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

Security Controls for PKI Systems

Version 2.0.0

April 14, 2014

Revision History

Document Version	Document Date	Revision Details
0.1.3	6 December 2010	Draft per several CPWG reviews.
0.2.0	30 January 2011	Revised presentation per NIST recommendations.
Release Candidate 1.0.0	9 February 2011	Version for ISIMC review and comment.
v1.0.0	18 April 2011	Approved version for publication.
v2.0.0	14 April 2014	Updated version to align with NIST SP 800-53 r4

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 an 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,b,c,d,e, h),i,j AC-2 (3) AC-2 (4) AC-2 (5) AC-2 (7) AC-2 (13) AC-2 (PKI-1) AC-2 (PKI-2)	AC-2a. [*Assignment: organization-defined information system account types*] Parameter: [PKI Trusted Roles] AC-2e. [*Assignment: [Assignment: organization-defined personnel or roles*] Parameter: [PKI management authority] AC-2j. [*Assignment: organization-defined frequency*] Parameter: [as defined in the PKI Certificate Policy (CP) and Certification Practices Statement (CPS)] AC-2 (3) [*Assignment: organization-defined time period*] Parameter: [---] AC-2 (4) [Assignment: organization-defined personnel or roles]. Parameter: PKI Trusted Role: Administrator and/or Auditor AC-2 (5) [*Assignment: organization-defined time period*]	AC-2c. Group, guest, temporary, shared and anonymous accounts are not permitted. AC-2d. Guest, temporary, and anonymous accounts are not permitted. AC-2g. Not Applicable – See PKI-3. AC-2h 3..Other Attributes selected must not contradict the requirements of the CP/CPS. AC-2j. See AC-2 (PKI-1). AC-2k. Group, guest, temporary, shared and anonymous 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 (6). Prohibited – Dynamic accounts are not permitted AC-2 (8). Prohibited – Dynamic accounts are not permitted

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
		Parameter: [---] AC-2 (7) [*Assignment: organization-defined actions*] Parameter: [---] AC-2 (13) [*Assignment: organization-defined time period*] Parameter: [---]	AC-2 (9). Not Applicable - Group, guest, temporary, shared and anonymous accounts are not permitted AC-2 (10). Not Applicable - Group, guest, temporary, shared and anonymous accounts are not permitted AC-2 (11). Replaced by AC-2 (PKI-2) AC-2 (12). Replaced by AC-2 (PKI-1) 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 and administrative control of the CA. AC-2 (PKI-3) The organization requires any monitoring mechanism which has access to CA functions or operating system or to the physical platform is under the control of PKI trusted roles in accordance with the CP/CPS
AC-3 Access Enforcement	AC-3 AC-3 (2) AC-3 (7)	AC-3 (2) [Assignment: organization-defined privileged commands and/or other organization-defined actions] Parameter: [in accordance with the CP/CPS] AC-3 (2) [Assignment: organization-defined roles and users authorized to assume such roles] Parameter: [in accordance with the CP/CPS]	None.
AC-4 Information Flow Enforcement	AC-4 AC-4 (PKI-1)	AC-4 [Assignment:	AC-4 (11). Replaced by AC-4 (PKI-1) and AC-4(PKI-2)

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
	AC-4 (PKI-2)	organization-defined information flow control policies]. Parameter: [---]	AC-4 (PKI-1) The information system requires a privileged administrator to configure all attributes and security policies. AC-4 (PKI-2) The organization ensures that privileged administrators operate in a two (or more) person control environment.
AC-5 Separation of Duties	AC-5	AC-5 [Assignment: organization-defined duties of individuals]; Parameter: [---]	None.
AC-6 Least Privilege	AC-6 AC-6 (2) AC-6 (5) AC-6 (7) AC-6 (8) AC-6 (9) AC-6 (10) AC-6 (PKI-1) AC-6 (PKI-2)	AC-6 (1) [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware and security-relevant information*] Parameter: Not Applicable AC-6 (5) [Assignment: organization-defined personnel or roles] Parameter: [Trusted Roles in accordance with the CP/CPS] AC-6 (7) [Assignment: organization-defined frequency] the privileges assigned to] Parameter: [---] [Assignment: organization-defined roles or classes of users] Parameter: [Trusted Roles in accordance with the CP/CPS] AC-6 (8) [Assignment: organization-defined software] Parameter: [---]	AC-6 (1). Replaced by AC-6 (PKI-1) AC-6 (6). Replaced by AC-6 (PKI-2) 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). AC-6 (PKI-2) The organization limits access to the PKI information systems as defined in the PKI CP/CPS..

