PROCESSING SITE**
CP-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes an alternate processing site;* *(ii) the organization defines the time period for achieving the recovery time objectives within which processing must be resumed at the alternate processing site;* *(iii) the organization includes necessary alternate processing site agreements to permit the resumption of information system operations for essential missions and business functions within organization-defined time period; and* *(iv) the equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate processing sites.

CP-7(1)	ALTERNATE PROCESSING SITE
CP-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies the primary processing site hazards; and* *(ii) the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate processing sites.

CP-7(2)	ALTERNATE PROCESSING SITE
CP-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and* *(ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate processing sites.

CP-7(3)	ALTERNATE PROCESSING SITE
CP-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate processing sites.

CP-7(4)	ALTERNATE PROCESSING SITE
CP-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate processing site is configured so that it is ready to be used as the operational site to support essential missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate processing sites. **Test**: [*SELECT FROM:* Information system at the alternate processing site].

CP-7(5)	ALTERNATE PROCESSING SITE
CP-7(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate processing site provides information security measures equivalent to that of the primary site.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for the establishment, operation, and maintenance of alternate processing sites.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-8	**TELECOMMUNICATIONS SERVICES**
CP-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes alternate telecommunications services to support the information system;* *(ii) the organization defines in the time period within which resumption of information system operations must take place; and* *(iii) the organization establishes necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for alternate telecommunications services.

CP-8(1)	TELECOMMUNICATIONS SERVICES
CP-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements; and* *(ii) the organization 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.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for alternate telecommunications services.

CP-8(2)	TELECOMMUNICATIONS SERVICES
CP-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers].

CP-8(3)	TELECOMMUNICATIONS SERVICES
CP-8(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies the primary provider's telecommunications service hazards; and* *(ii) the alternate telecommunications service providers are separated from the primary telecommunications service providers so as not to be susceptible to the same hazards.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for alternate telecommunications services. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers].

CP-8(4)	TELECOMMUNICATIONS SERVICES
CP-8(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires primary and alternate telecommunications service providers to have contingency plans.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for requirements and Trusted Role responsibilities for alternate telecommunications services. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-9	**INFORMATION SYSTEM BACKUP**
CP-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives;* *(ii) the organization defines the frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives;* *(iii) the organization defines the frequency of conducting information system documentation backups (including security-related information) to support recovery time objectives and recovery point objectives;* *(iv) the organization backs up user-level information in accordance with the organization-defined frequency;* *(v) the organization backs up system-level information in accordance with the organization-defined frequency; and* *(vi) the organization backs up information system documentation in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding the backup of specified user, system, and system documentation information. **Interview**: [*SELECT FROM:* Organizational personnel with information system backup responsibilities].
CP-9.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects the confidentiality and integrity of backup information at the storage location.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding the backup of specified user, system, and system documentation information. **Interview**: [*SELECT FROM:* Organizational personnel with information system backup responsibilities].

CP-9(1)	**INFORMATION SYSTEM BACKUP**
CP-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system backup testing; and* *(ii) the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding the backup of specified user, system, and system documentation information.

CP-9(2)	INFORMATION SYSTEM BACKUP
CP-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding the backup of specified user, system, and system documentation information.

CP-9(3)	INFORMATION SYSTEM BACKUP
CP-9(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization stores backup copies of operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures regarding the backup of specified user, system, and system documentation information. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information system backup responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-10	**INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**
CP-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS), and any Contingency Plan(s), for policies and procedures for the recovery and reconstitution of the PKI CA; and for the timeframe and external notification requirements. **Test**: [*SELECT FROM:* Automated mechanisms and/or manual procedures for implementing information system recovery and reconstitution operations].

CP-10(2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements transaction recovery for systems that are transaction-based.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS), and any Contingency Plan(s), for policies and procedures for the recovery and reconstitution of the PKI CA; and for the timeframe and external notification requirements. **Test**: [*SELECT FROM:* Automated mechanisms implementing transaction recovery capability].

CP-10(3)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state; and* *(ii) the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS), and any Contingency Plan(s), for policies and procedures for the recovery and reconstitution of the PKI CA; and for the timeframe and external notification requirements. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities].

CP-10(4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time-periods within which information system components must be reimaged from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components; and* *(ii) the organization provides the capability to reimage information system components, within organization-defined time-periods, from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS), and any Contingency Plan(s), for policies and procedures for the recovery and reconstitution of the PKI CA; and for the timeframe and external notification requirements. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities].

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

ASSESSMENT PROCEDURE	
IA-1	**IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**
IA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents identification and authentication policy;* *(ii) the organization identification and authentication policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities;* *(iv) the organization develops and formally documents identification and authentication procedures;* *(v) the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls; and* *(vi) the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with identification and authentication responsibilities].
IA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of identification and authentication policy reviews/updates;* *(ii) the organization reviews/updates identification and authentication policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of identification and authentication procedure reviews/updates;* *(iv) the organization reviews/updates identification and authentication procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with identification and authentication responsibilities].

ASSESSMENT PROCEDURE	
IA-1(PKI)	**IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**
IA-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local identification and Authentication policy, identification and Authentication policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Identification and Authentication policy and procedures, and frequency of review/update.

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

ASSESSMENT PROCEDURE	
IA-2	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**
IA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(1)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for network access to privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(2)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for network access to non-privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(3)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for local access to privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(4)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for local access to non-privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(5)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and* *(ii) the organization requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(8)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and* *(ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(9)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(9).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the replay-resistant authentication mechanisms to be used for network access to non-privileged accounts; and* *(ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that Trusted Roles are uniquely authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

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

ASSESSMENT PROCEDURE	
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**
IA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system; and* *(ii) the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the policies and procedures to ensure that devices are uniquely identified and authenticated prior to taking any other action. **Test**: [*SELECT FROM:* Automated mechanisms implementing device identification and authentication].

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

ASSESSMENT PROCEDURE	
IA-4	**IDENTIFIER MANAGEMENT**
IA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages information system identifiers for users and devices by:* - *receiving authorization from a designated organizational official to assign a user or device identifier;* - *selecting an identifier that uniquely identifies an individual or device; and* - *assigning the user identifier to the intended party or the device identifier to the intended device.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with identifier management responsibilities].

IA-4(4)	IDENTIFIER MANAGEMENT
IA-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the characteristic to be used to identify user status; and* *(ii) the organization manages user identifiers by uniquely identifying the user with a PKI Trusted Role identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify Trusted Roles are uniquely authenticated prior to taking any other action.

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

ASSESSMENT PROCEDURE	
IA-5	**AUTHENTICATOR MANAGEMENT**
IA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period (by authenticator type) for changing/refreshing authenticators; and* *(ii) the organization manages information system authenticators for users and devices by:* - *verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;* - *establishing initial authenticator content for authenticators defined by the organization;* - *ensuring that authenticators have sufficient strength of mechanism for their intended use;* - *establishing and implementing administrative procedures for initial authenticator distribution;* - *establishing and implementing administrative procedures for lost/compromised or damaged authenticators;* - *establishing and implementing administrative procedures for revoking authenticators;* - *changing default content of authenticators upon information system installation;* - *establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);* - *changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;* - *protecting authenticator content from unauthorized disclosure and modification; and* - *requiring users to take, and having devices implement, specific measures to safeguard authenticators.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for determining initial authenticator content]. **Test**: [*SELECT FROM:* Automated mechanisms implementing authenticator management functions].

IA-5(1)	AUTHENTICATOR MANAGEMENT
IA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type;* *(ii) the organization defines the minimum number of characters that must be changed when new passwords are created;* *(iii) the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters;* *(iv) the organization defines the number of generations for which password reuse is prohibited; and* *(v) the information system, for password-based authentication:* - *enforces the minimum password complexity standards that meet the organization-defined requirements;* - *enforces the organization-defined minimum number of characters that must be changed when new passwords are created;* - *encrypts passwords in storage and in transmission;* - *enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and* - *prohibits password reuse for the organization-defined number of generations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing authenticator management functions].

IA-5(2)	AUTHENTICATOR MANAGEMENT
IA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, for PKI-based authentication:* - *validates certificates by constructing a certification path with status information to an accepted trust anchor;* - *enforces authorized access to the corresponding private key; and* - *maps the authenticated identity to the user account.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for PKI-based authentication management]. **Test**: [*SELECT FROM:* Automated mechanisms implementing PKI-based authenticator management functions].

IA-5(3)	AUTHENTICATOR MANAGEMENT
IA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and* *(ii) the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with authenticator management responsibilities].

