FPKIPA

Federal Public Key Infrastructure Policy Authority

Security Control Overlay of NIST Special Publication 800-53 Revision 5 Security Controls for Federal PKI Systems

Federal PKI Policy Authority

Version 3.0

February 26, 2021

Revision History

Document Version	Document Date	Revision Details
0.1.3	December 6, 2010	Draft per several CPWG reviews.
0.2.0	January 30, 2011	Revised presentation per NIST recommendations.
Release Candidate 1.0.0	February 9, 2011	Version for ISIMC review and comment.
1.0.0	April 18, 2011	Approved version for publication.
2.0.0	April 14, 2014	Updated version to align with NIST SP 800-53 Revision 4
3.0.0	February 26, 20201	Updated version to align with NIST SP 800-53 Revision 5. Formatting updates to enhance navigation and readability.

Table of Contents

1 INTRODUCTION

The Federal Public Key Infrastructure (FPKI) provides the U.S. Government with a common baseline to administer digital certificates and public-private key pairs used to support trust of some government devices and persons. This overlay was developed by the Federal Public Key Infrastructure Policy Authority (FPKIPA) to provide additional specifications and protections for PKIs participating in the FPKI.

While many NIST [SP 800-53] controls apply to FPKI service operators as written, some controls require specific interpretation or augmentation. This overlay leverages [COMMON] to tailor appropriate [SP 800-53] controls to facilitate implementation. This overlay seeks to:

- Add, eliminate, or extend controls.
- Provide control applicability and interpretations.
- Specify values for organizationally defined parameters.
- Extend the supplemental guidance for controls, where necessary.

This overlay was built based on the controls appropriate for a system categorized at High under FIPS 199. Affiliates with systems categorized as Moderate may ignore the guidance for baseline controls and enhancements applicable to higher categories.

The following resources were used to create this document:

- NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, September 2020

2 APPLICABILITY AND USE

All PKIs participating in the FPKI should use this overlay and apply each control as specified to realize its full benefit.

This overlay covers only PKI-relevant controls, and does not replace other controls, requirements, or overlays, as applicable. If this overlay conflicts with guidance from government-wide or agency information security policies, regulations, or mission specific statutes, the system owner and information security officer must perform a risk assessment to determine how to resolve the difference.

Locally trusted Certification Authorities (CAs), public trust CAs[1], private CAs, and mission specific PKIs and CAs are not included in this overlay. These CAs do not have a certification path to the Federal Common Policy CA.

The FPKI Policy Authority will revise this overlay based on updates to the FPKI mission or policy, emerging threats, or discovery of additional protections. CAs participating in the FPKI are responsible for incorporating these updates into their documentation as part of their continuous monitoring support for their system where applicable.

Agencies can direct questions about this overlay to FPKI@gsa.gov.

[1] Public trust PKI is also commonly referred to as Web PKI.

3 FPKI OVERLAY TO NIST SP 800-53 SECURITY CONTROL FAMILIES

The following Figure shows the Security Control Families listing from NIST [SP 800-53].

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System Acquisition
IR	Incident Response	SC	System and Communication Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

3.1 Overlay Applicability Reference Tables

The following tables show the applicability of the [SP 800-53] controls in the context of the FPKI. For each control, we indicate whether a control applies or not, and identify relevant control enhancements. Appendix A provides full detail of the applicability of each control and enhancement.

Each row of the table has three columns:

1. **Control:** This lists the control identifier, e.g., AC-1
2. **Base Control:** This column indicates whether the control is applicable to Agency PKIs participating in the FPKI
    a. controls marked with the ● symbol are applicable and have additional guidance
    b. controls marked with the ⬜ symbol are applicable, but do not have additional guidance
3. **Enhancements with Guidance:** This column indicates which control enhancements are relevant to the analysis and subject to additional guidance provided in this document.
    a. Applicable controls are listed by number. Multiple controls are comma separated, e.g. “4,7,12”
    b. ✖ - this symbol indicates that there are no control enhancements with guidance for this base control
4. Enhancements w/o Guidance: This column indicates which control enhancements are relevant to the analysis, but which do not have any additional guidance. The same symbols are used to communicate controls in this column as in the “Enhancements with Guidance” column

Access Control

Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
AC-1	●	✖	✖
AC-2	●	4,14	1,2,3,5,7,11,12,13
AC-3	◻	2,11	✖
AC-4	●	11	4
AC-5	●	✖	✖
AC-6	●	1,5,6,7	2,3,9,10
AC-7	◻	✖	✖
AC-8	◻	✖	✖
AC-10	◻	✖	✖
AC-11	◻	✖	1
AC-12	◻	✖	✖
AC-14	●	✖	✖
AC-16	◻	2	✖
AC-17	●	✖	1,2,3,4
AC-18	●	✖	1,3,4,5
AC-19	●	✖	5

Access Control			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
AC-20	●	✖	1,2
AC-21	□	✖	✖
AC-22	□	✖	✖

Awareness and Training			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
AT-1	●	✖	✖
AT-2	□	✖	2,3
AT-3 AT-4	● □	✖ ✖	✖ ✖

Audit and Accountability			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
AU-1	●	✖	✖
AU-2	●	✖	✖
AU-3	●	✖	1
AU-4	●	✖	✖
AU-5	●	✖	1,2
AU-6	●	✖	1,3,5,6
AU-7	●	✖	1
AU-8	□	✖	✖
AU-9	□	2,4	3
AU-10	□	✖	✖
AU-11	●	1	✖
AU-12	□	✖	1,3

Assessment, Authorization and Monitoring			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
CA-1	●	✖	✖
CA-2	□	✖	1,2
CA-3	□	✖	6
CA-5	□	✖	✖
CA-6	□	✖	✖
CA-7	●	✖	1,4
CA-8	●	✖	1
CA-9	□	✖	✖