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	AC-6 (8a) [Assignment: organization-defined system use notification message or banner] Parameter: [---] AC-6 (8c) [Assignment: organization-defined conditions] Parameter: [---]	None.
AC-11 Session Lock	AC-11	AC-11a. [*Assignment: organization-defined time period*] Parameter: [---]	None.
AC-12 Session Termination	AC-12	AC-12 [Assignment: organization-defined conditions or trigger events requiring session disconnect] Parameter: [---]	
AC-14 Permitted Actions Without Identification/ Authentication	AC-14	AC-12 [Assignment: organization-defined user actions] Parameter: [---]	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 (9) AC-17 (PKI-1)	AC-17 (3) [Assignment: organization-defined number] Parameter: [---] AC-17 (4) [Assignment: organization-defined needs] 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 (4) AC-18 (5)	AC-18 (1) [*Selection (one or more): users; devices*] Parameter: [---]	None.
AC-19 Access Control for Mobile Devices	AC-19		None.
AC-20 Use of External Information Systems	AC-20 AC-20 (1) AC-20 (2) AC-20 (PKI-1) AC-20 (PKI-2)	AC-20 (2) [*Selection restricts; prohibits*] Parameter: [---]	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.
AC-22 Publicly Accessible Content	AC-22	AC-22d. [*Assignment: organization-defined frequency*] Parameter: [---]	None.
AWARENESS AND TRAINING			

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
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 (1) AT-2 (2)	AT-2 [*Assignment: organization-defined frequency*] Parameter: [---]	None.
AT-3 Security Training	AT-3 AT-3 (PKI-1)	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 personnel or roles*] Parameter: [---] [Assignment: organization-defined frequency] Parameter: [---] [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 (PKI-1)	AU-2a. [*Assignment: organization-defined list of auditable events*] Parameter: [---] AU-2d. [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited*] Parameter: Not Applicable AU-2d. [*Assignment: organization-defined frequency of (or situation requiring) auditing for each identified event*] Parameter: Not Applicable AU-2 (3) [*Assignment: organization-defined frequency*] Parameter: [---]	AU-2c. Not Applicable AU-2d. Not Applicable AU-2 (PKI-1) The organization ensures that the minimum list of auditable events is specified in the PKI Certificate Policy.
AU-3 Content of Audit Records	AU-3 AU-3 (1) AU-3 (PKI-1) AU-3 (PKI-2)	AU-3 (1) [*Assignment: organization-defined additional, more detailed information*] Parameter: [---] AU-3 (PKI-2) [*Assignment: organization-defined* information system components] Parameter: [PKI System Components]	AU-3 (PKI-1) The organization PKI Program controls and manages the content of audit records generated by the PKI CAs and RAs. AU-3 (PKI-2) Centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components] shall be under the control of PKI Trusted Roles.
AU-4 Audit Storage Capacity	AU-4 AU-4 (PKI-1)	AU-4 [Assignment: organization-defined audit record storage requirements].. Parameter: [PKI CP and CPS]	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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AU-5 Response to Audit Processing Failures	AU-5 AU-5 (1) AU-5 (2)	AU-5a [Assignment: organization-defined personnel or roles] Parameter: [---] 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.] AU-5 (1) [Assignment: organization-defined personnel, roles, and/or locations] Parameter: [---] [Assignment: organization-defined time period] Parameter: [---] AU-5 (2) [Assignment: organization-defined real-time period] Parameter: [---] [Assignment: organization-defined personnel, roles, and/or locations] Parameter: [---]	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 (7) AU-6 (PKI-1)	AU-6a. [*Assignment: organization-defined frequency*] Parameter: [---] AU-6a. [Assignment: organization-defined inappropriate or unusual activity] Parameter: [---] [Assignment: organization-defined frequency] Parameter: [---] AU-6b. [Assignment: organization-defined frequency] Parameter: [---] AU-6 (7). [Selection (one or more): information system process; role; user] Parameter: [---]	AU-6 (PKI-1) The organization employs automated mechanisms, under the control of PKI Trusted Roles, to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
AU-7 Audit Reduction and Report Generation	AU-7 AU-7 (1) AU-7 (PKI-1)	AU-7 (1) [*Assignment: organization-defined audit fields within audit records*] Parameter: [---]	AU-7 (PKI-1) The organization ensures that Audit reduction and report generation tools are used under the control of Trusted Roles.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AU-8 Time Stamps	AU-8 AU-8 (1)	AU-8b [*Assignment: organization-defined granularity of time measurement*] Parameter: [---] AU-8 (1) [*Assignment: organization-defined **f**requency*] Parameter: [---] AU-8 (1) [*Assignment: organization-defined authoritative time source*] Parameter: [---] AU-8 (1) [*Assignment: organization-defined time period*] Parameter: [---]	None.
AU-9 Protection of Audit Information	AU-9 AU-9 (2) AU-9 (3) AU-9 (4)	AU-9 (2) [*Assignment: organization-defined frequency*] Parameter: [---]. AU-9 (4) [*Assignment: organization-defined subset of users*] Parameter: [PKI Trusted Roles]	None.
AU-10 Non-Repudiation	AU-10	AU-10 [*Assignment: organization-defined actions to be covered by non-repudiation*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
AU-11 Audit Record Retention	AU-11 AU-11 (1)	AU-11 [*Assignment: organization-defined time period consistent with records retention policy*] 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)] AU-11 [*Assignment: organization-defined measures*] Parameter: [in accordance with the PKI CP and/or CPS]	None.
AU-12 Audit Generation	AU-12 AU-12 (1) AU-12 (PKI-1)	AU-12a. [*Assignment: organization-defined information system components*] Parameter: [---] AU-12b. [*Assignment: organization-defined personnel or roles*] 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: [---]	AU-12 (PKI-1) Replaces AU-12 (3). The scope of the audit parameters for the PKI system is defined in the PKI CP and/or CPS.
ASSESSMENT AND AUTHORIZATION			