IA-5(6)	AUTHENTICATOR MANAGEMENT
IA-5(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects authenticators commensurate with the classification or sensitivity of the information accessed.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify the PKI protects authenticators commensurate with the classification or sensitivity of the information accessed. **Interview**: [*SELECT FROM:* Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections].

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

ASSESSMENT PROCEDURE	
IA-6	**AUTHENTICATOR FEEDBACK**
IA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing authenticator feedback].

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

ASSESSMENT PROCEDURE	
IA-7	**CRYPTOGRAPHIC MODULE AUTHENTICATION**
IA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses 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.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify that the CA information system uses mechanisms for authentication to the hardware cryptographic module that meet the requirements of FIPS 140. **Test**: [*SELECT FROM:* Automated mechanisms implementing cryptographic module authentication].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-1	**INCIDENT RESPONSE POLICY AND PROCEDURES**
IR-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents incident response policy;* *(ii) the organization incident response policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;* *(iv) the organization develops and formally documents incident response procedures;* *(v) the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls; and* *(vi) the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response responsibilities].
IR-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of incident response policy reviews/updates;* *(ii) the organization reviews/updates incident response policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of incident response procedure reviews/updates; and* *(iv) the organization reviews/updates incident response procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response responsibilities].

IR-1(PKI)	INCIDENT RESPONSE POLICY AND PROCEDURES
IR-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Incident Response policy, Incident Response policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Incident Response policy and procedures, and frequency of review/update.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-2	**INCIDENT RESPONSE TRAINING**
IR-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies personnel with incident response roles and responsibilities with respect to the information system;* *(ii) the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;* *(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; and* *(iv) the organization provides refresher incident response training as required by local policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Incident Response policy and procedures initial and refresher training, and the frequency of training. **Interview**: [*SELECT FROM:* Organizational personnel with incident response training and operational responsibilities].

IR-2(1)	**INCIDENT RESPONSE TRAINING**
IR-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Incident Response policy and procedures initial and refresher training, and the frequency of training. **Interview**: [*SELECT FROM:* Organizational personnel with incident response training and operational responsibilities].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-3	**INCIDENT RESPONSE TESTING AND EXERCISES**
IR-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines incident response tests/exercises;* *(ii) the organization defines the frequency of incident response tests/exercises;* *(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;* *(iv) the organization documents the results of incident response tests/exercises; and* *(v) the organization determines the effectiveness of the incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Incident Response testing and exercises policy and procedures. **Interview:** [*SELECT FROM:* Organizational personnel with incident response testing responsibilities].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-4	**INCIDENT HANDLING**
IR-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization implements an incident handling capability for security incidents that includes:* - *preparation;* - *detection and analysis;* - *containment;* - *eradication; and* - *recovery;* *(ii) the organization coordinates incident handling activities with contingency planning activities; and* *(iii) the organization incorporates lessons learned from ongoing incident handling activities into:* - *incident response procedures;* - *training; and* - *testing/exercises; and* *(iv) the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities]. **Test**: [*SELECT FROM:* Incident handling capability for the organization].

IR-4(3)	**INCIDENT HANDLING**
IR-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies classes of incidents; and* *(ii) the organization defines the appropriate actions to take in response to each class of incidents to ensure continuation of organizational missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities].

IR-4(PKI)	INCIDENT HANDLING
IR-4(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) automated Incident Response mechanisms are implemented on the CA; and* *(ii) control of these mechanisms are limited to Trusted Roles.*

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-5	**INCIDENT MONITORING**
IR-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tracks and documents information system security incidents.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident monitoring responsibilities]. **Test**: [*SELECT FROM:* Incident monitoring capability for the organization].

IR-5(PKI)	**INCIDENT MONITORING**
IR-5(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if any automated mechanisms used to support incident monitoring are under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure control of any automated mechanisms are limited to Trusted Roles.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-6	**INCIDENT REPORTING**
IR-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines in the time period required to report suspected security incidents to the organizational incident response capability;* *(ii) the organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period; and* *(iii) the organization reports security incident information to designated authorities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident reporting responsibilities].

IR-6(PKI)	**INCIDENT REPORTING**
IR-6(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if any automated mechanisms used to support incident reporting are under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure control of any automated mechanisms are limited to Trusted Roles.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-7	**INCIDENT RESPONSE ASSISTANCE**
IR-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and* *(ii) the incident response support resource is an integral part of the organization's incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response assistance and support responsibilities].

IR-7(2)	**INCIDENT RESPONSE ASSISTANCE**
IR-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and* *(ii) the organization identifies organizational incident response team members to the external providers.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response support and assistance responsibilities; external providers of information system protection capability].

IR-7(PKI)	**INCIDENT RESPONSE ASSISTANCE**
IR-7(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if automated mechanisms used to support incident response are under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure control of any automated mechanisms are limited to Trusted Roles.

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-8	**INCIDENT RESPONSE PLAN**
IR-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops an incident response plan that:* – *provides the organization with a roadmap for implementing its incident response capability;* – *describes the structure and organization of the incident response capability;* – *provides a high-level approach for how the incident response capability fits into the overall organization;* – *meets the unique requirements of the organization, which relate to mission, size, structure, and functions;* – *defines reportable incidents;* – *provides metrics for measuring the incident response capability within the organization;* – *defines the resources and management support needed to effectively maintain and mature an incident response capability; and* – *is reviewed and approved by designated officials within the organization*. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Incident Response planning policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with incident response planning responsibilities].
IR-8.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;* *(ii) the organization distributes copies of the incident response plan to PKI Trusted Roles identified in the CP and the organization's PKI Policy Authority;* *(iii) the organization defines, in the incident response plan, the frequency to review the plan;* *(iv) the organization reviews the incident* response plan Annually*;* *(v) the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and* *(vi) the organization communicates incident response plan changes to PKI Trusted Roles identified in the CP and the organization's PKI Policy Authority.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Incident Response planning policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with incident response planning responsibilities].

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-1	**SYSTEM MAINTENANCE POLICY AND PROCEDURES**
MA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system maintenance policy;* *(ii) the organization system maintenance policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;* *(iv) the organization develops and formally documents system maintenance procedures;* *(v) the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls; and* *(vi) the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].
MA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system maintenance policy reviews/updates;* *(ii) the organization reviews/updates system maintenance policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of system maintenance procedure reviews/updates;* *(iv) the organization reviews/updates system maintenance procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-1(PKI)	SYSTEM MAINTENANCE POLICY AND PROCEDURES
MA-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local System Maintenance policy, System Maintenance policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System Maintenance policy and procedures, and frequency of review/update.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-2	**CONTROLLED MAINTENANCE**
MA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization 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;* *(ii) the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;* *(iii) the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;* *(iv) the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and* *(v) the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-2(1)	**CONTROLLED MAINTENANCE**
MA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains maintenance records for the information system that include:* - *date and time of maintenance;* - *name of the individual performing the maintenance;* - *name of escort, if necessary;* - *a description of the maintenance performed; and* - *a list of equipment removed or replaced (including identification numbers, if applicable).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records].

MA-2(PKI)	CONTROLLED MAINTENANCE
MA-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if maintenance of the PKI System Components is performed under the control of the PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure Maintenance of the PKI System Components is performed under the control of Trusted Roles.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-3	**MAINTENANCE TOOLS**
MA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization approves, controls, and monitors the use of information system maintenance tools; and* *(ii) the organization maintains information system maintenance tools on an ongoing basis.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records].

MA-3(1)	**MAINTENANCE TOOLS**
MA-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-3(3)	**MAINTENANCE TOOLS**
MA-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prevents the unauthorized removal of maintenance equipment by one of the following:* - *verifying that there is no organizational information contained on the equipment;* - *sanitizing or destroying the equipment;* - *retaining the equipment within the facility; or* - *obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-3(PKI)	MAINTENANCE TOOLS
MA-3(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if any diagnostic and test programs or equipment used on the PKI System are approved by the PKI Operational or Policy Management Authority prior to use and are used under the control of the PKI Trusted Roles identified in the CP; and* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure any diagnostic and test programs or equipment used on the PKI System shall be approved by the PKI Operational or Policy Management Authority prior to use and shall be used under the control of the Trusted Roles and that the Trusted Roles are responsible for checking all media containing diagnostic and test programs for malicious code before the media are used in the information system.
MA-3(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if the Trusted Roles are responsible for checking all media containing diagnostic and test programs for malicious code before the media are used in the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure any diagnostic and test programs or equipment used on the PKI System shall be approved by the PKI Operational or Policy Management Authority prior to use and shall be used under the control of the Trusted Roles and that the Trusted Roles are responsible for checking all media containing diagnostic and test programs for malicious code before the media are used in the information system.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-4(PKI)	**NON-LOCAL MAINTENANCE**
MA-4(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) Non-local maintenance is only permitted if all the control requirements apply equally to the CA and any remote workstations used to administer the CA.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to ensure Non-local maintenance is only permitted if all the control requirements apply equally to the CA and any remote workstations used to administer the CA. **Interview**: PKI Trusted Roles identified in the CP to ensure Non-local maintenance is only permitted if all the control requirements apply equally to the CA and any remote workstations used to administer the CA.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-5	**MAINTENANCE PERSONNEL**
MA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a process for maintenance personnel authorization;* *(ii) the organization maintains a current list of authorized maintenance organizations or personnel; and* *(iii) personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-5(PKI)	**MAINTENANCE PERSONNEL**
MA-5(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if maintenance personnel are under the supervision of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure Maintenance personnel are under the supervision of Trusted Roles.

