



**Federal Public Key Infrastructure (FPKI)
Security Controls Profile
of
Special Publication 800-53**

Security Controls for 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 800-53 FPKI Security Controls Profile

The following table summarizes the security controls and control enhancements required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53 for Federal Public Key Infrastructure (PKI) Systems. .

The subsequent Security Control Family tables list the complete subset of NIST SP 800-53 security controls and control enhancements required for evaluation of a PKI System. In addition, this table shows control and control enhancement text modifications made to accommodate PKI systems.

The companion to this document is *Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53A, Assessment Guidance for Security Controls in PKI Systems*, which is tailored to provide guidance for evaluating a PKI System against the requirements specified herein.

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

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
ACCESS CONTROL			
AC-1 Access Control Policy and Procedures	AC-1 AC-1 (PKI-1)	AC-1 [Assignment: organization-defined frequency] Parameter: [---]	AC-1 (PKI-1) In addition to local access control policy, the organization specifies access control policy and procedures in the PKI Certificate Policy and Certification Practices Statement (CPS).
AC-2 Account Management	AC-2a,c,d,e,g, h(ii),i,j AC-2 (3) AC-2 (4) AC-2 (5c/5d) AC-2 (7) AC-2 (PKI-1) AC-2 (PKI-2)	AC-2. [Assignment: organization-defined frequency] Parameter: [---] AC-2 (2) [Assignment: organization-defined time period for each type of account (temporary and emergency)] Parameter: Not Applicable AC-2 (3) [Assignment: organization-defined time period] Parameter: [---]	AC-2a. Group, guest, temporary, and anonymous accounts are not permitted. AC-2b. Not Applicable – Group membership is not permitted AC-2f. Not Applicable – Guest, temporary, and anonymous accounts are not permitted. AC-2g. Temporary accounts are not permitted – the remainder of the enhancement is applicable. AC-2h(i). Not Applicable – Temporary accounts are not permitted AC-2 (1). Replaced by AC-2 (PKI-1) AC-2 (2). Not Applicable – Temporary and emergency accounts are not permitted AC-2 (PKI-1) The organization employs automated mechanisms under the control of PKI Trusted Roles identified in the CP to support the management of information system accounts. AC-2 (PKI-2) The organization requires at least two-person PKI Trust Role access control for access to CA equipment.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AC-3 Access Enforcement	AC-3	None.	None.
AC-4 Information Flow Enforcement	AC-4 AC-4 (PKI-1) AC-4 (PKI-2)	None.	<p>AC-4 (11). Replaced by AC-4 (PKI-1) and AC-4(PKI-2)</p> <p>AC-4 (PKI-1) The information system requires a privileged administrator to configure all attributes and security policies.</p> <p>AC-4 (PKI-2) The organization ensures that privileged administrators operate in a two (or more) person control environment.</p>
AC-5 Separation of Duties	AC-5	None.	None.
AC-6 Least Privilege	AC-6 AC-6 (2) AC-6 (5) AC-6 (PKI-1) AC-6 (PKI-2)	<p>AC-6 (1) [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware and security-relevant information)] Parameter: Not Applicable</p>	<p>AC-6 (1). Replaced by AC-6 (PKI-1)</p> <p>AC-6 (6). Replaced by AC-6 (PKI-2)</p> <p>AC-6 (PKI-1) The organization ensures that access to CA and RA security and audit functions is limited to specifically designated Trusted Roles as detailed in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).</p> <p>AC-6 (PKI-2) The organization prohibits access to the information system by users not designated as Trusted Roles of the PKI system.</p>

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AC-7 Unsuccessful Login Attempts	AC-7	AC-7a. [Assignment: organization-defined number] Parameter: [---] AC-7a. [Assignment: organization-defined time period] Parameter: [---] AC-7b. [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] Parameter: [---]	None.
AC-8 System Use Notification	AC-8	None.	None.
AC-10 Concurrent Session Control	AC-10	AC-10 [Assignment: organization-defined number] Parameter: [---]	None.
AC-11 Session Lock	AC-11	AC-11a. [Assignment: organization-defined time period] Parameter: [---]	None.
AC-14 Permitted Actions Without Identification/ Authentication	AC-14 AC-14 (1)	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AC-17 Remote Access	AC-17 AC-17 (1) AC-17 (2) AC-17 (3) AC-17 (4) AC-17 (5) AC-17 (7) AC-17 (8) AC-17 (PKI-1)	AC-17 (5) [Assignment: organization-defined frequency] Parameter: [---] AC-17 (7) [Assignment: organization-defined list of security functions and security-relevant information] Parameter: [---] AC-17 (8) [Assignment: organization-defined networking protocols within the information system deemed to be nonsecure] Parameter: [---]	AC-17 (PKI-1) The organization ensures that remote access devices for administration of Certification Authorities implement the same physical and logical controls as the CA itself.
AC-18 Wireless Access	AC-18 AC-18 (1) AC-18 (2) AC-18 (4) AC-18 (5)	AC-18 (2) [Assignment: organization-defined frequency] Parameter: [---]	None.
AC-19 Access Control for Mobile Devices	AC-19 AC-19 (1) AC-19 (2) AC-19 (3)	AC-19g. [Assignment: organization-defined inspection and preventative measures] Parameter: [---]	None.