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CA-1 Security Assessment and Authorization Policies and Procedures	CA-1 CA-1 (PKI-1)	CA-1 [*Assignment: organization-defined frequency*] Parameter: [---] [*Assignment: organization-defined frequency*] Parameter: [---] [*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: [---] CA-2d. [*Assignment: organization-defined individuals or roles*] Parameter: [---] CA-2 (1). [*Assignment: organization-defined level of independence*] Parameter: [---] CA-2 (2). [*Assignment: organization-defined frequency*] Parameter: [---] [*Selection: announced; unannounced*] Parameter: [---] [*Selection: (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing*] Parameter: [---] [*Assignment: organization-defined other forms of security assessment*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CA-3 Information System Connections	CA-3 CA-3 (5)	CA-3 [*Assignment: organization-defined frequency*] Parameter: [---] CA-3 (5) [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] Parameter: [permit-by-exception] [Assignment: organization-defined information systems] to connect to external information systems Parameter: [---]	None.
CA-5 Plan of Action and Milestones	CA-5	CA-5b. [Assignment: organization-defined frequency] Parameter: [---]	None.
CA-6 Security Authorization	CA-6	CA-6c. [*Assignment: organization-defined frequency*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CA-7 Continuous Monitoring	CA-7 CA-7 (PKI-1)	CA-7a. [*Assignment: organization-defined metrics*] Parameter: [---] CA-7b. [*Assignment: organization-defined frequencies*] Parameter: [---] [*Assignment: organization-defined frequencies*] Parameter: [---] CA-7g. [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined frequency*] 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-1a [*Assignment: organization-defined frequency*] Parameter: [---] CM-1b [*Assignment: organization-defined frequency*] Parameter: [---] [*Assignment: organization-defined frequency*] 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 (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 (3) [*Assignment: organization-defined previous versions of baseline configurations of 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-3 Configuration Change Control	CM-3 CM-3 (1) CM-3 (2) CM-3 (PKI-1)	CM-3e. [*Assignment: organization-defined time period*] Parameter: [---] CM-3g. [*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) (b) [*Assignment: organization-defined approval authorities*] Parameter: [---] CM-3 (1) (c) [*Assignment: organization-defined time period*] Parameter: [---] CM-3 (1) (f) [*Assignment: organization-defined personnel*] 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.
CM-5 Access Restrictions for Change	CM-5 CM-5 (1) CM-5 (2) CM-5 (5) CM-5 (PKI-1)	CM-5 (2) [*Assignment: organization-defined frequency]* Parameter: [CA Systems] [*Assignment: organization-defined circumstances]* Parameter: [CA Systems] CM-5 (2) (b) [*Assignment: organization-defined frequency]* Parameter: [---]	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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-6 Configuration Settings	CM-6b,c,d CM-6 (PKI-1) CM-6 (PKI-2)	CM-6a – See CM-6 (PKI-1). CM-6c [*Assignment: organization-defined information system components*] Parameter: [---] [*Assignment: organization-defined operational components*] Parameter: [---]	CM-6a. Replaced by CM-6 (PKI-1). CM-6 (1). Replaced by CM-6 (PKI-2) CM-6 (2). 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).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-7 Least Functionality	CM-7 CM-7 (1) CM-7 (5)	CM-7 [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*] Parameter: [as specified in the PKI CP and CPS] CM-7 (1a) [*Assignment: organization-defined frequency*] Parameter: [---] CM-7 (1b) [*Assignment: organization-defined functions, ports, protocols, and services within the information systems deemed to be unnecessary and/or non-secure*] Parameter: [---] CM-5 (5c) [*Assignment: organization-defined software programs authorized to execute on the information system*] Parameter: [---] [*Assignment: organization-defined frequency*] Parameter: [---]	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-8a, 4.. [*Assignment: organization-defined information deemed necessary to achieve effective information system accountability accountability*] Parameter: [---] CM-8b [*Assignment: organization-defined frequency*] Parameter: [---] CM-8 (3) (a) [*Assignment: organization-defined frequency*] Parameter: [---] CM-8 (3) (b) [*Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles*] 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.
CM-10 Software Usage Restrictions	CM-10	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CM-11 User-Installed Software	CM-11	CM-11a [*Assignment: organization-defined policies*] Parameter: [---] CM-11b [*Assignment: organization-defined methods*] Parameter: [---] CM-11c [*Assignment: organization-defined frequency*] Parameter: [---]	
CONTINGENCY PLANNING			
CP-1 Contingency Planning Policy and Procedures	CP-1 CP-1 (PKI-1)	CP-1 [*Assignment: organization-defined frequency*] Parameter: [---] CP-1 [*Assignment: organization-defined frequency*] Parameter: [---] 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-4 (4) CP-4 (5) CP-4 (8)	CP-2a (6). [*Assignment: organization-defined personnel or roles*] Parameter: [---] 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: [---] CP-2 (4). [*Assignment: organization-defined time period*] Parameter: [---]	None.
CP-3 Contingency Training	CP-3 CP-3 (1)	CP-3 [*Assignment: organization-defined time period*] Parameter: [---] CP-3 [*Assignment: organization-defined frequency*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
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.
CP-7 Alternate Processing Site	CP-7 CP-7 (1) CP-7 (2) CP-7 (3) CP-7 (4)	CP-7a. [*Assignment*: *organization-defined information system operations]* Parameter: [PKI System] 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 (5)	CP-8 [*Assignment*: *organization-defined information system operations*] Parameter: [PKI System] CP-8 [*Assignment*: *organization-defined time period*] Parameter: [---] CP-8 (4) [*Assignment*: *organization-defined frequency*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
CP-9 Information System Backup	CP-9 CP-9 (1) CP-9 (2) CP-9 (3) CP-9 (5)	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: [---] CP-9 (3) [*Assignment: organization-defined organization-defined critical information system software and other security-related information*] Parameter: [---]	None.
CP-10 Information System Recovery and Reconstitution	CP-10 CP-10 (2) CP-10 (4) CP-10 (6)	CP-10 (4) [*Assignment: organization-defined restoration time-periods*] Parameter: [---]	None.
IDENTIFICATION AND AUTHENTICATION			