Configuration Management			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
CM-1	●	✖	✖
CM-2	●	2	3,7
CM-3	●	3,7	1,2,4,6
CM-4	⬜	✖	1,2
CM-5	●	✖	1
CM-6	●	1,2	✖
CM-7	●	4	1,2,5
CM-8	●	✖	1,2,3,4
CM-9	⬜	✖	✖
CM-10	⬜	✖	✖
CM-11	⬜	✖	✖
CM-12	⬜	✖	1

Contingency Planning			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
CP-1	●	✖	✖
CP-2	◻	3	1,2,5,8
CP-3	◻	✖	1
CP-4	◻	✖	1,2
CP-6	◻	✖	1,2,3
CP-7	●	✖	1,2,3,4
CP-8	●	✖	1,2,3,4
CP-9	●	✖	1,2,3,5,8
CP-10	●	4	2

Identification and Authentication			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
IA-1	●	✖	✖
IA-2	■	8	1,2
IA-3	●	✖	✖
IA-4	■	4	✖
IA-7	●	✖	✖
IA-12	●	✖	✖

Identification and Authentication			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
IA-1	●	✖	✖
IA-2	□	8	1,2,5,12
IA-3	●	✖	✖
IA-4	□	4	✖
IA-5	□	✖	1,2,6
IA-6	□	✖	✖
IA-7	●	✖	✖
IA-8	□	✖	1,2,4
IA-11	□	✖	✖
IA-12	●	✖	2,3,4,5

Incident Response			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
IR-1	■	✖	✖
IR-2	●	✖	1,2
IR-3	■	✖	2
IR-4	■	1,2	4,11
IR-5	●	✖	1
IR-6	●	✖	1,3
IR-7	●	✖	1
IR-8	●	✖	✖

Maintenance			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
MA-1	●	✖	✖
MA-2	●	✖	2
MA-3	●	✖	1,2,3
MA-4	●	✖	3
MA-5	●	✖	1
MA-6	●	✖	✖

Media Protection			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
MP-1	●	✖	✖
MP-2	●	✖	✖
MP-3	■	✖	✖
MP-4	●	✖	3
MP-5	●	✖	✖
MP-6	■	✖	1,2,3
MP-7	●	✖	✖

Physical and Environmental Protection

Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
PE-1	●	✖	✖
PE-2	●	✖	✖
PE-3	●	4	1
PE-4	●	✖	✖
PE-5	□	✖	✖
PE-6	●	✖	1,4
PE-8	●	1	✖
PE-9	□	✖	✖
PE-11	●	✖	1
PE-12	□	✖	✖
PE-13	□	✖	1,2
PE-14	□	✖	✖
PE-15	□	✖	1
PE-16	●	✖	✖
PE-17	●	✖	✖
PE-18	●	✖	✖

Planning			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
PL-1	●	✖	✖
PL-2	□	✖	✖
PL-4	□	✖	1
PL-8	□	✖	✖
PL-10	□	✖	✖
PL-11	□	✖	✖

Personnel Security			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
PS-1	●	✖	✖
PS-2	⬜	✖	✖
PS-3	●	✖	✖
PS-4	⬜	✖	2
PS-5	⬜	✖	✖
PS-6	●	✖	✖
PS-7	⬜	✖	✖
PS-8	⬜	✖	✖
PS-9	⬜	✖	✖

Risk Assessment			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
RA-1	●	✖	✖
RA-2	■	✖	✖
RA-3	■	✖	1
RA-5	●	✖	2,4,5,11
RA-7	■	✖	✖
RA-9	■	✖	✖

System and Services Acquisition			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
SA-1	●	✖	✖
SA-2	□	✖	✖
SA-3	□	✖	✖
SA-4	□	✖	1,2,5,9,10
SA-5	□	✖	✖
SA-8	□	✖	✖
SA-9	□	✖	2
SA-10	□	✖	✖
SA-11	□	✖	✖
SA-15	□	✖	3
SA-16	□	✖	✖
SA-17	□	✖	✖
SA-21	□	✖	✖
SA-22	□	✖	✖

System and Communications Protection			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
SC-1	●	✖	✖
SC-2	■	✖	✖
SC-3	■	✖	✖
SC-4	■	✖	✖
SC-5	■	✖	✖
SC-7	■	✖	3,4,5,7,8,18,21
SC-8	■	✖	1
SC-10	■	✖	✖
SC-12	■	✖	1
SC-13	●	✖	✖
SC-15	●	✖	✖
SC-17	■	✖	✖
SC-18	■	✖	✖

System and Communications Protection			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
SC-20	□	✖	✖
SC-21	□	✖	✖
SC-22	□	✖	✖
SC-23	□	✖	✖
SC-24	□	✖	✖
SC-28	□	✖	1
SC-39	□	✖	✖

System and Information Integrity			
Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
SI-1	●	✖	✖
SI-2	●	✖	2
SI-3	●	✖	✖
SI-4	●	✖	2,4,5,10,12,14,20,22
SI-5	□	✖	✖
SI-6	●	✖	✖
SI-7	□	✖	1,2,5,7,15
SI-8	□	✖	2
SI-10	□	✖	✖
SI-11	□	✖	✖
SI-12	□	✖	✖
SI-16	□	✖	✖

Supply Chain Risk Management

Control	Base Control	Enhancements with Guidance	Enhancements w/o Guidance
SR-1	□	✖	✖
SR-2	□	✖	1
SR-3	□	✖	✖
SR-5	□	✖	✖
SR-6	□	✖	✖
SR-8	□	✖	✖
SR-9	□	✖	1
SI-10	□	✖	✖
SI-11	□	✖	1,2
SI-12	□	✖	✖

3.2 How to Use FPKI Overlay Security Controls Table

The following table summarizes the security controls selection as required by [SP 800-53] for FPKI systems, and any additional security requirements that are expected to be addressed in more detail in other policy documents (e.g., a Certification Practice Statement):

- **A-** This row within each table provides the security control number and the security control title name [control family identifier & control number, e.g., AC-1-Access Control Policy and Procedure].
- **B-** The base control is listed.
- **C-** Additional PKI requirement descriptions relating to the processes or activities to be implemented for alignment with a Certificate Policy (CP) or Certification Practice Statement (CPS). The PKI requirement has a unique identifier, which is associated with a security control shown as, for example, "AC-1 (PKI-1)." The PKI identifier numbering restarts for each associated security control. The FPKI parameters are the processes or activities that the CAs and PKIs implement to comply with a security control or security control enhancement.
- **D-** (OPTIONAL) One or more control enhancements may be documented, if they are relevant.
  - a. This column lists the identifier for the control enhancement
  - b. This column provides the text of the enhancement itself.
  - c. This column provides PKI requirements and parameters related to the control enhancement.