AC-20 Use of External Information Systems	AC-20 AC-20 (1) AC-20 (2) AC-20 (PKI-1) AC-20 (PKI-2)	None.	AC-20 (PKI-1) The organization ensures that downloading/uploading configuration information from/to the CA is restricted to authorized Trusted Roles of the PKI system. AC-20 (PKI-2) The organization ensures that the use of external systems to process, store, or transmit information is limited to /from the PKI repositories and CSS.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AC-22 Publicly Accessible Content	AC-22	AC-22d. [Assignment: organization-defined frequency] Parameter: [---]	None.
AWARENESS AND TRAINING			
AT-1 Security Awareness and Training Policy and Procedures	AT-1 AT-1 (PKI-1)	AT-1 [Assignment: organization-defined frequency] Parameter: [---]	AT-1 (PKI-1) In addition to local awareness and training policy, the organization specifies awareness and training policy and procedures in the PKI Certificate Policy and Certification Practices Statement (CPS).
AT-2 Security Awareness	AT-2	AT-2 [Assignment: organization-defined frequency] Parameter: [---]	None.
AT-3 Security Training	AT-3 3 (PKI-1) AT-	AT-3 [Assignment: organization-defined frequency] Parameter: [---]	AT-3 (PKI-1) In addition to local awareness and training policy, the organization specifies awareness and training policy and procedures in the PKI Certificate Policy and Certification Practices Statement (CPS).
AT-4 Security Training Records	AT-4	AT-4b. [Assignment: organization-defined frequency] Parameter: [---]	None.
AUDIT AND ACCOUNTABILITY			
AU-1 Audit and Accountability Policy and Procedures	AU-1 AU-1 (PKI-1)	AU-1 [Assignment: organization-defined frequency] Parameter: [---]	AU-1 (PKI-1) In addition to local Audit and Accountability policy, the organization specifies Audit and Accountability policy and procedures in the PKI Certificate Policy and Certification Practices Statement (CPS).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AU-2 Auditable Events	AU-2a,b AU-2 (3) AU-2 (4) AU-2 (PKI-1)	<p>AU-2a. [Assignment: organization-defined list of auditable events] Parameter: [---]</p> <p>AU-2d. [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited] Parameter: Not Applicable</p> <p>AU-2d. [Assignment: organization-defined frequency of (or situation requiring) auditing for each identified event] Parameter: Not Applicable</p> <p>AU-2 (3) [Assignment: organization-defined frequency] Parameter: [---]</p>	<p>AU-2c. Not Applicable</p> <p>AU-2d. Not Applicable</p> <p>AU-2 (PKI-1) The organization ensures that the minimum list of auditable events is specified in the PKI Certificate Policy.</p>
AU-3 Content of Audit Records	AU-3 AU-3 (1) AU-3 (2) AU-3 (PKI-1)	<p>AU-3 (1) [Assignment: organization-defined additional, more detailed information] Parameter: [---]</p> <p>AU-3 (2) [Assignment: organization-defined additional, more detailed information] Parameter: [---]</p>	<p>AU-3 (PKI-1) For enhancement (2), the organization PKI Program controls and manages the content of audit records generated by the PKI CAs and RAs.</p>
AU-4 Audit Storage Capacity	AU-4 AU-4 (PKI-1)	None.	<p>AU-4 (PKI-1) The organization ensures that Audit logs for the PKI are backed up and archived prior to overwriting or deletion of the audit log.</p>
AU-5 Response to Audit Processing Failures	AU-5 AU-5 (1) AU-5 (2)	<p>AU-5b [Assignment: Organization-defined actions to be taken] Parameter: [The appropriate authority as specified in the CP and CPS shall determine whether to suspend PKI System operation until the problem is remedied.]</p>	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AU-6 Audit Review, Analysis, and Reporting	AU-6 AU-6 (1) AU-6 (7)	AU-6a. [Assignment: <i>organization-defined frequency</i>] Parameter: [---]	None.
AU-7 Audit Reduction and Report Generation	AU-7 AU-7 (1) AU-7 (PKI-1)	None.	AU-7 (PKI-1) The organization ensures that Audit reduction and report generation tools are used under the control of Trusted Roles.
AU-8 Time Stamps	AU-8 AU-8 (1)	AU-8 (1) [Assignment: <i>organization-defined frequency</i>] Parameter: [---] AU-8 (1) [Assignment: <i>organization-defined authoritative time source</i>] Parameter: [---]	None.
AU-9 Protection of Audit Information	AU-9	None.	None.
AU-10 Non-Repudiation	AU-10	None.	None.
AU-11 Audit Record Retention	AU-11	AU-11 [Assignment: <i>organization-defined time period consistent with records retention policy</i>] Parameter: [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)]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AU-12 Audit Generation	AU-12 AU-12 (1)	AU-12a. [Assignment: organization-defined information system components] Parameter: [---] AU-12 (1) [Assignment: organization-defined information system components] Parameter: [---] [Assignment: logical or physical] Parameter: [---] [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail] Parameter: [---]	None.
ASSESSMENT AND AUTHORIZATION			
CA-1 Security Assessment and Authorization Policies and Procedures	CA-1 CA-1 (PKI-1)	CA-1 [Assignment: organization-defined frequency] Parameter: [---]	CA-1 (PKI-1) In addition to local Security Assessment and Authorization policy, the organization specifies access control Security Assessment and Authorization in the PKI Certificate Policy and Certification Practices Statement (CPS).