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IA-1 Identification and Authentication Policy and Procedures	IA-1 IA-1 (PKI-1)	IA-1 [*Assignment: organization-defined frequency*] Parameter: [---] 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 (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*: o*rganization-defined list of specific and/or types of devices*] Parameter: [---] [Selection (one or more): local; remote; network] 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, d, e IA-4 (3) IA-4 (4)	IA-4a [Assignment: organization-defined personnel or roles] Parameter: [---] IA-4d [Assignment: organization-defined time period] Parameter: [---] IA-4e [Assignment: organization-defined time period of inactivity] Parameter: [---] IA-4 (4) [*Assignment: organization-defined characteristic identifying individual status*] Parameter: [a Trusted Role]	

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IA-5 Authenticator Management	IA-5 IA-5 (1) IA-5 (2) IA-5 (3) IA-5 (6) IA-5 (11) IA-5 (14) IA-5 (15)	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*] 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: [---] [*Selection: in person; by a trusted third party*] Parameter: [---] [*Assignment: organization-defined registration authority*] Parameter: [---] [*Assignment: organization-defined personnel roles*] Parameter: [---] IA-5 (11) [*Assignment: organization-defined token quality requirements*] Parameter: [FIPS 140-2]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IA-6 Authenticator Feedback	IA-6	None.	None.
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 personnel or roles*] Parameter: [---] [*Assignment: organization-defined frequency*] Parameter: [---] [*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 time period*] Parameter: [---] [*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 (2)	IR-3 [*Assignment: organization-defined frequency*] Parameter: [---] [*Assignment: organization-defined tests*] 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IR-4 Incident Handling	IR-4 IR-4 (3) IR-4 (8) IR-4 (PKI-1)	IR-4 (3) [*Assignment: organization-defined actions to take in response to classes of incidents*] Parameter: [---] IR-4 (8) [*Assignment: organization-defined external organizations*] Parameter: [---] [*Assignment: organization-defined incident information*] Parameter: [---]	IR-4 (1). Not Applicable because other non-automated mechanisms can be used to satisfy incident handling within a PKI environment IR-4 (2). Prohibited. Configuration of the PKI System should only be performed under the control of PKI Trusted Roles. 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.
IR-5 Incident Monitoring	IR-5 IR-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 (2) IR-6 (PKI-1)	IR-6a. [*Assignment: organization-defined time period*] Parameter: [---] [*Assignment: organization-defined authorities*] Parameter: [---] IR-6 (2) [*Assignment: organization-defined personnel or roles*] 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
IR-8 Incident Response Plan	IR-8	IR-8a. [*Assignment: organization-defined personnel or roles*] Parameter: [Trusted Roles and the organization's PKI Policy Authority] 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.
MAINTENANCE			