<table>
<tr><th colspan="3">A - AC-2 Account Management</th></tr>
<tr><th colspan="3">Base Control</th></tr>
<tr><td colspan="3">B - <<Base control listing>></td></tr>
<tr><th colspan="3">PKI Specific Requirements Guidance/FPKI Parameter</th></tr>
<tr><td colspan="3">C - <<FPKI Guidance/Parameters related to base control>></td></tr>
<tr><th colspan="3">D - AC-2 Account Management Security Control Enhancements</th></tr>
<tr><td>a.</td><td>b. - <<(Optional) control enhancement>></td><td>c. - <<FPKI Guidance/Parameters related to enhancement>></td></tr>
</table>

APPENDIX A: FPKI NIST 800-53 REV 5 SECURITY CONTROL DETAILS

AC: Access Control

AC-1 Access Control Policy and Procedure

Base Control

Control:

- a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
  - 1. An access control policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    - Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
  - 2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
- b. Designate an [*Assignment: organization-defined senior management official*] to manage the access control policy and procedures;
- c. Review and update the current access control:
  - 1. Policy [Assignment: organization-defined frequency]; and
  - 2. Procedures [Assignment: organization-defined frequency];
- d. Ensure that the access control procedures implement the access control policy and controls; and
- e. Develop, document, and implement remediation actions for violations of the access control policy.

AC-1 PKI Specific Requirements Guidance/FPKI Parameter

AC-1 (PKI-1)

In addition to local access control policy, the organization specifies and complies with access control policy and procedures in the PKI CP/CPS.

FPKI Parameter:

AC-1a. [Assignment: organization-organization-defined personnel or roles]

Parameter: PKI Trusted Roles

AC-1b. [Assignment: organization-defined senior management official]

Parameter: PKI Policy Authority

CP Section(s):

2.4, 5.1.2, 6.5.1, 6.7

AC-2 Account Management

Base Control

Control:

a. Define and document the types of system accounts allowed for use within the system in support of organizational missions and business functions;
b. Assign account managers for system accounts;
c. Establish conditions for group and role membership;
d. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create system accounts;
f. Create, enable, modify, disable, and remove system accounts in accordance with [*Assignment: organization-defined policy, procedures, and conditions*];
g. Monitor the use of system accounts;
h. Notify account managers within [Assignment: organization-defined time-period for each situation]:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions and business functions;
j. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*];
k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

PKI Specific Requirements Guidance/FPKI Parameter
AC-2 (PKI-1) The organization employs 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 Trusted 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 be under the control of PKI Trusted Roles in accordance with the CP/CPS **FPKI Parameters:** AC-2c. Group, guest, temporary, shared and anonymous accounts are not permitted. AC-2d. Guest, temporary, and anonymous accounts are not permitted. AC-2h 3. Other Attributes selected must not contradict the requirements of the CP/CPS AC-2k. Shared/group accounts are not permitted. AC-2j. See AC-2 (PKI-1) AC-2i. 3 Other Attributes selected must not contradict the requirements of the CP/CPS. **CP Section(s):** 6.5.1

AC-2 Account Management Security Control Enhancements		
(4)	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS Automatically audit account creation, modification, enabling, disabling, and removal actions	**FPKI Parameters:** [Assignment: organization-defined personnel or roles] Parameter: PKI Trusted Role: Administrator and/or Auditor **CP Section(s):** 5.4.1
(14)	ACCOUNT MANAGEMENT | PROHIBIT SPECIFIC ACCOUNT TYPES Prohibit the use of [Selection (one or more): shared; guest; anonymous; temporary; emergency] accounts for access to [Assignment: organization-defined information types].	[Selection (one or more): guest; anonymous; temporary; emergency] Parameter: [guest; anonymous; temporary; emergency unless permitted by the PKI CP] **CP Section(s):** 5.2.3

AC-3 Access Enforcement Security Control Enhancements		
(2)	ACCESS ENFORCEMENT | DUAL AUTHORIZATION Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions]	**FPKI Parameters:** [Assignment: organization-defined privileged commands and/or other organization-defined actions] Parameter: [in accordance with the CP/CPS] **CP Section(s):** 5.2.2
(11)	ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES Restrict direct access to data repositories containing [Assignment: organization-defined information types].	**FPKI Parameters:** [organization-defined information types] Parameter: [in accordance with the CP/CPS] **CP Section(s):** 5.2.1

AC-4 Information Flow Enforcement

Base Control

Control:

Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on *[Assignment: organization-defined information flow control policies*].

PKI Specific Requirements Guidance/FPKI 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.

CP Section(s):

5.2.1, 5.2.2

AC-4 Information Flow Enforcement Control Enhancements

(11)	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.	Replaced by AC-4 (PKI-1) and AC-4 (PKI-2)

AC-5 Separation of Duties

Base Control

Control:

a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and

b. Define system access authorizations to support separation of duties.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Assignment: organization-defined duties of individuals]

Parameter: [in accordance with the CP/CPS]

CP Section(s):

5.2.4

AC-6 Least Privilege

Base Control

Control:

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

PKI Specific Requirements Guidance/FPKI Parameter

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.