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-6	**TIMELY MAINTENANCE**
MA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines security-critical information system components and/or key information technology components for which it will obtain maintenance support and/or spare parts;* *(ii) the organization defines the time period within which support and/or spare parts must be obtained after a failure; and* *(iii) the organization obtains maintenance support and/or spare parts for any PKI System Component within a maximum of 72 hours of failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policies and procedures requiring provision of maintenance support and time limits on the CA information system down time. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-1	**MEDIA PROTECTION POLICY AND PROCEDURES**
MP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents media protection policy;* *(ii) the organization media protection policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;* *(iv) the organization develops and formally documents media protection procedures;* *(v) the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls; and* *(vi) the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Media protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].
MP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of media protection policy reviews/updates;* *(ii) the organization reviews/updates media protection policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of media protection procedure reviews/updates;* *(iv) the organization reviews/updates media protection procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Media protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].

MP-1(PKI)	MEDIA PROTECTION POLICY AND PROCEDURES
MP-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Media Protection policy, Media Protection policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Media Protection policy and procedures, and frequency of review/update.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-2	**MEDIA ACCESS**
MP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *digital and non-digital media requiring restricted access;* - *individuals authorized to access the media;* - *security measures taken to restrict access; and* *(ii) the organization restricts access to all media to PKI Trusted Roles identified in the CP using procedures defined in the CPS.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].

MP-2(PKI)	**MEDIA ACCESS**
MP-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs control mechanisms to restrict access to media storage areas and to audit access attempts and access granted as defined in the CPS.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to ensure access control mechanisms for media are specified.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-3	**MEDIA MARKING**
MP-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines removable media types and information system output that require marking;* *(ii) the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;* *(iii) the organization defines:* - *removable media types and information system output exempt from marking;* - *controlled areas designated for retaining removable media and information output exempt from marking; and* *(iv) removable media and information system output exempt from marking remain within designated controlled areas.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection and marking responsibilities].

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-4	**MEDIA STORAGE**
MP-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *types of digital and non-digital media physically controlled and securely stored within designated controlled areas;* - *controlled areas designated to physically control and securely store the media;* - *security measures to physically control and securely store the media within designated controlled areas;* *(ii) the organization physically controls and securely stores all CA media within PKI System-controlled areas using procedures defined in the CPS; and* *(iii) the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Media Storage policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection and storage responsibilities].

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-5	**MEDIA TRANSPORT**
MP-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *types of digital and non-digital media protected and controlled during transport outside of controlled areas;* - *security measures (e.g., locked container, encryption) for such media transported outside of controlled areas;* *(ii) the organization protects and controls all CA media during transport outside of controlled areas using Mitigating security mechanisms;* *(iii) the organization maintains accountability for information system media during transport outside of controlled areas;* *(iv) the organization identifies personnel authorized to transport information system media outside of controlled areas; and* *(v) the organization restricts the activities associated with transport of information system media to authorized personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media transport responsibilities].

MP-5(2)	**MEDIA TRANSPORT**
MP-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization documents activities associated with the transport of information system media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media transport records; audit records; other relevant documents or records].

MP-5(3)	MEDIA TRANSPORT
MP-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an identified custodian throughout the transport of information system media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media transport responsibilities].

MP-5(PKI)	MEDIA TRANSPORT
MP-5(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs mitigating security mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure security mechanisms are required to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. **Interview**: PKI Trusted Roles identified in the CP to ensure security mechanisms are implemented to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-6	**MEDIA SANITIZATION**
MP-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization sanitizes information system media both digital and non-digital prior to:* - *disposal;* - *release out of organizational control; or* - *release for reuse; and* *(ii) the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for media sanitization policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(1)	MEDIA SANITIZATION
MP-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for media sanitization policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(2)	MEDIA SANITIZATION
MP-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance; and* *(ii) the organization tests sanitization equipment and procedures to verify correct performance in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for media sanitization policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(3)	MEDIA SANITIZATION
MP-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines circumstances requiring sanitization of portable, removable storage devices prior to connecting such devices to the information system; and* *(ii) the organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under organization-defined circumstances.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for media sanitization policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-1	**PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**
PE-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents physical and environmental protection policy;* *(ii) the organization physical and environmental protection policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;* *(iv) the organization develops and formally documents physical and environmental protection procedures;* *(v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and* *(vi) the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical and environmental protection responsibilities].
PE-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of physical and environmental protection policy reviews/updates;* *(ii) the organization reviews/updates physical and environmental protection policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of physical and environmental protection procedure reviews/updates;* *(iv) the organization reviews/updates physical and environmental protection procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical and environmental protection responsibilities].

PE-1(PKI)	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
PE-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Physical and Environmental Protection policy, Physical and Environmental Protection policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Physical and Environmental Protection policy and procedures, and frequency of review/update.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-2	**PHYSICAL ACCESS AUTHORIZATIONS**
PE-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies areas within the facility that are publicly accessible;* *(ii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and* *(iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; other relevant documents or records].
PE-2.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility;* *(ii) organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and* *(iii) the organization removes from the access list personnel no longer requiring access.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; other relevant documents or records].

PE-2(1)	**PHYSICAL ACCESS AUTHORIZATIONS**
PE-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies personnel positions or roles authorized for physical access to the facility where the information system resides; and* *(ii) the organization authorizes physical access to the facility where the information system resides based on position or role.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; physical access control logs or records; information system entry and exit points; other relevant documents or records].

PE-2(PKI)	PHYSICAL ACCESS AUTHORIZATIONS
PE-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if multi-party control by specified PKI Trusted Roles identified in the CP is required for access to PKI CA information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to ensure multi-party control is required for access to PKI CA information systems. **Interview**: PKI Trusted Roles identified in the CP to ensure multi-party control by specified Trusted Roles is implemented for access to PKI CA information systems.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-3	**PHYSICAL ACCESS CONTROL**
PE-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);* *(ii) the organization verifies individual access authorizations before granting access to the facility;* *(iii) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;* *(iv) the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; and* *(v) the organization secures keys, combinations, and other physical access devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; storage locations for physical access devices; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical access control responsibilities]. **Test**: [*SELECT FROM:* Physical access control capability; physical access control devices].
PE-3.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for conducting inventories of physical access devices;* *(ii) the organization inventories physical access devices in accordance with the organization-defined frequency;* *(iii) the organization defines the frequency of changes to combinations and keys; and* *(iv) the organization changes combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records]. **Test**: [*SELECT FROM:* Physical access control devices].

PE-3(1)	PHYSICAL ACCESS CONTROL
PE-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records].

PE-3(PKI)	PHYSICAL ACCESS CONTROL
PE-3(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if multi-party control by specified PKI Trusted Roles identified in the CP is required for access to PKI CA information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to ensure multi-party control is required for access to PKI CA information systems. **Interview**: PKI Trusted Roles identified in the CP to ensure multi-party control by specified Trusted Roles is implemented for access to PKI CA information systems.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-4	**ACCESS CONTROL FOR TRANSMISSION MEDIUM**
PE-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for transmission medium access control policy and procedures.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-5	**ACCESS CONTROL FOR OUTPUT DEVICES**
PE-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for output device access control policy and procedures.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-6	**MONITORING PHYSICAL ACCESS**
PE-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization monitors physical access to the information system to detect and respond to physical security incidents;* *(ii) the organization defines the frequency to review physical access logs;* *(iii) the organization reviews physical access logs in accordance with the organization-defined frequency; and* *(iv) the organization coordinates results of reviews and investigations with the organization's incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for physical access control policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with physical access monitoring responsibilities]. **Test**: [*SELECT FROM:* Physical access monitoring capability].

PE-6(1)	MONITORING PHYSICAL ACCESS
PE-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization monitors real-time physical intrusion alarms and surveillance equipment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for physical access control policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with physical access monitoring responsibilities]. **Test**: [*SELECT FROM:* Physical access monitoring capability].