CA-2 Security Assessments	CA-2 CA-2 (1) CA-2 (2)	CA-2b. [Assignment: organization-defined frequency] Parameter: [---]	None.
CA-3 Information System Connections	CA-3	None.	None.
CA-5 Plan of Action and Milestones	CA-5	CA-5b. [Assignment: organization-defined frequency] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CA-6 Security Authorization	CA-6	CA-6c. [Assignment: <i>organization-defined frequency</i>] Parameter: [---]	None.
CA-7 Continuous Monitoring	CA-7 CA-7 (PKI-1)	CA-7d. [Assignment: <i>organization-defined frequency</i>] Parameter: [---]	CA-7 (PKI-1) The organization ensures that 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).
CONFIGURATION MANAGEMENT			
CM-1 Configuration Management Policy and Procedures	CM-1 CM-1 (PKI-1)	CM-1 [Assignment: <i>organization-defined frequency</i>] Parameter: [---]	CM-1 (PKI-1) In addition to local Configuration Management policy, the organization specifies Configuration Management in the PKI Certificate Policy and Certification Practices Statement (CPS).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-2 Baseline Configuration	CM-2 CM-2 (1) CM-2 (3) CM-2 (5) CM-2 (6) CM-2 (PKI-1) CM-2 (PKI-2) CM-2 (PKI-3)	CM-2 (1) (a) [Assignment: organization-defined frequency] Parameter: [---] CM-2 (1) (b) [Assignment: organization-defined circumstances] Parameter: [---] CM-2 (5) (a) [Assignment: organization-defined list of software programs authorized to execute on the information system] Parameter: [---]	CM-2 (2). Replaced by CM-2 (PKI-3). CM-2 (4). Prohibited because PKI-1 and PKI-2 are required. CM-2 (PKI-1) The organization ensures that the PKI CA hardware, software, and middleware are dedicated to performing one task: the CA. CM-2 (PKI-2) The organization ensures that there are no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation. CM-2 (PKI-3) The organization ensures that any automated mechanisms employed by the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system are under the control of PKI Trusted Roles.
CM-3 Configuration Change Control	CM-3 CM-3 (1) CM-3 (2) CM-3 (PKI-1)	CM-3f. [Assignment: organization-defined configuration change control element] Parameter: [---] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]] Parameter: [---] CM-3 (1) (c) [Assignment: organization-defined time period] Parameter: [---]	CM-3 (3). Prohibited because CM-3 (PKI-1) is required. CM-3 (PKI-1) The organization ensures that 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.
CM-4 Security Impact Analysis	CM-4 CM-4 (1)	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-5 Access Restrictions for Change	CM-5 CM-5 (1) CM-5 (2) CM-5 (3) CM-5 (4) CM-5 (PKI-1)	CM-5 (4) <i>[Assignment: organization-defined information system components and system-level information]</i> Parameter: [CA Systems]	CM-5 (5). Prohibited because CM-5 (PKI-1) is required. CM-5 (PKI-1) The organization ensures that all changes to hardware, software, and firmware components and system information directly within a production environment are administered by PKI Trusted Roles.
CM-6 Configuration Settings	CM-6b,c,d CM-6 (PKI-1) CM-6(PKI-2)	CM-6a. <i>[Assignment: organization-defined security configuration checklists]</i> Parameter: [---] CM-6 (2) <i>[Assignment: organization-defined configuration settings]</i> Parameter: Not Applicable	CM-6a. Replaced by CM-6 (PKI-1). CM-6 (1). Replaced by CM-6 (PKI-2) CM-6 (2). Not Applicable CM-6 (3). Not Applicable CM-6 (PKI-1) The organization establishes and documents mandatory configuration settings unique to the CA and RA systems in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS) CM-6 (PKI-2) The organization ensures that If the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings, this function is under the control of the PKI System Trusted Roles as defined in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
CM-7 Least Functionality	CM-7 CM-7 (1) CM-7 (2)	CM-7 <i>[Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]</i> Parameter: [as specified in the PKI CP and CPS]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-8 Information System Component Inventory	CM-8 CM-8 (1) CM-8 (2) CM-8 (3) CM-8 (4) CM-8 (5) CM-8 (PKI-1)	CM-8d. [Assignment: organization-defined information deemed necessary to achieve effective property accountability] Parameter: [---] CM-8 (3) (a) [Assignment: organization-defined frequency] Parameter: [---] CM-8 (4) [Selection (one or more): name; position; role] Parameter: [---]	CM-8 (PKI-1) The organization ensures that automated inventory collection mechanisms do not violate the physical access, logical access, and network security requirements defined in the CP and CPS.
CM-9 Configuration Management Plan	CM-9	None.	None.
CONTINGENCY PLANNING			
CP-1 Contingency Planning Policy and Procedures	CP-1 CP-1 (PKI-1)	CP-1 [Assignment: organization-defined frequency] Parameter: [---]	CP-1 (PKI-1) In addition to local Contingency Planning policy, the organization specifies Contingency Planning in the PKI Certificate Policy and Certification Practices Statement (CPS).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CP-2 Contingency Plan	CP-2 CP-2 (1) CP-2 (2) CP-2 (3)	CP-2b. [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements] Parameter: [---] CP-2d. [Assignment: organization-defined frequency] Parameter: [---] CP-2f. [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements] Parameter: [---] CP-2 (3) [Assignment: organization-defined time period] Parameter: [---]	None.