FPKI Parameters:

[Assignment: organization-defined duties of individuals]

Parameter: [in accordance with the CP/CPS]

CP Section(s):

5.2.4

AC-6 Least Privilege Security Control Enhancements		
(1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS Explicitly authorize access for [Assignment: organization-defined individuals or roles] to: (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and (b) [Assignment: organization-defined security-relevant information].	Replaced by AC-6 (PKI-1)
(5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	**FPKI Parameters:** [Assignment: organization-defined personnel or roles] Parameter: [Trusted Roles in accordance with the CP/CPS] **CP Section(s):** 6.5.1
(6)	LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS Prohibit privileged access to the system by non-organizational users.	Replaced by AC-6 (PKI-1)
(7)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	**FPKI Parameters:** [Assignment: organization-defined roles or classes of users] Parameter: [Trusted Roles in accordance with the CP/CPS] **CP Section(s):** 5.4.2

AC-14 Permitted Actions Without Identification or Authentication

Base Control

Control:

a. Identify [*Assignment: organization-defined user actions*] that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Assignment: organization-defined user actions]

Parameter: [in accordance with the CP/CPS]

CP Section(s):

6.5.1

AC-16 Security and Privacy Attributes Security Control Enhancements

(2)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.	Limit authority to make attribute changes to appropriate Trusted Roles as required by the CP/CPS. **CP Section(s):** 6.5.1

AC-17 Remote Access

Base Control

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorize remote access to the system prior to allowing such connections.

PKI Specific Requirements Guidance/FPKI Parameter

AC-17 (PKI-1)

The organization ensures that remote workstations for administration of PKI Components are implemented with the same physical and logical controls as required by the CP/CPS.

CP Section(s):

5.1, 6.5.1, 6.7

AC-18 Wireless Access

Base Control

Control:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorize wireless access to the system prior to allowing such connections.

PKI Specific Requirements Guidance/FPKI Parameter

AC-18 (PKI-1)

The organization prohibits wireless access for administrative access to PKI components

CP Section(s):

6.7

AC-19 Access Control for Mobile Devices

Base Control

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
c. Authorize the connection of mobile devices to organizational systems.

PKI Specific Requirements Guidance/FPKI Parameter

AC-19 (PKI-1)

The organization prohibits the use of mobile devices for access to PKI components unless explicitly allowed in the CP/CPS.

CP Section(s):

5.1, 6.7

AC-20 Use of External Systems

Base Control

Control:

Establish [Selection (one or more): [Assignment: organization-defined terms and conditions]; [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

a. Access the system from external systems; and
b. Process, store, or transmit organization-controlled information using external systems.

PKI Specific Requirements Guidance/FPKI 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 Certificate Status Servers (“CSS”).

CP Section(s):

2.2, 4.3.1

AT: Awareness and Training

AT-1 Awareness and Training Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system level] awareness and training policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current security and privacy awareness and training:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency];

AT-1 PKI Specific Requirements Guidance/FPKI 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 CP/CPS. **FPKI Parameters:** **AT-1b.** [Assignment: organization-defined official] Parameter: [PKI Policy Authority] **AT-1c.** [Assignment: organization-defined frequency]; Parameter [per CP/CPS]; **CP Section(s):** 5.3.3

AT- 3 Role-Based Training

Base Control

Control:

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

PKI Specific Requirements Guidance/FPKI 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 CP/CPS.

FPKI Parameters:

AT-1b.

[Assignment: organization-defined official]

Parameter: [PKI Policy Authority]

AT-1c.

[Assignment: organization-defined frequency];

Parameter [per CP/CPS];

CP Section(s):

5.3.3

AU: Audit and Accountability

AU-1 Audit and Accountability Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): organization-level; mission/business process-level; system level] audit and accountability policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [Assignment: organization-defined senior management official] to manage the audit and accountability policy and procedures;

c. Review and update the current audit and accountability:
   1. Policy [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI 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 CP and CPS.

FPKI Parameters:

AU-1b.

[Assignment: organization-defined senior management official]

Parameter: [Auditor Trusted Role]

CP Section(s):

5.4

AU-2 Event Logging

Base Control

Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization defined event types (subset of the event types defined in AU-2 a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

PKI Specific Requirements Guidance/FPKI Parameter

AU-2 (PKI-1)

The organization ensures that the minimum list of auditable events is specified in the PKI CP/CPS.

CP Section(s):

5.4.1

AU-3 Content of Audit Records

Base Control

Control:

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

PKI Specific Requirements Guidance/FPKI Parameter

AU-3 (PKI-1)

The organization 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 PKI System Components shall be under the control of PKI Trusted Roles.

CP Section(s):

5.4.1

AU-4 Audit Log Storage Capacity
Base Control
Control: Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit record retention requirements].
PKI Specific Requirements Guidance/FPKI Parameter
AU-4 (PKI-1) The organization ensures that audit records for the PKI System Components are backed up and archived prior to overwriting or deletion of the audit record. **FPKI Parameter:** [Assignment: organization-defined audit record storage requirements] Parameter: [PKI CP/CPS] **CP Section(s):** 5.4.4, 5,4,5

AU-5 Response to Audit Processing Failures

Base Control

Control:

a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and
b. Take the following additional actions: [Assignment: organization-defined actions to be taken].

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

AU-5b.

[Assignment: organization-defined actions to be taken]

[The appropriate authority as specified in the CP/CPS shall determine whether to suspend PKI System operation until the problem is remedied.]

CP Section(s):

5.4.1, 5.4.6

AU-6 Audit Record Review, Analysis, and Reporting
Base Control
Control: a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
PKI Specific Requirements Guidance/FPKI Parameter
AU-6 (PKI-1) The organization employs mechanisms to integrate audit log review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. These mechanisms must be configured under the control of PKI Trusted Roles. **CP Section(s):** 5.4.2

AU-7 Audit Record Reduction and Report Generation

Base Control

Control: Provide and implement an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

PKI Specific Requirements Guidance/FPKI Parameter

AU-7 (PKI-1)

The organization ensures that audit reduction and report generation tools used are under the control of Trusted Roles.