PE-6(2)	MONITORING PHYSICAL ACCESS
PE-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for physical access control policy and procedures. **Test**: [*SELECT FROM:* Automated mechanisms implementing physical access monitoring capability].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-7	**VISITOR CONTROL**
PE-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for visitor access control policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with visitor access control responsibilities]. **Test**: [*SELECT FROM:* Visitor access control capability].

PE-7(1)	**VISITOR CONTROL**
PE-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization escorts visitors and monitors visitor activity, when required.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for visitor access control policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with visitor access control responsibilities].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-8	**ACCESS RECORDS**
PE-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);* *(ii) the organization defines the frequency to review visitor access records;* *(iii) the organization reviews the visitor access records in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for visitor access control policy and procedures. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for reviewing physical access records].

PE-8(2)	**ACCESS RECORDS**
PE-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for visitor access control policy and procedures.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-9	**POWER EQUIPMENT AND POWER CABLING**
PE-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-10	**EMERGENCY SHUTOFF**
PE-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides the capability of shutting off power to the information system or individual system components in emergency situations;* *(ii) the organization defines the location of emergency shutoff switches or devices by information system or system component;* *(iii) the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel; and* *(iv) the organization protects the emergency power shutoff capability from unauthorized activation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-11	**EMERGENCY POWER**
PE-11.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls. **Test**: [*SELECT FROM:* Uninterruptible power supply].

PE-11(1)	**EMERGENCY POWER**
PE-11(1).1	**ASSESSMENT OBJECTIVE:** *Determine if 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.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls. **Test**: [*SELECT FROM:* Alternate power supply].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-12	**EMERGENCY LIGHTING**
PE-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;* *(ii) the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility; and* *(iii) the organization maintains the automatic emergency lighting for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls. **Interview**: [*SELECT FROM:* Organizational personnel with emergency planning responsibilities]. **Test**: [*SELECT FROM:* Emergency lighting capability].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-13	**FIRE PROTECTION**
PE-13.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source; and* *(ii) the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility fire protection. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems].

PE-13(1)	**FIRE PROTECTION**
PE-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility fire protection. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems]. **Test**: [*SELECT FROM:* Simulated activation of fire detection devices/systems and automated notifications].

PE-13(2)	**FIRE PROTECTION**
PE-13(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility fire protection. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems]. **Test**: [*SELECT FROM:* Simulated activation of fire suppression devices/systems and automated notifications].

PE-13(3)	FIRE PROTECTION
PE-13(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility fire protection. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems]. **Test**: [*SELECT FROM:* Simulated activation of fire suppression devices/systems].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-14	**TEMPERATURE AND HUMIDITY CONTROLS**
PE-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;* *(ii) the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;* *(iii) the organization defines the frequency to monitor temperature and humidity levels; and* *(iv) the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-15	**WATER DAMAGE PROTECTION**
PE-15.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly; and* *(ii) key personnel within the organization have knowledge of the master water shutoff valves.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls. **Interview**: [*SELECT FROM:* Organization personnel with physical and environmental protection responsibilities]. **Test**: [*SELECT FROM:* Master water-shutoff valves; process for activating master water-shutoff].

PE-15(1)	WATER DAMAGE PROTECTION
PE-15(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls. **Test**: [*SELECT FROM:* Automated mechanisms implementing master water shutoff valve activation].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-16	**DELIVERY AND REMOVAL**
PE-16.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of information system components to be authorized, monitored, and controlled as such components are entering or exiting the facility;* *(ii) the organization authorizes, monitors, and controls all PKI System components entering and exiting the facility; and* *(iii) the organization maintains records of information system components entering and exiting the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for material handling policy and procedures. **Interview**: [*SELECT FROM:* Organization personnel with responsibilities for controlling information system components entering and exiting the facility]. **Test**: [*SELECT FROM:* Process for controlling information system-related items entering and exiting the facility].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-17	**ALTERNATE WORK SITE**
PE-17.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites;* *(ii) the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites;* *(iii) the organization assesses, as feasible, the effectiveness of security controls at alternate work sites; and* *(iv) the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for PKI CA facility access control policy and procedures. **Interview**: [*SELECT FROM:* Organization personnel using alternate work sites].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-18	**LOCATION OF INFORMATION SYSTEM COMPONENTS**
PE-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and* *(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls.

PE-18(1)	**LOCATION OF INFORMATION SYSTEM COMPONENTS**
PE-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards; and* *(ii) the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA facility environmental controls. **Interview**: [*SELECT FROM:* Organization personnel with site selection responsibilities for the facility housing the information system].

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-1	**SECURITY PLANNING POLICY AND PROCEDURES**
PL-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents security planning policy;* *(ii) the organization security planning policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;* *(iv) the organization develops and formally documents security planning procedures;* *(v) the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls; and* *(vi) the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security planning responsibilities].
PL-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of security planning policy reviews/updates;* *(ii) the organization reviews/updates security planning policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of security planning procedure reviews/updates;* *(iv) the organization reviews/updates security planning procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security planning responsibilities].

PL-1(PKI)	SECURITY PLANNING POLICY AND PROCEDURES
PL-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Security Planning policy, Security Planning policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Security Planning policy and procedures, and frequency of review/update.

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-2	**SYSTEM SECURITY PLAN**
PL-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a security plan for the information system that:* - *is consistent with the organization's enterprise architecture;* - *explicitly defines the authorization boundary for the system;* - *describes the operational context of the information system in terms of mission and business processes;* - *provides the security categorization of the information system including supporting rationale;* - *describes the operational environment for the information system;* - *describes relationships with or connections to other information systems;* - *provides an overview of the security requirements for the system;* - *describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions; and* - *is reviewed and approved by the authorizing official or designated representative prior to plan implementation;* *(ii) the organization defines the frequency of security plan reviews;* *(iii) the organization reviews the security plan in accordance with the organization-defined frequency; and* *(iv) the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA system security planning requirements. **Interview**: [*SELECT FROM:* Organization personnel with security planning and plan implementation responsibilities for the information system].

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-4	**RULES OF BEHAVIOR**
PL-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;* *(ii) the organization makes the rules available to all information system users; and* *(iii) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding rules governing the responsibilities and behavior of PKI Trusted Roles identified in the CP and PKI Subscribers/Sponsors. **Interview**: [*SELECT FROM:* Organizational personnel who are authorized users of the information system and have signed rules of behavior].

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-5	**PRIVACY IMPACT ASSESSMENT**
PL-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts a privacy impact assessment on the information system; and* *(ii) the privacy impact assessment is in accordance with OMB policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the protection of privacy information and preparation of Privacy Impact Assessments and Privacy Plans.

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-6	**SECURITY-RELATED ACTIVITY PLANNING**
PL-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding PKI CA system security planning requirements. **Interview**: [*SELECT FROM:* Organizational personnel with security planning and plan implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-1	**INFORMATION SECURITY PROGRAM PLAN**
PM-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops an information security program plan for the organization that:* - *provides an overview of the requirements for the security program;* - *provides a description of the security program management controls and common controls in place or planned for meeting security program requirements;* - *provides sufficient information about the program management controls and common controls (including specification of parameters for any* assignment *and* selection *operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;* - *includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;* - *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;* *(ii) the organization defines the frequency of information security program plan reviews;* *(iii) the organization reviews the organization-wide information security program plan in accordance with the organization-defined frequency;* *(iv) the organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments; and* *(v) the organization disseminates the most recent information security program plan to appropriate entities in the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security planning and plan implementation responsibilities for the information security program].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-2	**SENIOR INFORMATION SECURITY OFFICER**
PM-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) organization appoints a senior information security officer to coordinate, develop, implement, and maintain an organization-wide information security program; and* *(ii) the organization empowers the senior information security officer with the mission and resources required to coordinate, develop, implement, and maintain an organization-wide information security program.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational person appointed to the senior information security officer position].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-3	**INFORMATION SECURITY RESOURCES**
PM-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization includes in its capital planning and investment requests the resources needed to implement the information security program;* *(ii) the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program;* *(iii) the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and* *(iv) the organization makes the required information security resources available for expenditure as planned.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; Exhibit 300; Exhibit 53; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-4	**PLAN OF ACTION AND MILESTONES PROCESS**
PM-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and* *(ii) the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with plan of action and milestones development and implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-5	**INFORMATION SYSTEM INVENTORY**
PM-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops an inventory of its information systems; and* *(ii) the organization maintains an inventory of its information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; procedures addressing information system inventory development and maintenance; information system inventory records, other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system inventory development and maintenance responsibilities].