CP-3 Contingency Training	CP-3 CP-3 (1)	CP-3 [Assignment: organization-defined frequency] Parameter: [---]	None.
CP-4 Contingency Plan Testing and Exercises	CP-4 CP-4 (1) CP-4 (2) CP-4 (4)	CP-4a. [Assignment: organization-defined frequency] Parameter: [---] [Assignment: organization-defined tests and/or exercises] Parameter: [---]	None.
CP-6 Alternate Storage Site	CP-6 CP-6 (1) CP-6 (2) CP-6 (3)	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CP-7 Alternate Processing Site	CP-7 CP-7 (1) CP-7 (2) CP-7 (3) CP-7 (4) CP-7 (5)	CP-7a. [Assignment: organization-defined time period consistent with recovery time objectives] Parameter: [---]	None.
CP-8 Telecommunications Services	CP-8 CP-8 (1) CP-8 (2) CP-8 (3) CP-8 (4)	CP-8 [Assignment: organization-defined time period] Parameter: [---]	None.
CP-9 Information System Backup	CP-9 CP-9 (1) CP-9 (2) CP-9 (3)	CP-9a. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [---] CP-9b. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [---] CP-9c. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [---] CP-9 (1) [Assignment: organization-defined frequency] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CP-10 Information System Recovery and Reconstitution	CP-10 CP-10 (2) CP-10 (3) CP-10 (4)	CP-10 (3) [Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state] Parameter: [---] CP-10 (4) [Assignment: organization-defined restoration time-periods] Parameter: [---]	None.
IDENTIFICATION AND AUTHENTICATION			
IA-1 Identification and Authentication Policy and Procedures	IA-1 IA-1 (PKI-1)	IA-1 [Assignment: organization-defined frequency] Parameter: [---]	IA-1 (PKI-1) In addition to local Identification and Authentication policy and procedures, the organization specifies Identification and Authentication policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
IA-2 Identification and Authentication (Organizational Users)	IA-2 IA-2 (1) IA-2 (2) IA-2 (3) IA-2 (4) IA-2 (5) IA-2 (8) IA-2 (9)	IA-2 (8) [Assignment: organization-defined replay-resistant authentication mechanisms] Parameter: [---] IA-2 (9) [Assignment: organization-defined replay-resistant authentication mechanisms] Parameter: [---]	None.
IA-3 Device Identification and Authentication	IA-3	IA-3 [Assignment: organization-defined list of specific and/or types of devices] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IA-4 Identifier Management	IA-4 a,b,c IA-4 (4)	IA-4 (4) [Assignment: organization-defined characteristic identifying user status] Parameter: [a Trusted Role]	IA-4d. Not Applicable because Trusted Roles are uniquely authenticated prior to taking any action IA-4e. Not Applicable because Trusted Roles are unique and limited in number.
IA-5 Authenticator Management	IA-5 IA-5 (1) IA-5 (2) IA-5 (3) IA-5 (6)	IA-5g. [Assignment: organization-defined time period by authenticator type] Parameter: [---] IA-5 (1) (a) [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type] Parameter: [---] IA-5 (1) (b) [Assignment: organization-defined number of changed characters] Parameter: [---] IA-5 (1) (d) [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum] Parameter: [---] IA-5 (1) (e) [Assignment: organization-defined number] Parameter: [---] IA-5 (3) [Assignment: organization-defined types of and/or specific authenticators] Parameter: [---]	None.
IA-6 Authenticator Feedback	IA-6	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IA-7 Cryptographic Module Authentication	IA-7	None.	None.
INCIDENT RESPONSE			
IR-1 Incident Response Policy and Procedures	IR-1 IR-1 (PKI-1)	IR-1 [Assignment: organization-defined frequency] Parameter: [---]	IR-1 (PKI-1) In addition to local Incident Response policy and procedures, the organization specifies Incident Response policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
IR-2 Incident Response Training	IR-2 IR-2 (1)	IR-2b. [Assignment: organization-defined frequency] Parameter: [as required by local policy]	IR-2 (2). Not Applicable because other non-automated mechanisms can be used to satisfy incident response training within a PKI environment.
IR-3 Incident Response Testing and Exercises	IR-3	IR-3 [Assignment: organization-defined frequency] Parameter: [---] [Assignment: organization-defined tests and/or exercises] Parameter: [---]	IR-3 (1). Not Applicable because other non-automated mechanisms can be used to satisfy incident response testing and exercises within a PKI environment.
IR-4 Incident Handling	IR-4 IR-4 (3) IR-4 (PKI-1)	None.	IR-4 (1). Not Applicable because other non-automated mechanisms can be used to satisfy incident handling within a PKI environment IR-4 (PKI-1) The organization ensures that if automated Incident Response mechanisms are implemented on the CA, control of these mechanisms are limited to Trusted Roles.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IR-5 Incident Monitoring	IR-5 IIR-5 (PKI-1)	None.	IR-5 (1). Not Applicable because of IR-5 (PKI-1). IR-5 (PKI-1) The organization ensures that any automated mechanisms used to support incident monitoring are under the control of Trusted Roles.