MA-1 System Maintenance Policy and Procedures	MA-1 MA-1 (PKI-1)	MA-1a [*Assignment: organization-defined personnel or roles*] Parameter: [---] MA-1b [*Assignment: organization-defined frequency*] Parameter: [---] *[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).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MA-2 Controlled Maintenance	MA-2 MA-2 (PKI-1)	MA-2c [*Assignment: organization-defined personnel or roles*] Parameter: [---] MA-2f [*Assignment: organization-defined maintenance-related information*] Parameter: [---]	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)	MA-3(3d) [*Assignment: organization-defined personnel or roles*] Parameter: [---]	MA-3 (2). Not Applicable because of MA-3 (PKI-1) and MA-3 (PKI-2). MA-3 (4). 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.	MA-4. Not Applicable because of MA-4 (PKI-1). MA-4 (1). Not Applicable because of MA-4 modification. MA-4 (2). Not Applicable because of MA-4 modification. MA-4 (3). Not Applicable because of MA-4 modification. MA-4 (6). Not Applicable because of MA-4 (PKI-1). 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.
MA-5 Maintenance Personnel	MA-5 MA-5 (PKI-1)	None.	MA-5 (1). Not Applicable because of MA-5 (PKI-1). MA-5 (4). Not Applicable because of MA-5 (PKI-1). MA-5 (5). Not Applicable because of MA-5 (PKI-1). MA-5 (PKI-1) The organization ensures that Maintenance personnel are under the supervision of Trusted Roles.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MA-6 Timely Maintenance	MA-6 MA-6 (1)	MA-6 [*Assignment*: *organization-defined list of security-critical information system components and/or key information technology components*] Parameter:[any PKI System Component] [*Assignment: organization-defined time period*] Parameter: [a maximum of 72 hours] MA-6 (1) [*Assignment: organization-defined information system components]* Parameter: [any PKI System Component] [*Assignment: organization-defined time intervals]* *Parameter: [---]*	None.
MEDIA PROTECTION			
MP-1 Media Protection Policy and Procedures	MP-1 MP-1 (PKI-1)	MP-1a [*Assignment: organization-defined personnel or roles*] Parameter: [---] MP-1b(1) [*Assignment: organization-defined frequency*] Parameter: [---] MP-1b(2) [*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).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
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 personnel or roles*] Parameter: [Trusted Roles]	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 types of information media*] Parameter: [---] [*Assignment: organization-defined controlled areas*] Parameter: [---]	None.
MP-4 Media Storage	MP-4	MP-4a. [*Assignment: organization-defined types of digital and/or non-digital media*] Parameter: [all CA media] [*Assignment: organization-defined controlled areas*] Parameter: [areas controlled by PKI Trusted Roles]	None.
MP-5 Media Transport	MP-5 MP-5 (3) MP-5 (PKI-1)	MP-5a. [*Assignment: organization-defined types of information system media*] Parameter: [all CA media] [*Assignment: organization-defined security safeguards*] 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
MP-6 Media Sanitization	MP-6 MP-6 (1) MP-6 (2) MP-6 (3)	MP-6a [Assignment: organization-defined information system media] Parameter: [---] MP-6a [Assignment: organization-defined sanitization techniques and procedures] Parameter: [---] 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.
MP-7 Media Use	MP-7 MP-7 (1)	MP-7 [Selection: restricts; prohibits] Parameter: [restricts] MP-7 [Assignment: organization-defined types of information system media] Parameter: [---] MP-7 [Assignment: organization-defined information systems or system components] Parameter: [PKI Systems] MP-7 [Assignment: organization-defined security safeguards] Parameter: [[Assignment: organization-defined security safeguards] that are under the control of Trusted Roles]	
PHYSICAL AND ENVIRONMENTAL PROTECTION			