PM-5(PKI)	**INFORMATION SYSTEM INVENTORY**
PM-5(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if inventory of PKI System Components is performed under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure inventory of PKI System Components is performed under the control of Trusted Roles.

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-6	**INFORMATION SECURITY MEASURES OF PERFORMANCE**
PM-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops information security measures of performance;* *(ii) the organization monitors information security measures of performance; and* *(iii) the organization reports on the results of information security measures of performance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; procedures addressing development, monitoring, and reporting of information security performance measures; information security performance metrics; information security performance measures; results of information security performance measures; other relevant documents or records].

PM-6(PKI)	**INFORMATION SECURITY MEASURES OF PERFORMANCE**
PM-6(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if monitoring and reporting of information security measures of PKI System Components performance is performed under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure Monitoring and reporting of information security measures of PKI System Components performance is performed under the control of Trusted Roles.

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-7	**ENTERPRISE ARCHITECTURE**
PM-7.1	**ASSESSMENT OBJECTIVE:** *Determine if 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.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-8	**CRITICAL INFRASTRUCTURE PLAN**
PM-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents a critical infrastructure and key resource protection plan;* *(ii) the organization updates the critical infrastructure and key resource protection plan; and* *(iii) the organization addresses information security issues in the critical infrastructure and key resource protection plan.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; critical infrastructure protection policy; procedures addressing critical infrastructure plan development and implementation; procedures addressing critical infrastructure plan reviews and updates; records of critical infrastructure plan reviews and updates; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with critical infrastructure plan development and implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-9	**RISK MANAGEMENT STRATEGY**
PM-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization 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; and* *(ii) the organization implements that strategy consistently across the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk management strategy development and implementation responsibilities].

PM-9(PKI)	RISK MANAGEMENT STRATEGY
PM-9(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if :* *(i) PKI is used to manage and mitigate risk to other systems and information; and* *(ii) the risk management strategy in the PKI environment is specific to the PKI infrastructure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI System Security Plan (SSP) to ensure the risk management strategy for the PKI System is specific to the PKI System.

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-10	**SECURITY AUTHORIZATION PROCESS**
PM-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; and* *(ii) the organization fully integrates the security authorization processes into an organization-wide risk management program.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities].

PM-10(PKI)	SECURITY AUTHORIZATION PROCESS
PM-10(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the specific roles and responsibilities for the risk management process are the Trusted Roles or other responsible parties as defined by the PKI CP and CPS.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure the specific roles and responsibilities for the risk management process are identified.

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-11	**MISSION / BUSINESS PROCESS DEFINITION**
PM-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and* *(ii) the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; risk management policy; procedures addressing security categorization of organizational information and information systems; organizational mission/business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with mission/business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-1	**PERSONNEL SECURITY POLICY AND PROCEDURES**
PS-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents personnel security policy;* *(ii) the organization personnel security policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;* *(iv) the organization develops and formally documents personnel security procedures;* *(v) the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls; and* *(vi) the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy and procedures, other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].
PS-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of personnel security policy reviews/updates;* *(ii) the organization reviews/updates personnel security policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of personnel security procedure reviews/updates;* *(iv) the organization reviews/updates personnel security procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

PS-1(PKI)	PERSONNEL SECURITY POLICY AND PROCEDURES
PS-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Personnel Security policy, Personnel Security policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Personnel Security policy and procedures, and frequency of review/update.

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-2	**POSITION CATEGORIZATION**
PS-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assigns a risk designation to all positions within the organization;* *(ii) the organization establishes a screening criteria for individuals filling organizational positions;* *(iii) the organization defines the frequency of risk designation reviews and updates for organizational positions; and* *(iv) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding designation and appointment of PKI CA and RA system Trusted Roles. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-3	**PERSONNEL SCREENING**
PS-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization screens individuals prior to authorizing access to the information system;* *(ii) the organization defines conditions requiring re-screening and, where re-screening is so indicated, the frequency of such re-screening; and* *(iii) the organization re-screens individuals according to organization-defined conditions requiring re-screening and, where re-screening is so indicated, the organization-defined frequency of such re-screening.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding designation and appointment of PKI CA and RA system Trusted Roles. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-4	**PERSONNEL TERMINATION**
PS-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization terminates information system access upon termination of individual employment;* *(ii) the organization conducts exit interviews of terminated personnel;* *(iii) the organization retrieves all security-related organizational information system-related property from terminated personnel; and* *(iv) the organization retains access to organizational information and information systems formerly controlled by terminated personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding designation and appointment, and responsibilities and behavior of PKI CA and RA system Trusted Roles, and revocation of PKI Trusted Role certificates. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-5	**PERSONNEL TRANSFER**
PS-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;* *(ii) the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment; and* *(iii) the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding designation and appointment of PKI CA and RA system Trusted Roles. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-6	**ACCESS AGREEMENTS**
PS-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies appropriate access agreements for individuals requiring access to organizational information and information systems;* *(ii) individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;* *(iii) the organization defines the frequency of reviews/updates for access agreements; and* *(iv) the organization reviews/updates the access agreements in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding access agreements. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

PS-6(PKI)	**ACCESS AGREEMENTS**
PS-6(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if individuals in PKI Trusted Roles identified in the CP acknowledge operational and security responsibilities upon appointment to the role;* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding access agreements. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-7	**THIRD-PARTY PERSONNEL SECURITY**
PS-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers* *(ii) the organization documents personnel security requirements for third-party providers; and* *(iii) the organization monitors third-party provider compliance with personnel security requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding third party personnel security. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities; third-party providers].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-8	**PERSONNEL SANCTIONS**
PS-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding personnel sanctions. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-1	**RISK ASSESSMENT POLICY AND PROCEDURES**
RA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents risk assessment policy;* *(ii) the organization risk assessment policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;* *(iv) the organization develops and formally documents risk assessment procedures;* *(v) the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; and* *(vi) the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities].
RA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of risk assessment policy reviews/updates;* *(ii) the organization reviews/updates risk assessment policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of risk assessment procedure reviews/updates;* *(iv) the organization reviews/updates risk assessment procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities].

RA-1(PKI)	RISK ASSESSMENT POLICY AND PROCEDURES
RA-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local Risk Assessment policy, Risk Assessment policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for Risk Assessment policy and procedures, and frequency of review/update.

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-2	**SECURITY CATEGORIZATION**
RA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;* *(ii) the organization documents the security categorization results (including supporting rationale) in the security plan for the information system; and* *(iii) the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS), and PKI System Security Plan, for policy and procedures regarding security categorization of CA and RA systems, and ancillary systems under the control of the PKI Program. **Interview**: [*SELECT FROM:* Organizational personnel with security categorization and risk assessment responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-3	**RISK ASSESSMENT**
RA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:* - *access;* - *use;* - *disclosure;* - *disruption;* - *modification; or* - *destruction;* *(ii) the organization defines the document in which risk assessment results are documented, selecting from the security plan, risk assessment report, or other organization-defined document;* *(iii) the organization documents risk assessment results in the organization-defined document;* *(iv) the organization defines the frequency for review of the risk assessment results;* *(v) the organization reviews risk assessment results in accordance with the organization-defined frequency;* *(vi) the organization defines the frequency that risk assessments are updated; and* *(vii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS), and PKI System Security Plan, for policy and procedures regarding the conduct, documentation, and review of CA and RA system risk assessments. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-5	**VULNERABILITY SCANNING**
RA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *the frequency for conducting vulnerability scans on the information system and hosted applications and/or;* - *the organization-defined process for conducting random vulnerability scans on the information system and hosted applications;* *(ii) the organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency and/or the organization-defined process for random scans;* *(iii) the organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported;* *(iv) the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:* - *enumerating platforms, software flaws, and improper configurations;* - *formatting/and making transparent checklists and test procedures; and* - *measuring vulnerability impact, and* *(v) the organization analyzes vulnerability scan reports and results from security control assessments.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].
RA-5.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the response times for remediating legitimate vulnerabilities in accordance with an organizational assessment of risk;* *(ii) the organization remediates legitimate vulnerabilities in accordance with organization-defined response times; and* *(iii) the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].

RA-5(1)	VULNERABILITY SCANNING
RA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Test**: [*SELECT FROM:* Vulnerability scanning capability and associated scanning tools].

RA-5(2)	VULNERABILITY SCANNING
RA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of updates for information system vulnerabilities scanned; and* *(ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when new vulnerabilities are identified and reported.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning..

RA-5(3)	VULNERABILITY SCANNING
RA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs vulnerability scanning procedures that can demonstrate the breadth of coverage (i.e., information system components scanned); and* *(ii) the organization employs vulnerability scanning procedures that can demonstrate the depth of coverage (i.e., vulnerabilities checked).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning..