IR-6 Incident Reporting	IR-6 IR-6 (PKI-1)	IR-6a. [Assignment: organization-defined time period] Parameter: [---]	IR-6 (1). Not Applicable because of IR-6 (PKI-1). IR-6 (PKI-1) The organization ensures that any automated mechanisms used to support incident reporting are under the control of Trusted Roles.
IR-7 Incident Response Assistance	IR-7 IR-7 (2) IR-7 (PKI-1)	None.	IR-7 (1). Not Applicable because of IR-7 (PKI-1). IR-7 (PKI-1) The organization ensures that any automated mechanisms used to support incident response are under the control of Trusted Roles.
IR-8 Incident Response Plan	IR-8	IR-8b. [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements] Parameter: [Trusted Roles and the organization's PKI Policy Authority] IR-8c. [Assignment: organization-defined frequency] Parameter: [annually] IR-8e. [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements] Parameter: [Trusted Roles and the organization's PKI Policy Authority]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MAINTENANCE			
MA-1 System Maintenance Policy and Procedures	MA-1 MA-1 (PKI-1)	MA-1 [Assignment: organization-defined frequency] Parameter: [---]	MA-1 (PKI-1) In addition to local System Maintenance policy and procedures, the organization specifies System Maintenance policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
MA-2 Controlled Maintenance	MA-2 MA-2 (1) MA-2 (PKI-1)	None.	MA-2 (2). Not Applicable because of MA-2 (PKI-1). MA-2 (PKI-1) The organization ensures that Maintenance of the PKI System Components is performed under the control of the Trusted Roles.
MA-3 Maintenance Tools	MA-3 MA-3 (1) MA-3 (3) MA-3 (PKI-1) MA-3 (PKI-2)	None.	MA-3 (2). Not Applicable because of MA-3 (PKI-1) and MA-3 (PKI-2). MA-3 (PKI-1) The organization ensures that 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 Trusted Roles. MA-3 (PKI-2) The organization ensures 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MA-4 Non-Local Maintenance	MA-4 (PKI-1)	None.	<p>MA-4. Not Applicable because of MA-4 (PKI-1).</p> <p>MA-4 (1). Not Applicable because of MA-4 modification.</p> <p>MA-4 (2). Not Applicable because of MA-4 modification.</p> <p>MA-4 (3). Not Applicable because of MA-4 modification.</p> <p>MA-4 (PKI-1) The organization only permits non-local maintenance if all the control requirements apply equally to the CA and any remote workstations used to administer the CA.</p>
MA-5 Maintenance Personnel	MA-5 MA-5 (PKI-1)	None.	<p>MA-5 (PKI-1) The organization ensures that Maintenance personnel are under the supervision of Trusted Roles.</p>
MA-6 Timely Maintenance	MA-6	<p>MA-6 [Assignment: organization-defined list of security-critical information system components and/or key information technology components] Parameter:[any PKI System Component]</p> <p>[Assignment: organization-defined time period] Parameter: [a maximum of 72 hours]</p>	None.
MEDIA PROTECTION			

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MP-1 Media Protection Policy and Procedures	MP-1 MP-1 (PKI-1)	MP-1 [Assignment: organization-defined frequency] Parameter: [---]	MP-1 (PKI-1) In addition to local Media Protection policy and procedures, the organization specifies Media Protection policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
MP-2 Media Access	MP-2 MP-2 (PKI-1)	MP-2 [Assignment: organization-defined types of digital and non-digital media] Parameter: [all media] [Assignment: organization-defined list of authorized individuals] Parameter: [Trusted Roles] [Assignment: organization-defined security measures] Parameter: [procedures defined in the CPS]	MP-2 (1). Not Applicable MP-2 (PKI-1) 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.
MP-3 Media Marking	MP-3	MP-3b. [Assignment: organization-defined list of removable media types] Parameter: [---] [Assignment: organization-defined controlled areas] Parameter: [---]	None.
MP-4 Media Storage	MP-4	MP-4a. [Assignment: organization-defined types of digital and non-digital media] Parameter: [all CA media] [Assignment: organization-defined controlled areas] Parameter: [areas controlled by PKI Trusted Roles] [Assignment: organization-defined security measures] Parameter: [procedures defined in the CPS]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MP-5 Media Transport	MP-5 MP-5 (2) MP-5 (3) MP-5 (PKI-1)	MP-5a. [Assignment: organization-defined types of digital and non-digital media] Parameter: [all CA media] [Assignment: organization-defined security measures] Parameter: [mitigating security mechanisms]	MP-5 (4). Not Applicable because of MP-5 (PKI-1). MP-5 (PKI-1) The organization employs mitigating security mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
MP-6 Media Sanitization	MP-6 MP-6 (1) MP-6 (2) MP-6 (3)	MP-6 (2) [Assignment: organization-defined frequency] Parameter: [---] MP-6 (3) [Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices] Parameter: [---]	None.