CP Section(s):

5.4.2

AU-9 Protection of Audit Security Control Enhancements		
(2)	PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	**FPKI Parameter:** [Assignment: organization-defined frequency] Parameter: [Per CP/CPS]. **CP Section(s):** 5.4.4, 5.5.3
(4)	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].	**FPKI Parameters:** [Assignment: organization-defined subset of users] Parameter: [PKI Trusted Roles] **CP Section(s):** 5.4.4

AU-11 Audit Record Retention		
Base Control		
Control: Retain audit records for [Assignment: organization-defined time-period consistent with records retention policy] to provide support for after-the-fact investigations of security and privacy incidents and to meet regulatory and organizational information retention requirements.		
PKI Specific Requirements Guidance/FPKI Parameter		
FPKI Parameters: [Assignment: organization-defined time period consistent with records retention policy] Parameter: [2 months onsite or until reviewed, and within a long term archive for the period of time specified in the CP and CPS] **CP Section(s):** 5.4.3		
AU-11 Audit Record Retention Security Control Enhancements		
(1)	AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY AU-11 (1) Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.	**FPKI Parameters:** [Assignment: organization-defined measures] Parameter: [in accordance with the PKI CP and CPS] **CP Section(s):** 5.5.2

CA: Security Assessment and Authorization

CA-1 Assessment, Authorization, and Monitoring

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): organization-level; mission/business process-level; system level] assessment, authorization, and monitoring policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the security and privacy assessment, authorization, and monitoring policy and the associated security and privacy assessment, authorization, and monitoring controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:
   1. Policy [Assignment: organization-defined frequency]; and

Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI Parameter

CA-1 (PKI-1)

In addition to local Assessment, Authorization and Monitoring policy, the organization specifies access control Security Assessment and Authorization in the PKI CP and CPS

FPKI Parameters:

CA-1b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority]

CP Section(s):

5.4.2, 5.4.8, 8.2, 8.4, 8.5, 8.6

CA-7 Continuous Monitoring

Base Control

Control:

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [*Assignment: organization-defined metrics*];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessments and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

PKI Specific Requirements Guidance/FPKI 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 CP and CPS

CP Section(s):

5.4.2, 5.4.8, 8.2, 8.4, 8.5, 8.6

CA-8 Penetration Testing

Base Control

Control:

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

PKI Specific Requirements Guidance/FPKI Parameter

CA-8 (PKI-1)

The organization ensures that detailed rules of engagement are agreed upon by Trusted Roles before the commencement of any vulnerability scanning.

FPKI Parameters:

[Assignment: organization-defined systems or system components]

Parameter: [PKI System Components]

CP Section(s):

5.4.8

CM: Configuration Management

CM-1 Configuration Management Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system level] configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the configuration management policy and procedures;

c. Review and update the current configuration management:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI Parameter

CM-1 (PKI-1)

In addition to local Configuration Management policy, the organization specifies Configuration Management in the PKI CP and CPS

FPKI Parameters:

CM-1b.

[Assignment: organization-defined senior management official;]

Parameter: [PKI Policy Authority]

CP Section(s):

6.6.2

CM-2 Baseline Configuration

Base Control

Control:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system.
   1. [Assignment: organization-defined frequency];
   2. When required due to [Assignment organization-defined circumstances]; and
   3. When system components are installed or upgraded.

PKI Specific Requirements Guidance/FPKI Parameter

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 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.

CP Section(s):

6.6.2, 6.7

CM-2 Baseline Configuration Security Control Enhancements

(2)	BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	**FPKI Parameter:** Replaced by CM-2 (PKI-3) **CP Section(s):** N/A

CM-3 Configuration Change Control

Base Control

Control:

a. Determine the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time-period*];
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

PKI Specific Requirements Guidance/FPKI Parameter

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 to deploy updated baselines across the installed base are under the control of PKI Trusted Roles.

CP Section(s):

6.6.2

CM-3 Baseline Configuration Security Control Enhancements		
(3)	CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].	**FPKI Parameter:** Prohibited because CM-3 (PKI-1) is required. **CP Section(s):** N/A
(7)	CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	**FPKI Parameters:** [Assignment: organization-defined frequency] Parameter: [CA Systems] [Assignment: organization-defined circumstances] Parameter: [CA Systems] **CP Section(s):** 6.6.2

CM-5 Access Restrictions for Change
Base Control
Control: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
PKI Specific Requirements Guidance/FPKI 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. **CP Section(s):** 5.1.2, 6.5.1, 6.6.2, 6.7

CM-6 Configuration Setting

Base Control

Control:

a. Establish and document configuration settings for components employed within the system using [*Assignment: organization-defined common secure configurations*] that reflect the most restrictive mode consistent with operational requirements;
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [*Assignment: organization-defined system components*] based on [*Assignment: organization- defined operational requirements*]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

PKI Specific Requirements Guidance/FPKI Parameter

CM-6 (PKI-1)

The organization establishes and documents mandatory configuration settings unique to the CA and RA systems in the PKI CP/CPS*[6.6.2]*

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 CP /CPS

FPKI Parameters:

CM-6a. —Replaced by CM-6 (PKI-1)

CP Section(s):

6.6.2

<table>
<tr><th colspan="3">CM-6 Configuration Setting Security Control Enhancements</th></tr>
<tr><td>(1)</td><td>CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION
Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].</td><td><b>FPKI Parameter:</b>
CM-6 (1). Replaced by CM-6 (PKI-2)
<b>CP Section(s):</b>
6.6.2</td></tr>
</table>

CM-7 Least Functionality

Base Control

Control:

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities] ; and
b. Prohibit or restrict the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]

Parameter: [as specified in the PKI CP/CPS]

CP Section(s):

6.6.1

CM-7 Least Functionality Security Control Enhancements

(4)	LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE (a) Identify [Assignment: organization-defined software programs not authorized to execute on the system]; (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].	**FPKI Parameter:** Prohibited because CM-2 (PKI-1) and CM-2 (PKI-2) are required. **CP Section(s):** N/A

CM-8 System Component Inventory

Base Control

Control:

a. Develop and document an inventory of system components that:
   1. Accurately reflects the current system;
   2. Includes all components within the system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

PKI Specific Requirements Guidance/FPKI Parameter

CM-8 (PKI-1)

The organization ensures that inventory of PKI System Components is performed under the control of Trusted Roles.