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PE-1 Physical and Environmental Protection Policy and Procedures	PE-1 PE-1 (PKI-1)	PE-1a. [*Assignment: organization-defined personnel or roles*] Parameter: [---] PE-1b, 1. [*Assignment: organization-defined frequency*] Parameter: [---] PE-1b, 2. [*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.
PE-3 Physical Access Control	PE-3 PE-3 (1) PE-3 (4) PE-3 (PKI-1)	PE-3a. [Assignment: organization-defined entry/exit points to the facility where the information system resides] Parameter: [---] PE-3a, 2. [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards] Parameter: [---] PE-3b [Assignment: organization-defined entry/exit points] Parameter: [---] PE-3c [Assignment: organization-defined security safeguards] Parameter: [---] PE-3d [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]	PE-3 (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
		Parameter: [---] PE-3f. [*Assignment: organization-defined physical access devices*] Parameter: [---] [*Assignment: organization-defined frequency*] Parameter: [---] PE-3g. [*Assignment: organization-defined frequency*] Parameter: [---] PE-3 (1) [*Assignment: organization-defined physical spaces containing one or more components of the information system*] Parameter: [---] PE-3 (4) [*Assignment: organization-defined information system components one or more components of the information system*] Parameter: [PKI System Components]	
PE-4 Access Control for Transmission Medium	PE-4	PE-4. [*Assignment: organization-defined information system distribution and transmission lines*] Parameter: [---] [*Assignment: organization-defined security safeguards*] Parameter: [---]	None.
PE-5 Access Control for Output Devices	PE-5	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PE-6 Monitoring Physical Access	PE-6 PE-6 (1) PE-6 (3) PE-6 (4)	PE-6b. [*Assignment: organization-defined frequency*] Parameter: [---] [*Assignment: organization-defined events or potential indications of events*] Parameter: [---] PE-6 (4) [*Assignment: organization-defined physical spaces containing one or more components of the information system*] Parameter: [---]	None.
PE-8 Access Records	PE-8	PE-8a. [*Assignment: organization-defined time period*] Parameter: [---] 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PE-11 Emergency Power	PE-11 PE-11 (1)	PE-11 [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] Parameter: [---]	None.
PE-12 Emergency Lighting	PE-12	None.	None.
PE-13 Fire Protection	PE-13 PE-13 (1) PE-13 (2) PE-13 (3)	PE-13 (1) [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined emergency responders*] Parameter: [---] PE-13 (2) [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined emergency responders*] Parameter: [---]	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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PE-15 Water Damage Protection	PE-15 PE-15 (1)	PE-15 (1) [*Assignment: organization-defined personnel or roles*] Parameter: [---]	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 security controls*] Parameter: [---]	None.
PE-18 Location of Information System Components	PE-18	PE-17a. [*Assignment: organization-defined physical and environmental hazards*] Parameter: [---]	None.
PLANNING			
PL-1 Security Planning Policy and Procedures	PL-1 PL-1 (PKI-1)	PL-1 [*Assignment: organization-defined frequency*] Parameter: [---] PL-1 [*Assignment: organization-defined frequency*] Parameter: [---] [*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).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PL-2 System Security Plan	PL-2	PL-2b. [*Assignment: organization-defined personnel or roles*] Parameter: [---] PL-2c. [*Assignment: organization-defined frequency*] Parameter: [---]	None.
PL-4 Rules of Behavior	PL-4	PL-4c. [*Assignment: organization-defined frequency*] Parameter: [---]	None.
PERSONNEL SECURITY			
PS-1 Personnel Security Policy and Procedures	PS-1 PS-1 (PKI-1)	PS-1a. [*Assignment: organization-defined personnel or roles*] Parameter: [---] PS-1b. [*Assignment: organization-defined frequency*] Parameter: [---] [*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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PS-3 Personnel Screening	PS-3	PS-3b. [*Assignment: organization-defined list of conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening*] Parameter: [---]	None.
PS-4 Personnel Termination	PS-4	PS-4a. [*Assignment: organization-defined time-period*] Parameter: [---] PS-4c. [*Assignment: organization-defined information security topics*] Parameter: [---] PS-4f. [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined time period*] Parameter: [---]	None.
PS-5 Personnel Transfer	PS-5	PS-5b. [*Assignment: organization-defined transfer or reassignment actions*] Parameter: [---] [*Assignment: organization-defined time period following the formal transfer action*] Parameter: [---] PS-5d. [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined time period*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
PS-6 Access Agreements	PS-6a PS-6 (PKI-1)	PS-6b. [*Assignment: organization-defined frequency*] Parameter: Not Applicable PS-6c. 2. [*Assignment: organization-defined frequency*] Parameter: [---]	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	PS-7d. [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined time period*] Parameter: [---]	None.
PS-8 Personnel Sanctions	PS-8	PS-8b. [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Assignment: organization-defined time period*] Parameter: [---]	None.
RISK ASSESSMENT			
RA-1 Risk Assessment Policy and Procedures	RA-1 RA-1 (PKI-1)	RA-1a [*Assignment: organization-defined personnel or roles*] Parameter: [---] RA-1b [*Assignment: organization-defined frequency*] Parameter: [---] [*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 personnel or roles*] Parameter: [---] RA-3e. [*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 (5) RA-5 (PKI-1) RA-5 (PKI-2) RA-5 (PKI-3) 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-5e. *Assignment: organization-defined personnel or roles*] Parameter: [---] RA-5 (2) [*Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported*] Parameter: [---] RA-5 (2) [*Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported*] Parameter: [---]	RA-5a. Replaced by RA-5 (PKI-1) and RA-5 (PKI-2). RA-5b. Replaced by RA-5 (PKI-3). 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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
		RA-5 (4) [*Assignment: organization-defined corrective actions*] Parameter: [---] RA-5 (5) [*Assignment: organization-identified information system components*] Parameter: [---] [*Assignment: organization-defined vulnerability scanning activities*] 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-5 (PKI-4) [Withdrawn] 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. 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.
SYSTEM AND SERVICES ACQUISITION			
SA-1 System and Services Acquisition Policy and Procedures	SA-1 SA-1 (PKI-1)	SA-1a [*Assignment: organization-defined personnel or roles*] Parameter: [---] SA-1b, 1. [*Assignment: organization-defined frequency*] Parameter: [---] SA-1b, 2. [*Assignment: organization-defined frequency*] 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).