PHYSICAL AND ENVIRONMENTAL PROTECTION			
PE-1 Physical and Environmental Protection Policy and Procedures	PE-1 PE-1 (PKI-1)	PE-1 [Assignment: organization-defined frequency] Parameter: [---]	PE-1 (PKI-1) In addition to local Physical and Environmental Protection policy and procedures, the organization specifies Physical and Environmental Protection policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
PE-2 Physical Access Authorizations	PE-2 PE-2 (1) PE-2 (PKI-1)	PE-2c. [Assignment: organization-defined frequency] Parameter: [---]	PE-2 (PKI-1) The organization ensures multi-party control by specified Trusted Roles for access to PKI CA information systems.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PE-3 Physical Access Control	PE-3 PE-3 (1) PE-3 (PKI-1)	PE-3f. [Assignment: organization-defined frequency] Parameter: [---] PE-3g. [Assignment: organization-defined frequency] Parameter: [---]	PE-3 (PKI-1) The organization ensures multi-party control by specified Trusted Roles for access to PKI CA information systems.
PE-4 Access Control for Transmission Medium	PE-4	None.	None.
PE-5 Access Control for Output Devices	PE-5	None.	None.
PE-6 Monitoring Physical Access	PE-6 PE-6 (1) PE-6 (2)	PE-6b. [Assignment: organization-defined frequency] Parameter: [---]	None.
PE-7 Visitor Control	PE-7 PE-7 (1)	None.	None.
PE-8 Access Records	PE-8 PE-8 (2)	PE-8b. [Assignment: organization-defined frequency] Parameter: [---]	PE-8 (1). Not Applicable because automated mechanisms for access records are not required.
PE-9 Power Equipment and Power Cabling	PE-9	None.	None.
PE-10 Emergency Shutoff	PE-10	PE-10b. [Assignment: organization-defined location by information system or system component] Parameter: [---]	None.
PE-11 Emergency Power	PE-11 PE-11 (1)	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PE-12 Emergency Lighting	PE-12	None.	None.
PE-13 Fire Protection	PE-13 PE-13 (1) PE-13 (2) PE-13 (3)	None.	None.
PE-14 Temperature and Humidity Controls	PE-14	PE-14a. [Assignment: organization-defined acceptable levels] Parameter: [---] PE-14b. [Assignment: organization-defined frequency] Parameter: [---]	None.
PE-15 Water Damage Protection	PE-15 PE-15 (1)	None.	None.
PE-16 Delivery and Removal	PE-16	PE-16 [Assignment: organization-defined types of information system components] Parameter: [all PKI System components]	None.
PE-17 Alternate Work Site	PE-17	PE-17a. [Assignment: organization-defined management, operational, and technical information system security controls] Parameter: [---]	None.
PE-18 Location of Information System Components	PE-18 PE-18 (1)	None.	None.
PLANNING			

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PL-1 Security Planning Policy and Procedures	PL-1 PL-1 (PKI-1)	PL-1 [Assignment: organization-defined frequency] Parameter: [---]	PL-1 (PKI-1) In addition to local Security Planning policy and procedures, the organization specifies Security Planning policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
PL-2 System Security Plan	PL-2	None.	None.
PL-4 Rules of Behavior	PL-4	None.	None.
PL-5 Privacy Impact Assessment	PL-5	None.	None.
PL-6 Security-Related Activity Planning	PL-6	None.	None.
PERSONNEL SECURITY			
PS-1 Personnel Security Policy and Procedures	PS-1 PS-1 (PKI-1)	PS-1 [Assignment: organization-defined frequency] Parameter: [---]	PS-1 (PKI-1) In addition to local Personnel Security policy and procedures, the organization specifies Personnel Security policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
PS-2 Position Categorization	PS-2	PS-2c. [Assignment: organization-defined frequency] Parameter: [---]	None.
PS-3 Personnel Screening	PS-3	PS-3b. [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PS-4 Personnel Termination	PS-4	None.	None.
PS-5 Personnel Transfer	PS-5	PS-5 [Assignment: organization-defined transfer or reassignment actions] Parameter: [---] [Assignment: organization-defined time period following the formal transfer action] Parameter: [---]	None.
PS-6 Access Agreements	PS-6a PS-6 (PKI-1)	PS-6b. [Assignment: organization-defined frequency] Parameter: Not Applicable	PS-6b. Replaced by PS-6 (PKI-1) PS-6 (PKI-1) Ensures that individuals in PKI Trusted Roles acknowledge operational and security responsibilities upon appointment to the role.
PS-7 Third-Party Personnel Security	PS-7	None.	None.
PS-8 Personnel Sanctions	PS-8	None.	None.
RISK ASSESSMENT			
RA-1 Risk Assessment Policy and Procedures	RA-1 RA-1 (PKI-1)	RA-1 [Assignment: organization-defined frequency] Parameter: [---]	RA-1 (PKI-1) In addition to local Risk Assessment policy and procedures, the organization specifies Risk Assessment policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
RA-2 Security Categorization	RA-2	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
RA-3 Risk Assessment	RA-3	RA-3b. [Selection: security plan; risk assessment report; [Assignment: organization-defined document]] Parameter: [---] RA-3c. [Assignment: organization-defined frequency] Parameter: [---] RA-3d. [Assignment: organization-defined frequency] Parameter: [---]	None.