RA-5(4)	VULNERABILITY SCANNING
RA-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization attempts to discern what information about the information system is discoverable by adversaries.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning..

RA-5(PKI)	VULNERABILITY SCANNING
RA-5(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization scans for vulnerabilities in the CA information system and hosted applications are conducted by PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].
RA-5(PKI).2	**ASSESSMENT OBJECTIVE:** *Determine if the organization scans for vulnerabilities within the network outside the CA information system are conducted in accordance with local Risk Assessment vulnerability scanning policy and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].
RA-5(PKI).3	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs vulnerability scanning tools and techniques on the CA information system and hosted applications under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].
RA-5(PKI).4	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) The organization reports results of selected vulnerability scanning activities of PKI System Components to designated Risk Assessment personnel in accordance with local Risk Assessment vulnerability scanning policy and procedures to facilitate more thorough scanning;* *(ii) the organization defines the list of information system components to which privileged access is authorized for selected vulnerability scanning activities; and* *(iii) the organization includes privileged access authorization to PKI System components for selected vulnerability scanning activities to facilitate more thorough scanning.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning..
RA-5(PKI).5	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for employing automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials; and* *(ii) The organization employs automated mechanisms under the control of Trusted Roles as required by local policy to detect the presence of unauthorized software on organizational CA information systems and notifies designated organizational officials.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding vulnerability scanning.. **Test**: [*SELECT FROM:* Vulnerability scanning capability and associated scanning tools].
RA-5(PKI).6	**ASSESSMENT OBJECTIVE:** *Determine if detailed rules of engagement are agreed upon by PKI Trusted Roles identified in the CP before the commencement of any vulnerability scanning is performed.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure detailed rules of engagement are agreed upon before the commencement of any vulnerability scanning is performed.

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-1	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**
SA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system services and acquisition policy;* *(ii) the organization system services and acquisition policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities;* *(iv) the organization develops and formally documents system services and acquisition procedures;* *(v) the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls; and* *(vi) the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities].
SA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system services and acquisition policy reviews/updates;* *(ii) the organization reviews/updates system services and acquisition policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of system services and acquisition procedure reviews/updates;* *(iv) the organization reviews/updates system services and acquisition procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities].

ASSESSMENT PROCEDURE	
SA-1(PKI)	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**
SA-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local System and Services Acquisition policy, System and Services Acquisition policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Services Acquisition policy and procedures, and frequency of review/update.

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-2	**ALLOCATION OF RESOURCES**
SA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization includes a determination of the information security requirements for the information system in mission/business process planning;* *(ii) the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and* *(iii) the organization establishes a discrete line item for information security in organizational programming and budgeting documentation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding allocation of resources for the CA and RA systems, and ancillary systems under the control of the PKI Program. **Interview**: [*SELECT FROM:* Organizational personnel with capital planning and investment responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-3	**LIFE CYCLE SUPPORT**
SA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations;* *(ii) the organization defines and documents information system security roles and responsibilities throughout the system development life cycle; and* *(iii) the organization identifies individuals having information system security roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding life cycle support for the CA and RA systems, and ancillary systems under the control of the PKI Program. **Interview**: [*SELECT FROM:* Organizational personnel with information security and system life cycle development responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-4	**ACQUISITIONS**
SA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:* – *security functional requirements/specifications;* – *security-related documentation requirements; and* – *developmental and evaluation-related assurance requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities].

SA-4(1)	ACQUISITIONS
SA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires in acquisition documents that vendors/contractors provide information describing in the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-4(2)	ACQUISITIONS
SA-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-4(4)	ACQUISITIONS
SA-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization explicitly assigns each acquired information system component to an information system; and* *(ii) the owner of the system acknowledges each assignment of information system components to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; information system owner].

SA-4(7)	ACQUISITIONS
SA-4(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires a commercially-provided information technology product to rely on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type; and* *(ii) the organization requires the use of a FIPS-validated, cryptographic module for a technology product that relies on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to verify that only FIPS-validated cryptographic modules are implemented in the PKI system. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-5	**INFORMATION SYSTEM DOCUMENTATION**
SA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:* - *secure configuration, installation, and operation of the information system;* - *effective use and maintenance of the security features/functions; and* - *known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;* *(ii) the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:* - *user-accessible security features/functions and how to effectively use those security features/functions;* - *methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and* - *user responsibilities in maintaining the security of the information and information system; and* *(iii) the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the availability of CA and RA information system documentation. **Interview**: [*SELECT FROM:* Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(1)	INFORMATION SYSTEM DOCUMENTATION
SA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the availability of CA and RA information system documentation. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(2)	INFORMATION SYSTEM DOCUMENTATION
SA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the availability of CA and RA information system documentation. **Interview**: [*SELECT FROM:* Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(3)	INFORMATION SYSTEM DOCUMENTATION
SA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the availability of CA and RA information system documentation. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-6	**SOFTWARE USAGE RESTRICTIONS**
SA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization uses software and associated documentation in accordance with contract agreements and copyright laws;* *(ii) the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and* *(iii) the organization 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.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding usage restrictions of CA and RA information system software. **Interview**: [*SELECT FROM:* Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-7(PKI)	**USER-INSTALLED SOFTWARE**
SA-7(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) The organization specifically prohibits the installation or use of software not installed by Trusted Roles in accordance with the PKI Certificate Policy (CP) and Certification Practices Statement (CPS);* *(ii) the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users; and* *(iii) the organization (or information system) enforces explicit rules governing the installation of software by users.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) to verify policy and procedures regarding installation of software to CA and RA information systems. **Interview:** PKI Trusted Roles identified in the CP regarding the procedures for installing software to CA and RA information systems. **Test**: [*SELECT FROM:* Enforcement of rules for user installed software on the information system; information system for prohibited software].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-8	**SECURITY ENGINEERING PRINCIPLES**
SA-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) The organization applies information system security engineering principles in the specification of the information system;* *(ii) the organization applies information system security engineering principles in the design of the information system;* *(iii) the organization applies information system security engineering principles in the development of the information system;* *(iv) the organization applies information system security engineering principles in the implementation of the information system; and* *(v) the organization applies information system security engineering principles in the modification of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding application of information system security engineering principles in the specification, design, development, implementation, and modification of CA and RA information system. **Interview**: [*SELECT FROM:* Organizational personnel with information system design, development, implementation, and modification responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-9	**EXTERNAL INFORMATION SYSTEM SERVICES**
SA-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;* *(ii) the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services; and* *(iii) the organization monitors security control compliance by external service providers.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding external information system services for the CA and RA information system. **Interview**: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities; external providers of information system services].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-10	**DEVELOPER CONFIGURATION MANAGEMENT**
SA-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators:* *(i) perform configuration management during information system:* - *design;* - *development;* - *implementation; and* - *operation;* *(ii) manage and control changes to the information system during:* - *design;* - *development;* - *implementation; and* - *modification;* *(iii) implement only organization-approved changes;* *(iv) document approved changes to the information system; and* *(v) track security flaws and flaw resolution.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding developer configuration management for the CA and RA information system. **Interview**: [*SELECT FROM:* Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

	ASSESSMENT PROCEDURE
SA-11	**DEVELOPER SECURITY TESTING**
SA-11.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):* – *create and implement a security test and evaluation plan;* – *implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and* – *document the results of the security testing/evaluation and flaw remediation processes.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding developer security testing for the CA and RA information system. **Interview**: [*SELECT FROM:* Organizational personnel with developer security testing responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

	ASSESSMENT PROCEDURE
SA-12	**SUPPLY CHAIN PROTECTION**
SA-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the measures to be employed to protect against supply chain threats; and* *(ii) the organization protects against supply chain threats by employing organization-defined measures as part of a comprehensive, defense-in-breadth information security strategy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure that hardware and software procured to operate the CA is purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-13	**TRUSTWORTHINESS**
SA-13.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the organization's level of trustworthiness; and* *(ii) the organization requires that the information system meet the organization-defined level of trustworthiness.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures the level(s) of trustworthiness that the CA and RA information systems must meet. **Interview**: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities; information system authorizing official].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-1	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**
SC-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system and communications protection policy;* *(ii) the organization system and communications protection policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities;* *(iv) the organization develops and formally documents system and communications protection procedures;* *(v) the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls; and* *(vi) the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and communications protection responsibilities].
SC-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system and communications protection policy reviews/updates;* *(ii) the organization reviews/updates system and communications protection policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of system and communications protection procedure reviews/updates;* *(iv) the organization reviews/updates system and communications protection procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and communications protection responsibilities].