CP Section(s):

6.6

CM-8 (PKI-2)

The organization ensures that automated inventory collection mechanisms do not violate the physical access, logical access, and network security requirements defined in the CP/CPS.

CP Section(s):

6.6.2

CP: Contingency Planning

CP-1 Contingency Planning Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): organization-level; mission/business process-level; system level] contingency planning policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the contingency planning policy and procedures;

c. Review and update the current contingency planning:
   1. Policy [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI Parameter

CP-1 (PKI-1)

In addition to local Contingency Planning policy, the organization specifies Contingency Planning in the PKI CP/CPS.

FPKI Parameters:

CP-1 b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority]

CP Section(s):

5.7

CP-2 Contingency Plan Security Control Enhancements		
(3)	CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS Plan for the resumption of [Selection: all; essential] missions and business functions within [Assignment: organization-defined time-period] of contingency plan activation.	**FPKI Parameters:** [Assignment: organization-defined time period] Parameter: [Per CP/CPS] **CP Section(s):** 5.7.1, 5.7.4

CP-7 Alternate Processing Site

Base Control

Control:

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined system operations*] for essential missions and business functions within [*Assignment: organization-defined time-period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time-period for transfer and resumption; and

c. Provide information security and privacy safeguards at the alternate processing site that are equivalent to those at the primary site.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

CP-7a.

[Assignment: organization-defined information system operations]

Parameter: [PKI System]

CP Section(s):

5.1.8, 5.7.4, 6.2.4.1

CP-8 Telecommunication Services

Base Control

Control:

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [*Assignment: organization-defined system operations*] for essential missions and business functions within [*Assignment: organization-defined time-period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Assignment: organization-defined information system operations]

Parameter: [PKI System]

CP Section(s):

2.1, 5.7.4

CP-9 System Backups

Base Control

Control:

a. Conduct backups of user-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
c. Conduct backups of system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
d. Protect the confidentiality, integrity, and availability of backup information

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

CP-9c.

[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]

Parameter: [Per CP/CPS]

CP Section(s):

5.1.8, 6.2.4.1

CP-10 System Recovery And Reconstitution

Base Control

Control:

Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time-period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

CP-10.

[Assignment: organization-defined time-period consistent with recovery time and recovery point objectives]

Parameter: [Per CP/CPS] Control Enhancements:

CP-10 (4)

[Assignment: organization-defined restoration time-periods] Parameter: [Per CP/CPS]

CP Section(s):

5.1.8, 6.2.4.1

CP-10 System Recovery and Reconstitution Security Control Enhancements

(4)	SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME-PERIOD Provide the capability to restore system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	**FPKI Parameters:** [Assignment: organization-defined restoration time-periods] Parameter: [Per CP/CPS] **CP Section(s):** 5.7.4

IA: Identification and Authentication

IA-1 Identification and Authentication Policy and Procedures

Base Control

Control:

Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

[Selection (one or more): organization-level; mission/business process-level; system level] identification and authentication policy that:

Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures;

Review and update the current identification and authentication:

Policy [Assignment: organization-defined frequency]; and

Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI 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 CP/CPS

CP Section(s):

3.2, 3.3, 3.4, 5.2.3, 6.5.1, 6.7

IA-2 Identification and Authentication (Organizational Users) Security Control Enhancements		
(8)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS - REPLAY RESISTANT Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].	**FPKI Parameters:** [Assignment: Selection (one or more): privileged accounts; non-privileged accounts] Parameter: [Privileged Accounts], **CP Section(s):** 6.5.1

IA-3 Device Identification and Authentication
Base Control
Control: Uniquely identify and authenticate [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.
PKI Specific Requirements Guidance/FPKI Parameter
FPKI Parameters: [Assignment: organization-defined list of specific and/or types of devices] Parameter: [Per CP/CPS] [Selection (one or more): local; remote; network] Parameter: [Remote] **CP Section(s):** 6.7

IA-4 Identifier Management Security Control Enhancement		
(4)	IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS Manage individual identifiers by uniquely identifying each individual as [Assignment: organization- defined characteristic identifying individual status]	**FPKI Parameters:** [Assignment: organization-defined characteristic identifying individual status] Parameter: [a PKI Trusted Role] **CP Section(s):** 3.1.5

IA-7 Cryptographic Module Authentication
Base Control
Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines for such authentication.
PKI Specific Requirements Guidance/FPKI Parameter
IA-7 (PKI-1) **Implement mechanisms for c**ryptographic module activation, data creation, protection and use documented in the CP/CPS. **CP Section(s):** 6.2, 6.4

IA-12 Identity Proofing

Base Control

Control:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
b. Resolve user identities to a unique individual; and
c. Collect, validate, and verify identity evidence.

PKI Specific Requirements Guidance/FPKI Parameter

(PKI-1)

In addition to local identity proofing policy and procedures, the organization specifies identity proofing policy and procedures in the PKI CP/CPS.

CP Section(s):

3.2, 3.3, 3.4

IR: Incident Response

IR-1 Incident Response Policy and Procedures

Base Control

Control:

d. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. An incident response policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

e. Designate an [*Assignment: organization-defined senior management official*] to manage the incident response policy and procedures;

f. Review and update the current incident response:
   1. Policy [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency]

PKI Specific Requirements Guidance/FPKI 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 CP/CPS.

FPKI Parameters:

IR-1b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority]

CP Section(s):

5.7.1

IR-2 Incident Response Training

Base Control

Control:

Provide incident response training to system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time-period*] of assuming an incident response role or responsibility
b. When required by system changes; and
c. [Assignment: organization-defined frequency] thereafter.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

IR-2b.