RA-5 Vulnerability Scanning	RA-5c,d,e RA-5 (1) RA-5 (2) RA-5 (3) RA-5 (4) RA-5 (PKI-1) RA-5 (PKI-2) RA-5 (PKI-3) RA-5 (PKI-4) RA-5 (PKI-5) RA-5 (PKI-6)	RA-5a. [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] Parameter: Not Applicable RA-5d. Assignment: organization-defined response times] Parameter: [---] RA-5 (2) [Assignment: organization-defined frequency] Parameter: Not Applicable RA-5 (5) [Assignment: organization-identified information system components] Parameter: [---] RA-5 (7) [Assignment: organization-defined frequency] Parameter: Not Applicable – replaced by RA-5 (PKI-5). RA-5 (PKI-5) [Assignment: organization-defined frequency] Parameter: [as required by local policy]	RA-5a. Replaced by RA-5 (PKI-1) and RA-5 (PKI-2). RA-5b. Replaced by RA-5 (PKI-3). RA-5 (5). Replaced by RA-5 (PKI-4). RA-5 (7). Replaced by RA-5 (PKI-5). RA-5 (PKI-1) The organization ensures that scans for vulnerabilities in the CA information system and hosted applications are conducted by Trusted Roles. RA-5 (PKI-2) The organization ensures that scans for vulnerabilities within the network outside the CA information system are conducted in accordance with local Risk Assessment vulnerability scanning policy and procedures. RA-5 (PKI-3) The organization ensures that vulnerability scanning tools and techniques applied to the CA information system and hosted applications are only implemented and executed under the control of Trusted Roles. RA-5 (PKI-4) The organization reports results of selected

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
			<p>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.</p> <p>RA-5 (PKI-5) The organization employs automated mechanisms as required by local policy to detect the presence of unauthorized software on organizational CA information systems and notify designated organizational officials.</p> <p>RA-5 (PKI-6) The organization ensures that detailed rules of engagement are agreed upon by Trusted Roles before the commencement of any vulnerability scanning is performed.</p>
SYSTEM AND SERVICES ACQUISITION			
SA-1 System and Services Acquisition Policy and Procedures	SA-1 SA-1 (PKI-1)	SA-1 [Assignment: <i>organization-defined frequency</i>] Parameter: [---]	SA-1 (PKI-1) In addition to local System and Services Acquisition policy and procedures, the organization specifies System and Services Acquisition policy and procedures will be specified in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
SA-2 Allocation of Resources	SA-2	None.	None.
SA-3 Life Cycle Support	SA-3	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SA-4 Acquisitions	SA-4 SA-4 (1) SA-4 (2) SA-4 (4) SA-4(7b)	None.	None.
SA-5 Information System Documentation	SA-5 SA-5 (1) SA-5 (2) SA-5 (3)	None.	None.
SA-6 Software Usage Restrictions	SA-6	None.	None.
SA-7 User-Installed Software	SA-7 (PKI-1)	None.	SA-7. Replaced by SA-7 (PKI-1) SA-7 (PKI-1) 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).
SA-8 Security Engineering Principles	SA-8	None.	None.
SA-9 External Information System Services	SA-9	None.	None.
SA-10 Developer Configuration Management	SA-10	None.	None.
SA-11 Developer Security Testing	SA-11	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SA-12 Supply Chain Protection	SA-12	SA-12 [Assignment: organization-defined list of measures to protect against supply chain threats] Parameter: [---]	None.
SA-13 Trustworthiness	SA-13	SA-13 [Assignment: organization-defined level of trustworthiness] Parameter: [---]	None.
SYSTEM AND COMMUNICATIONS PROTECTION			
SC-1 System and Communications Protection Policy and Procedures	SC-1 SC-1 (PKI-1)	SC-1 [Assignment: organization-defined frequency] Parameter: [---]	SC-1 (PKI-1) In addition to local System and Communications Protection policy and procedures, the organization specifies System and Communications Protection policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
SC-2 Application Partitioning	SC-2	None.	None.
SC-3 Security Function Isolation	SC-3	None.	None.
SC-4 Information in Shared Resources	SC-4	None.	None.
SC-5 Denial of Service Protection	SC-5	SC-5 [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-7 Boundary Protection	SC-7 SC-7 (1) SC-7 (2) SC-7 (3) SC-7 (4) SC-7 (5) SC-7 (6) SC-7 (7) SC-7 (8) SC-7 (13)	SC-7 (4) (e) [Assignment: organization-defined frequency] Parameter: [---] SC-7 (8) [Assignment: organization-defined internal communications traffic] Parameter: [---] [Assignment: organization-defined external networks] Parameter: [---] SC-7 (13) [Assignment: organization defined key information security tools, mechanisms, and support components] Parameter: [PKI CA components]	None.
SC-8 Transmission Integrity	SC-8 SC-8 (1)	None.	None.
SC-9 Transmission Confidentiality	SC-9 SC-9 (1)	SC-9 (1) [Assignment: organization-defined alternative physical measures] Parameter: [---]	None.
SC-10 Network Disconnect	SC-10	SC-10 [Assignment: organization-defined time period] Parameter: [---]	None.
SC-12 Cryptographic Key Establishment and Management	SC-12 SC-12 (1)	None.	None.
SC-13 Use of Cryptography	SC-13 SC-13 (1)	None.	None.
SC-14 Public Access Protections	SC-14	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-15 Collaborative Computing Devices	SC-15 SC-15 (PKI-1)	SC-15a. [Assignment: organization-defined exceptions where remote activation is to be allowed] Parameter: [---]	SC-15 (PKI-1) The organization ensures that collaborative computing devices are prohibited on PKI System Components.