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SA-2 Allocation of Resources	SA-2	None.	None.
SA-3 Life Cycle Support	SA-3	SA-3a [*Assignment: organization-defined system development lifecycle*] Parameter: [---]	None.
SA-4 Acquisitions	SA-4 SA-4 (1) SA-4 (2) SA-4(7b) SA-4(9) SA-4 (10)	SA-4 (2) [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail*] Parameter: [---]	None.
SA-5 Information System Documentation	SA-5	SA-5c. [*Assignment: organization-defined actions*] Parameter: [---] SA-5e. [*Assignment: organization-defined personnel or roles*] Parameter: [---]	None.
SA-8 Security Engineering Principles	SA-8	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SA-9 External Information System Services	SA-9 SA-9 (2)	SA-9a [*Assignment: organization-defined security controls*] Parameter: [---] SA-9c [*Assignment: organization-defined process, methods, and techniques*] Parameter: [---] SA-9 (2) [*Assignment: organization-defined external information system services*] Parameter: [---]	None.
SA-10 Developer Configuration Management	SA-10	SA-10a [*Selection (one or more): design; development; implementation; operation*] Parameter: [---] SA-10b [*Assignment: organization-defined configuration items under configuration management*] Parameter: [---] SA-10e [*Assignment: organization-defined personnel*] Parameter: [---]	None.
SA-11 Developer Security Testing	SA-11	SA-11b [*Selection (one or more): unit; integration; system; regression*] Parameter: [---]	None.
SA-12 Supply Chain Protection	SA-12 SA-12 (11)	SA-12 [*Assignment: organization-defined security safeguards*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SA-13 Trustworthiness	SA-13	SA-13a [*Assignment: organization-defined information system, information system component, or information system service*] Parameter: [PKI System] SA-13b [*Assignment: organization-defined assurance overlay*] Parameter: [FPKI Security Controls Overlay]	None.
SA-15 Development Process, Standards, and Tools	SA-15	SA-15b [*Assignment: organization-defined frequency*] Parameter: [---] [*Assignment: organization-defined security requirements*] Parameter: [---]	
SYSTEM AND COMMUNICATIONS PROTECTION			
SC-1 System and Communications Protection Policy and Procedures	SC-1 SC-1 (PKI-1)	SC-1a [*Assignment: organization-defined personnel or roles*] Parameter: [---] SC-1b [*Assignment: organization-defined frequency*] Parameter: [---] [*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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-5 Denial of Service Protection	SC-5	SC-5 [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] Parameter: [---] SC-5 [*Assignment: organization-defined security safeguards*] Parameter: [---]	None.
SC-7 Boundary Protection	SC-7 SC-7 (3) SC-7 (4) SC-7 (5) SC-7 (7) SC-7 (8) SC-7 (13) SC-7 (18) SC-7 (21)	SC-7 (b) [*Selection: physically; logically*] Parameter: [---] 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 information security tools, mechanisms, and support components*] Parameter: [PKI CA components] SC-7 (21*)* [*Assignment: organization defined information system components*] Parameter: [PKI System components] [*Assignment: organization-defined missions and/or business functions*] Parameter: [PKI]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-8 Transmission Integrity	SC-8 SC-8 (1)	SC-8 [*Selection (one or more): confidentiality; integrity]*] Parameter: [---] SC-8 (1) [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] Parameter: [---] [*Assignment: organization-defined alternative physical safeguards*] 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 (3)	SC-12 [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*] Parameter: [---] SC-12 (3) [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or repositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key] Parameter: [---]	None.
SC-13 Use of Cryptography	SC-13	SC-13 [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] Parameter: [PKI cryptography and algorithms]	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) (replaces SC-15 (1), (3), (4)) 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)	SC-18 (1) [*Assignment: organization-defined unacceptable mobile code*] Parameter: [[*organization-defined unacceptable mobile code] in accordance with the applicable PKI certificate policy*] [*Assignment: organization-defined corrective actions*] Parameter: [---] SC-18 (3) [*Assignment: organization-defined unacceptable mobile code*] Parameter: [---]	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	None.	None.