ASSESSMENT PROCEDURE	
SC-1(PKI)	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**
SC-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local System and Communications Protection policy, System and Communications Protection policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Communications Protection policy and procedures, and frequency of review/update.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-2	**APPLICATION PARTITIONING**
SC-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system separates user functionality (including user interface services) from information system management functionality.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding separation of user functionality (including user interface services) from information system management functionality in the CA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Separation of user functionality from information system management functionality].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-3	**SECURITY FUNCTION ISOLATION**
SC-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and* *(ii) the information system isolates security functions from nonsecurity functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding isolation of security functions from non-security functions in the CA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Separation of security functions from nonsecurity functions within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-4	**INFORMATION IN SHARED RESOURCES**
SC-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding information in shared resources and unauthorized and unintended information transfer via shared system resources in the CA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Information system for unauthorized and unintended transfer of information via shared system resources].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-5	**DENIAL OF SERVICE PROTECTION**
SC-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and* *(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding protection against or limitations on the effects of denial of service attacks on the CA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Information system for protection against or limitation of the effects of denial of service attacks].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-7	**BOUNDARY PROTECTION**
SC-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the external boundary of the information system;* *(ii) the organization defines key internal boundaries of the information system;* *(iii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system; and* *(iv) the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Selected organizational personnel with boundary protection responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing boundary protection capability within the information system].

SC-7(1)	**BOUNDARY PROTECTION**
SC-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].

SC-7(2)	BOUNDARY PROTECTION
SC-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the mediation necessary for public access to the organization's internal networks; and* *(ii) the information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access controls for public access to the organization's internal networks].

SC-7(3)	BOUNDARY PROTECTION
SC-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; communications and network traffic monitoring logs; other relevant documents or records].

SC-7(4)	BOUNDARY PROTECTION
SC-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for reviewing exceptions to traffic flow policy;* *(ii) the organization implements a managed interface for each external telecommunication service;* *(iii) the organization establishes a traffic flow policy for each managed interface;* *(iv) the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;* *(v) the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;* *(vi) the organization reviews exceptions to the traffic flow policy in accordance with the organization-defined frequency; and* *(vii) the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; traffic flow policy; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow policy exceptions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Selected organizational personnel with boundary protection responsibilities]. **Test**: [*SELECT FROM:* Managed interfaces implementing organizational traffic flow policy].

SC-7(5)	BOUNDARY PROTECTION
SC-7(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system, at managed interfaces, denies network traffic by default; and* *(ii) the information system, at managed interfaces, allows network traffic by exception.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Selected organizational personnel with boundary protection responsibilities].

SC-7(6)	BOUNDARY PROTECTION
SC-7(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization prevents the unauthorized release of information outside of the information system boundary; or* *(ii) the organization prevents any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting the fail-safe boundary protection capability within the information system].

SC-7(7)	BOUNDARY PROTECTION
SC-7(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting non-remote connections with the information system].

SC-7(8)	BOUNDARY PROTECTION
SC-7(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the internal communications traffic to be routed to external networks;* *(ii) the organization defines the external networks to which the organization-defined internal communications traffic should be routed; and* *(iii) the information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Mechanisms implementing managed interfaces within information system boundary protection devices].

SC-7(13)	BOUNDARY PROTECTION
SC-7(13).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the key information security tools, mechanisms, and support components to be isolated from other internal information system components; and* *(ii) the organization isolates PKI CA components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure the organization isolates PKI CA Components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-8	**TRANSMISSION INTEGRITY**
SC-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the integrity of transmitted information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding protection of transmitted information by the CA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Transmission integrity capability within the information system].

SC-8(1)	**TRANSMISSION INTEGRITY**
SC-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding protection of transmitted information by the CA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Cryptographic mechanisms implementing transmission integrity capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-9	**TRANSMISSION CONFIDENTIALITY**
SC-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the confidentiality of transmitted information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding protection of transmitted information confidentiality by the CA and RA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Transmission confidentiality capability within the information system].

SC-9(1)	**TRANSMISSION CONFIDENTIALITY**
SC-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization optionally defines alternative physical measures to prevent unauthorized disclosure of information during transmission ; and* *(ii) the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organization-defined alternative physical measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding protection of transmitted information confidentiality by the CA and RA systems, and ancillary systems under the control of the PKI Program. **Test**: [*SELECT FROM:* Cryptographic mechanisms implementing transmission confidentiality capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-10	**NETWORK DISCONNECT**
SC-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of inactivity before the information system terminates a network connection associated with a communications session; and* *(ii) the information system terminates a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Network disconnect capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-12	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
SC-12.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the management of PKI cryptography. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for cryptographic key establishment or management]. **Test**: [*SELECT FROM:* Automated mechanisms implementing cryptographic key management and establishment within the information system].

SC-12(1)	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
SC-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains availability of information in the event of the loss of cryptographic keys by users.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for policy and procedures regarding the management of PKI cryptography.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-13	**USE OF CRYPTOGRAPHY**
SC-13.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to verify that only FIPS-validated cryptographic modules are implemented in the PKI system.

SC-13(1)	**USE OF CRYPTOGRAPHY**
SC-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-14	**PUBLIC ACCESS PROTECTIONS**
SC-14.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the integrity and availability of publicly available information and applications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures to validate the protection of integrity and availability of publicly available information and applications. **Test**: [*SELECT FROM:* Automated mechanisms protecting the integrity and availability of publicly available information and applications within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-15	**COLLABORATIVE COMPUTING DEVICES**
SC-15.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines exceptions to the prohibiting of collaborative computing devices where remote activation is to be allowed;* *(ii) the organization prohibits remote activation of collaborative computing devices, excluding the organization-defined exceptions where remote activation is to be allowed; and* *(iii) the organization provides an explicit indication of use to users physically present at the devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users].

SC-15(PKI)	COLLABORATIVE COMPUTING DEVICES
SC-15(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if collaborative computing devices are prohibited on PKI System Components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure networking equipment turns off unused network ports and services. Any network software installed on the PKI System components is necessary to the functioning of the PKI System Components.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-17	**PUBLIC KEY INFRASTRUCTURE CERTIFICATES**
SC-17.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a certificate policy for issuing public key certificates; and* *(ii) the organization issues public key certificates under the organization-defined certificate policy or obtains public key certificates under a certificate policy from an approved service provider.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures for PKI certificate issuance. **Interview**: [*SELECT FROM:* Organizational personnel with public key infrastructure certificate issuing responsibilities].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-18	**MOBILE CODE**
SC-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines acceptable and unacceptable mobile code and mobile code technologies;* *(ii) the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and* *(iii) the organization authorizes, monitors, and controls the use of mobile code within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure only authorized code and software is installed on the PKI System components. **Interview**: [*SELECT FROM:* Organizational personnel with mobile code authorization, monitoring, and control responsibilities]. **Test**: [*SELECT FROM:* Mobile code authorization and monitoring capability for the organization].

SC-18(1)	**MOBILE CODE**
SC-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system implements detection and inspection mechanisms to identify unauthorized mobile code; and* *(ii) the information system takes corrective action when unauthorized mobile code is identified.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing mobile code detection and inspection capability].

SC-18(3)	**MOBILE CODE**
SC-18(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents the download and execution of prohibited mobile code.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms preventing download and execution of prohibited mobile code].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-19	**VOICE OVER INTERNET PROTOCOL**
SC-19.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization 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* *(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with VoIP authorization and monitoring responsibilities]. **Test**: [*SELECT FROM:* VoIP authorization and monitoring capability for the organization].

SC-19(PKI)	VOICE OVER INTERNET PROTOCOL
SC-19(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if Voice Over Internet Protocol is prohibited on PKI CA Components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The CP and CPS to ensure only authorized code and software is installed on the PKI System components.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-20	**SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**
SC-20.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing secure name/address resolution service (authoritative source)].