[Assignment: organization-defined frequency]

Parameter: [as required by local policy]

CP Section(s):

5.3.3

IR-4 Incident Handling Security Control Enhancements		
(1)	INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES Support the incident handling process using [Assignment: organization-defined automated mechanisms].	IR-4 (1) The organization ensures that if automated Incident Response mechanisms are implemented on the CA, control of these mechanisms are is limited to Trusted Roles CP Section(s): 6.5.1, 6.6.2
(2)	INCIDENT HANDLING | DYNAMIC RECONFIGURATION Include the following types of dynamic reconfiguration for [Assignment: organization defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].	IR-4 (2) The organization ensures that if automated Incident Response mechanisms are implemented on the CA, control of these mechanisms are is limited to Trusted Roles CP Section(s): 6.5.1, 6.6.2

IR-5 Incident Monitoring
Base Control
Control: Track and document security, privacy, and supply chain incidents.
PKI Specific Requirements Guidance/FPKI Parameter
IR-5 (PKI-1) The organization ensures that any automated mechanisms used to support incident monitoring are under the control of Trusted Roles **CP Section(s):** 5.7.1

IR-6 Incident Reporting

Base Control

Control:

a. Require personnel to report suspected security and privacy incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and
b. Report security, privacy, and supply chain incident information to [*Assignment: organization- defined authorities*].

PKI Specific Requirements Guidance/FPKI Parameter

IR-6 (PKI-1)

The organization ensures that any automated mechanisms used to support incident reporting are under the control of Trusted Roles

CP Section(s):

5.7.1, 5.7.2

IR-7 Incident Response Assistance

Base Control

Control:

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

PKI Specific Requirements Guidance/FPKI Parameter

IR-7 (PKI-1)

The organization ensures that any automated mechanisms used to support incident response are under the control of Trusted Roles

CP Section(s):

5.7.1, 5.7.2

IR-8 Incident Response Plan

Base Control

Control:

a. Develop an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
   8. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and
   9. Explicitly designates responsibility for incident response to [*Assignment: organization-defined entities, personnel, or roles*].

b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

IR-8 PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

IR-8a.

[Assignment: organization-defined personnel or roles]

Parameter: [Trusted Roles and the organization’s PKI Policy Authority]

[Assignment: organization-defined entities, 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-8d.

[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

CP Section(s):

5.7

MA: Maintenance

MA-1 Policy and Procedures

Base Control

Control:

- a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
- b. [Selection (one or more): organization-level; mission/business process-level; system level] maintenance policy that:
  - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  - (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
  - 2. Procedures to facilitate the implementation of the system maintenance policy and the associated system maintenance controls;
- c. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the system maintenance policy and procedures;
- d. Review and update the current system maintenance:
  - 1. Policy [Assignment: organization-defined frequency]; and
  - 2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI Parameter

MA-1 (PKI-1)

In addition to local Maintenance policy and procedures, the organization specifies Maintenance policy and procedures in the PKI CP/CPS.

FPKI Parameters:

MA-1b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority].

CP Section(s):

6.6

MA-2 Controlled Maintenance

Base Control

Control:

a. Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
c. Require that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];
e. Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
f. Include the following information in organizational maintenance records: [Assignment: organization-defined information]

PKI Specific Requirements Guidance/FPKI Parameter

MA-2 (PKI-1)

The organization ensures that Maintenance of the PKI System Components is performed under the control of the Trusted Roles.

CP Section(s):

5.1.2, 6.6.1

MA-3 Maintenance Tools

Base Control

Control:

a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools [*Assignment: organization-defined frequency*].

PKI Specific Requirements Guidance/FPKI Parameter

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 Authority prior to use and are used under the control of the PKI Trusted Roles.A-3

MA-3 (PKI-2)

The organization ensures that the PKI 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

CP Section(s):

6.6

MA-4 Nonlocal Maintenance

Base Control

Control:

a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

PKI Specific Requirements Guidance/FPKI Parameter

MA-4 (PKI-1)

The organization only permits non-local maintenance if all the control requirements that apply to the CA are applied equally to any remote workstations used to administer the CA.

CP Section(s):

5.1, 6.7

MA-5 Maintenance Personnel

Base Control

Control:

a. Establish a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

PKI Specific Requirements Guidance/FPKI Parameter

MA-5 (PKI-1)

The organization ensures that Maintenance personnel are under the supervision of PKI Trusted Roles

CP Section(s):

5.1.2

MA-6 Timely Maintenance

Base Control

Control:

Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time-period] of failure.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[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]

CP Section(s):

5.7.4

MP: Media Protection

MP-1 Media Protection Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
    1. [Selection (one or more): organization-level; mission/business process-level; system level] media protection policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the media protection policy and procedures;

c. Review and update the current media protection:
    1. Policy [Assignment: organization-defined frequency]; and
    2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI 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 CP/CPS *[5.1 Physical Controls]*

FPKI Parameters:

MP-1b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority]

CP Section(s):

5.1.6

MP-2 Media Access

Base Control

Control:

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

PKI Specific Requirements Guidance/FPKI Parameter

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.

FPKI Parameters:

[Assignment: organization-defined types of digital and non-digital media]

Parameter: [all media]

[Assignment: organization-defined list personnel or roles]

Parameter: [Trusted Roles]

CP Section(s):

5.1.6

MP-4 Media Storage

Base Control

Control

a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and
b. Protect system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

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]

CP Section(s):

5.1.6, 5.1.7

MP-5 Media Transport

Base Control

Control:

a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];
b. Maintain accountability for system media during transport outside of controlled areas;
c. Document activities associated with the transport of system media; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

PKI Specific Requirements Guidance/FPKI Parameter

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.

FPKI Parameters:

MP-5a.

[Assignment: organization-defined types of information system media]

Parameter: [all CA media]

[Assignment: organization-defined security safeguards]

Parameter: [mitigating security mechanisms].