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21	None.	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-22 Architecture and Provisioning for Name/Address Resolution Service	SC-22	None.	None.
SC-23 Session Authenticity	SC-23	None.	None.
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	SC-28 [Selection (one or more): confidentiality; integrity] [Parameter: [---] [*Assignment: organization-defined information at rest*] Parameter: [---]	None.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SC-37 Out-Of-Band Channels	SC-37	SC-37 [*Assignment: organization-defined out-of-band channels*] [Parameter: [---] [*Assignment: organization-defined information, information system components, or devices*] Parameter: [self-signed certificates and/or sensitive data and information exchanged as part of the certificate enrollment & issuance process] [*Assignment: organization-defined individuals or information systems*] Parameter: [---]	
SC-39 Process Isolation	SC-39	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 personnel or roles*] Parameter: [---] [*Assignment: organization-defined frequency*] Parameter: [---] [*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 [*Assignment: organization-defined time-period*] Parameter: [---] SI-2 (2) [*Assignment: organization-defined frequency*] Parameter: [---]	SI-2 (1), (5). 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 (PKI-1)	SI-3c. [*Assignment: organization-defined frequency*] Parameter: [---][Selection (one or more); endpoint; network entry/exit points] 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 (PKI-1)	SI-4a. [*Assignment: organization-defined monitoring objectives*] Parameter: [---] SI-4g. [*Assignment: organization-defined information system monitoring*] Parameter: [---] [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*Selection (one or more): as needed*;] Parameter: [---] [*Assignment: organization-defined frequency*]] Parameter: [---] SI-4 (4) [*Assignment: organization-defined frequency*] Parameter: [---] SI-4 (5) [*Assignment: organization-defined personnel or roles*] Parameter: [---] [*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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SI-5 Security Alerts, Advisories, and Directives	SI-5 SI-5 (1)	SI-5a. [*Assignment: organization-defined external organizations*] Parameter: [---] SI-5c. [*Selection (one or more):* [*Assignment: organization-defined list of personnel or role)*]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]] Parameter: [---] Parameter: [---] Parameter: [---]	None.
SI-6 Security functionality verification	SI-6 SI-6 (PKI-1)	SI-6a. [*Assignment: organization-defined security functions*] Parameter: [---] SI-6b. [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]] Parameter: [---] SI-6c. [*Assignment: organization-defined personnel or roles*] Parameter: [---] SI-6d. [*Selection (one or more): shuts the information system down; restarts the information 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 (5) SI-7 (7) SI-7 (14) SI-7 (PKI-1)	SI-7 [Assignment: organization-defined software, firmware, and information] Parameter: [---] SI-7 (1) [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency] Parameter: [---] Parameter: [---] Parameter: [---] SI-7 (2) [Assignment: organization-defined personnel or roles] Parameter: [---] SI-7 (5) [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] Parameter: [---] Parameter: [---] SI-7 (7) [Assignment: organization-defined security-relevant changes to the information system] 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) SI-8 (PKI-1)	None.	SI-8 (2). Prohibited. SI-8 (PKI-1) The organization ensures that updates to Spam protection mechanisms for the PKI CA components are under the control of Trusted Roles

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
SI-10 Information Input Validation	SI-10	SI-10 [*Assignment: organization-defined information input*] Parameter: [---]	None.
SI-11 Error Handling	SI-11	SI-11b. [*Assignment: organization-defined personnel or roles*] Parameter: [---]	None.
SI-12 Information Output Handling and Retention	SI-12	None.	None.
SI-16 Memory Protection	SI-16	SI-16. [*Assignment: organization-defined security safeguards*] Parameter: [---]	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.
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.

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
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 for PKI information systems are approved by the PKI Policy Management Authority (PMA).
PM-11	PM-11	None.	None.