SC-20(1)	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
SC-20(1).1	**ASSESSMENT OBJECTIVE:** *Determine if* *(i) the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces; and* *(ii) the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-21	**SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**
SC-21.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing data origin authentication and integrity verification for resolution services].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-22	**ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**
SC-22.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information systems that collectively provide name/address resolution service for an organization are fault tolerant; and* *(ii) the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting name/address resolution service for fault tolerance and role separation].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-23	**SESSION AUTHENTICITY**
SC-23.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides mechanisms to protect the authenticity of communications sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing session authenticity].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-24	**FAIL IN KNOWN STATE**
SC-24.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the known-states the information system should fail to in the event of a system failure;* *(ii) the organization defines types of failures for which the information system should fail to an organization-defined known-state;* *(iii) the organization defines the system state information that should be preserved in the event of a system failure;* *(iv) the information system fails to an organization-defined known-state for an organization-defined type of failure; and* *(v) the information system preserves organization-defined system state information in the event of a system failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures regarding Incident Response and Disaster Recovery. **Test**: [*SELECT FROM:* Automated mechanisms implementing fail-in-known-state capability].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-28	**PROTECTION OF INFORMATION AT REST**
SC-28.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the confidentiality and integrity of information at rest.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing confidentiality and integrity protections for information at-rest].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-32	**INFORMATION SYSTEM PARTITIONING**
SC-32.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures, Concept of Operations, and system architecture. **Interview**: [*SELECT FROM:* Organizational personnel installing, configuring, and/or maintaining the information system].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-1	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**
SI-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system and information integrity policy;* *(ii) the organization system and information integrity policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities;* *(iv) the organization develops and formally documents system and information integrity procedures;* *(v) the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls; and* *(vi) the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and information integrity responsibilities].
SI-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system and information integrity policy reviews/updates;* *(ii) the organization reviews/updates system and information integrity policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of system and information integrity procedure reviews/updates; and* *(iv) the organization reviews/updates system and information integrity procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and information integrity responsibilities].

ASSESSMENT PROCEDURE	
SI-1(PKI)	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**
SI-1(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if in addition to local System and Information Integrity policy, System and Information Integrity policy and procedures are specified in the PKI Certificate Policy and Certification Practices Statement (CPS).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures, and frequency of review/update.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-2	**FLAW REMEDIATION**
SI-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies, reports, and corrects information system flaws;* *(ii) the organization tests software updates related to flaw remediation for effectiveness before installation;* *(iii) the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation; and* *(iv) the organization incorporates flaw remediation into the organizational configuration management process.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding system maintenance and flaw remediation. **Interview**: [*SELECT FROM:* Organizational personnel with flaw remediation responsibilities].

SI-2(2)	**FLAW REMEDIATION**
SI-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation; and* *(ii) the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding system maintenance and flaw remediation. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system flaw remediation update status].

SI-2(PKI)	**FLAW REMEDIATION**
SI-2(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if any Flaw Remediation mechanisms are under control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure flaw remediation mechanisms are under the control of Trusted Roles.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-3	**MALICIOUS CODE PROTECTION**
SI-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:* - *transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or* - *inserted through the exploitation of information system vulnerabilities;* *(ii) the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:* - *transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or* - *inserted through the exploitation of information system vulnerabilities;* *(iii) the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;* *(iv) the organization defines the frequency of periodic scans of the information system by malicious code protection mechanisms;* *(v) the organization defines one or more of the following actions to be taken in response to malicious code detection:* - *block malicious code;* - *quarantine malicious code; and/or* - *send alert to administrator;* *(vi) the organization configures malicious code protection mechanisms to:* - *perform periodic scans of the information system in accordance with organization-defined frequency;* - *perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and* - *take organization-defined action(s) in response to malicious code detection; and* *(vii) the organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding system maintenance and malicious code. **Interview**: [*SELECT FROM:* Organizational personnel with malicious code protection responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing malicious code protection capability].

SI-3(1)	MALICIOUS CODE PROTECTION
SI-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages malicious code protection mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding system maintenance and malicious code.

SI-3(3)	MALICIOUS CODE PROTECTION
SI-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding system maintenance and malicious code. **Test**: [*SELECT FROM:* Automated mechanisms implementing malicious code protection capability].

SI-3(PKI)	MALICIOUS CODE PROTECTION
SI-3(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if any Malicious Code Protection update mechanisms for the PKI CA components are under control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure Malicious Code Protection update mechanisms for the PKI CA components are under the control of Trusted Roles.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-4	**INFORMATION SYSTEM MONITORING**
SI-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines objectives for monitoring events on the information system;* *(ii) the organization monitors events on the information system in accordance with organization-defined objectives and detects information system attacks;* *(iii) the organization identifies unauthorized use of the information system;* *(iv) the organization deploys monitoring devices:* - *strategically within the information system to collect organization-determined essential information; and* - *at ad hoc locations within the system to track specific types of transactions of interest to the organization;* *(v) the organization 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; and* *(vi) the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding information system access privileges. **Interview**: [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

SI-4(2)	**INFORMATION SYSTEM MONITORING**
SI-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools to support near real-time analysis of events.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding information system access privileges. **Test**: [*SELECT FROM:* Automated tools supporting near real-time event analysis].

SI-4(4)	INFORMATION SYSTEM MONITORING
SI-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding information system access privileges. **Test**: [*SELECT FROM:* Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms].

SI-4(5)	INFORMATION SYSTEM MONITORING
SI-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines indicators of compromise or potential compromise to the security of the information system; and* *(ii) the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding information system access privileges. **Test**: [*SELECT FROM:* Information system monitoring real-time alert capability].

SI-4(6)	INFORMATION SYSTEM MONITORING
SI-4(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for System and Information Integrity policy and procedures regarding information system access privileges. **Test**: [*SELECT FROM:* Information system-wide intrusion detection and prevention capability].

SI-4(PKI)	INFORMATION SYSTEM MONITORING
SI-4(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if Information System Monitoring tools for the PKI CA components are under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure Information System Monitoring tools for the PKI CA components are under the control of Trusted Roles.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-5	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**
SI-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;* *(ii) the organization generates internal security alerts, advisories, and directives;* *(iii) the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;* *(iv) the organization disseminates security alerts, advisories, and directives to organization-identified personnel; and* *(v) the organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system].

SI-5(1)	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**
SI-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the distribution of security alert and advisory information].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-6	**SECURITY FUNCTIONALITY VERIFICATION**
SI-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the appropriate conditions, including the system transitional states if applicable, for verifying the correct operation of security functions;* *(ii) the organization defines for periodic security function verification, the frequency of the verifications;* *(iii) the organization defines information system responses and alternative action(s) to anomalies discovered during security function verification;* *(iv) the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and* *(v) the information system responds to security function anomalies in accordance with organization-defined responses and alternative action(s).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Security function verification capability].

SI-6(PKI)	**SECURITY FUNCTIONALITY VERIFICATION**
SI-6(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) systems must verify audit logging is turned on at startup; and* *(ii) notifications are received for any audit logging that fails.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: System configuration to ensure audit logging is turned on at startup and notifications are received for any audit logging that fails.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-7	**SOFTWARE AND INFORMATION INTEGRITY**
SI-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system detects unauthorized changes to software and information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Software integrity protection and verification capability].

SI-7(1)	SOFTWARE AND INFORMATION INTEGRITY
SI-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of integrity scans to be performed on the information system; and* *(ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records].

SI-7(2)	SOFTWARE AND INFORMATION INTEGRITY
SI-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records].

SI-7(PKI)	SOFTWARE AND INFORMATION INTEGRITY
SI-7(PKI).1	**ASSESSMENT OBJECTIVE:** *Determine if Software and Information Integrity tools are under the control of PKI Trusted Roles identified in the CP.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Interview**: PKI Trusted Roles identified in the CP to ensure that software and Information Integrity tools are used under the control of Trusted Roles.

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-8	**SPAM PROTECTION**
SI-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means;* *(ii) the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; and* *(iii) the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with spam protection responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing spam detection and handling capability].

SI-8(1)	**SPAM PROTECTION**
SI-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages spam protection mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-9	**INFORMATION INPUT RESTRICTIONS**
SI-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization restricts the capability to input information to the information system to authorized personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures regarding system access privileges and procedures. **Interview:** PKI Trusted Roles identified in the CP to ensure that system access privileges are enforced in accordance with the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-10	**INFORMATION INPUT VALIDATION**
SI-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system checks the validity of information inputs.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures regarding information validity check procedures. **Interview:** PKI Trusted Roles identified in the CP to ensure that information validity check procedures are enforced in accordance with the PKI Certificate Policy (CP) and Certification Practices Statement (CPS). **Test**: [*SELECT FROM:* Information system capability for checking validity of information inputs].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-11	**ERROR HANDLING**
SI-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system identifies potentially security-relevant error conditions;* *(ii) the organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages;* *(iii) the information system generates error messages that provide information necessary for corrective actions without revealing organization-defined sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and* *(iv) the information system reveals error messages only to authorized personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures regarding error handling procedures. **Interview:** PKI Trusted Roles identified in the CP to ensure that error handling procedures are enforced in accordance with the PKI Certificate Policy (CP) and Certification Practices Statement (CPS). **Test**: [*SELECT FROM:* Information system error handling capability].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-12	**INFORMATION OUTPUT HANDLING AND RETENTION**
SI-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and* *(ii) the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) policy and procedures regarding media and hardcopy handling and retention procedures. **Interview:** PKI Trusted Roles identified in the CP to ensure that media and hardcopy handling and retention procedures are enforced in accordance with the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).