SC-17 Public Key Infrastructure Certificates	SC-17	SC-17 [Assignment: organization-defined certificate policy] Parameter: [---]	None.
SC-18 Mobile Code	SC-18 SC-18 (1) SC-18 (3)	None.	None.
SC-19 Voice Over Internet Protocol	SC-19 SC-19 (PKI-1)	None.	SC-19 (PKI-1) The organization ensures that Voice Over Internet Protocol is not implemented on PKI CA Components.
SC-20 Secure Name /Address Resolution Service (Authoritative Source)	SC-20 SC-20 (1)	None.	None.
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21	None.	None.
SC-22 Architecture and Provisioning for Name/Address Resolution Service	SC-22	None.	None.
SC-23 Session Authenticity	SC-23	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-24 Fail in Known State	SC-24	SC-24 [Assignment: organization-defined known-state] Parameter: [---] [Assignment: organization-defined time] Parameter: [---] [Assignment: organization-defined system state information] Parameter: [---]	None.
SC-28 Protection of Information at Rest	SC-28	None.	None.
SC-32 Information System Partitioning	SC-32	None.	None.
SYSTEM AND INFORMATION INTEGRITY			
SI-1 System and Information Integrity Policy and Procedures	SI-1 SI-1 (PKI-1)	SI-1 [Assignment: organization-defined frequency] Parameter: [---]	SI-1 (PKI-1) In addition to local System and Information Integrity policy and procedures, the organization specifies System and Information Integrity policy and procedures in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS).
SI-2 Flaw Remediation	SI-2 SI-2 (2) SI-2 (PKI-1)	SI-2 (2) [Assignment: organization-defined frequency] Parameter: [---]	SI-2 (1). Prohibited SI-2 (PKI-1) The organization ensures that any Flaw Remediation mechanisms are under control of Trusted Roles.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SI-3 Malicious Code Protection	SI-3 SI-3 (1) SI-3 (3) SI-3 (PKI-1)	SI-3c. [Assignment: organization-defined frequency] Parameter: [---] [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] Parameter: [---]	SI-3 (2). Prohibited SI-3 (PKI-1) The organization ensures that any Malicious Code Protection update mechanisms for the PKI CA components are under control of Trusted Roles.
SI-4 Information System Monitoring	SI-4 SI-4 (2) SI-4 (4) SI-4 (5) SI-4 (6) SI-4 (PKI-1)	SI-4a. [Assignment: organization-defined monitoring objectives] Parameter: [---] SI-4 (5) [Assignment: organization-defined list of compromise indicators] Parameter: [---]	SI-4 (PKI-1) The organization ensures that Information System Monitoring tools for the PKI CA components are under the control of Trusted Roles.
SI-5 Security Alerts, Advisories, and Directives	SI-5 SI-5 (1)	SI-5c. [Assignment: organization-defined list of personnel (identified by name and/or by role)] Parameter: [---]	None.
SI-6 Security functionality verification	SI-6 SI-6 (PKI-1)	SI-6 [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] Parameter: [---] [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] Parameter: [---]	SI-6 (PKI-1) Systems verify audit logging is turned on at startup and notifications are received for any audit logging that fails.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SI-7 Software and Information Integrity	SI-7 SI-7 (1) SI-7 (2) SI-7 (PKI-1)	SI-7 (1) [Assignment: organization-defined frequency] Parameter: [---]	SI-7 (PKI-1) The organization ensures that Software and Information Integrity tools are under the control of Trusted Roles.
SI-8 Spam Protection	SI-8 SI-8 (1)	None.	None.
SI-9 Information Input Restrictions	SI-9	None.	None.
SI-10 Information Input Validation	SI-10	None.	None.
SI-11 Error Handling	SI-11	SI-11b. [Assignment: organization-defined sensitive or potentially harmful information] Parameter: [---]	None.
SI-12 Information Output Handling and Retention	SI-12	None.	None.
PROGRAM MANAGEMENT			
PM-1 Information Security Program Plan	PM-1	PM-1b. [Assignment: organization-defined frequency] Parameter: [---]	None.
PM-2 Senior Information Security Officer	PM-2	None.	None.
PM-3 Information Security Resources	PM-3	None.	None.
PM-4 Plan of Action and Milestones Process	PM-4	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PM-5	PM-5 PM-5 (PKI-1)	None.	PM-5 (PKI-1) The organization ensures that inventory of PKI System Components is performed under the control of Trusted Roles.
PM-6	PM-6 PM-6 (PKI-1)	None.	PM-6 (PKI-1) The organization ensures that monitoring and reporting of information security measures of PKI System Components performance is performed under the control of Trusted Roles.
PM-7	PM-7	None.	None.
PM-8	PM-8	None.	None.
PM-9	PM-9 PM-9 (PKI-1)	None.	PM-9 (PKI-1) Because PKI is used to manage and mitigate risk to other systems and information, the organization ensure that the risk management strategy in a PKI environment is specific to a PKI infrastructure.
PM-10	PM-10a,c PM-10 (PKI-1)	None.	PM-10b. Replaced by PM-10 (PKI-1) PM-10 (PKI-1) The organization ensures that 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.
PM-11	PM-11	None.	None.