CP Section(s):

5.1.6

MP-7 Media Use

Base Control

Control:

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Selection: restricts; prohibits]

Parameter: [restricts]

[Assignment: organization-defined information systems or system components]

Parameter: [PKI Systems]

[Assignment: organization-defined security safeguards]

Parameter: [Assignment: organization-defined security safeguards] that are under the control of PKI Trusted Roles]

CP Section(s):

5.1.6

PE: Physical and Environmental Protection

PE-1 Physical and Environmental Protection Policy and Procedures

Base Control

Control:

- a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
  - 1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that:
    - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
  - 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;
- b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
- c. Review and update the current physical and environmental protection:
  - 1. Policy [Assignment: organization-defined frequency]; and
  - 2. Procedures [Assignment: organization-defined frequency].

PKI Specific Requirements Guidance/FPKI 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 CP/CPS *[5.1.2]*

FPKI Parameters:

PE-1b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority]

CP Section(s):

5.1

PE-2 Physical Access Authorizations

Base Control

Control:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
b. Issue authorization credentials for facility access
c. Review the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and
d. Remove individuals from the facility access list when access is no longer required.

PKI Specific Requirements Guidance/FPKI Parameter

PE-2 (PKI-1)

The organization ensures required multi-party control by specified Trusted Roles for physical access to PKI CA information systems

CP Section(s):

5.2.1, 5.2.2

PE-3 Physical Access Control

Base Control

Control:

a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress and egress to the facility using [*Selection (one or more):*

b. Maintain physical access audit logs for [Assignment: organization-defined entry/exit points];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined controls];

d. Escort visitors and monitor visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and

g. Change combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

PKI Specific Requirements Guidance/FPKI Parameter

PE-3 (PKI-1)

The organization ensures required multi-party control by specified Trusted Roles for physical access to PKI CA information systems

CP Section(s):

5.2.1, 5.2.2

<table>
<tr><th colspan="3">PE-3 Physical Access Control Security Control Enhancements</th></tr>
<tr><td>(4)</td><td>PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS
Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.</td><td><b>FPKI Parameters:</b>
PE-3 (4)
[Assignment: organization-defined information system components one or more components of the information system]
Parameter: [PKI System Components]
<b>CP Section(s):</b>
5.1.2</td></tr>
</table>

PE-4 Access Control for Transmission
Base Control
Control: Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].
PKI Specific Requirements Guidance/FPKI Parameter
FPKI Parameters: **PE-4** [Assignment: organization-defined security safeguards] Parameter: [PKI CP/CPS] **CP Section(s):** 5.1.2

PE-6 Monitoring Physical Access

Base Control

Control:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

PE-6b.

[Assignment: organization-defined frequency]

Parameter: [PKI CP/CPS].

[Assignment: organization-defined events or potential indications of events]

Parameter: [PKI CP/CPS]

CP Section(s):

5.1.2

PE-8 Visitor Access Records

Base Control

Control:

a. Maintain visitor access records to the facility where the system resides for [*Assignment: organization-defined time-period*]; and
b. Review visitor access records [Assignment: organization-defined frequency].
c. Report anomalies in visitor access records to [Assignment: organization-defined personnel]

PKI Specific Requirements Guidance/FPKI Parameter

PE-8 (PKI-1)

PKI Systems must maintain physical access logs of all personnel, including visitors, as defined in the PKI CP/CPS.

FPKI Parameters:

PE-8a.

[Assignment: organization-defined time period]

Parameter: [PKI CP/CPS]

PE-8b.

[Assignment: organization-defined frequency]

Parameter: [PKI CP/CPS].

CP Section(s):

5.1.2

PE-8 Visitor Access Records Security Control Enhancements

(1)	VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].	**FPKI Parameter:** Optional: automated mechanisms for access records are not required. **CP Section(s):** N/A

PE-11 Emergency Power

Base Control

Control:

Provide a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] transition of the system to long-term alternate power] in the event of a primary power source loss.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power]

Parameter: [PKI CP/CPS].

CP Section(s):

5.1.3

PE-16 Delivery and Removal

Base Control

Control:

a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and
b. Maintain records of the system components.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Assignment: organization-defined types of information system components]

Parameter: [all PKI System components]

CP Section(s):

5.1.2

PE-17 Alternate Work Site

Base Control

Control:

a. Determine and document the [*Assignment: organization-defined alternate work sites*] allowed for use by employees;
b. Employ [Assignment: organization-defined security and privacy controls] at alternate work sites;
c. Assess the effectiveness of security and privacy controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

PE-17a.

[Assignment: organization-defined alternate worksite]

Parameter: [PKI CP/CPS]

PE-17b.

[Assignment: organization-defined security controls]

Parameter: [CP/CPS]

CP Section(s):

5.1.1

PE-18 Location of Information System Components
Base Control
Control: Position system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access
PKI Specific Requirements Guidance/FPKI Parameter
FPKI Parameters: [Assignment: organization-defined physical and environmental hazards] Parameter: [PKI CP/CPS] **CP Section(s):** 5.1.3, 5.1.4, 5.1.5

PL: Planning

PL-1 Planning Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): organization-level; mission/business process-level; system level] planning policy that:
      (a) Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Are consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the security and privacy planning policies and the associated security and privacy planning controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the security and privacy planning policies and procedures;

c. Review and update the current security and privacy planning:
   1. Policies [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI Parameter

PL-1 (PKI-1)

In addition to local Planning policy and procedures, the organization specifies Security Planning policy and procedures in the PKI CP/CPS

FPKI Parameters:

PL-1b.

[Assignment: organization-defined senior management official]

Parameter: [PKI Policy Authority]

CP Section(s):

1.5, 9.6, 9.12.1

PM: Program Management

PS: Personnel Security

PS-1 Personnel Security Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): organization-level; mission/business process-level; system level] personnel security policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [*Assignment: organization senior management official*] to manage the development, documentation, and dissemination of the personnel security policy and procedures;

c. Review and update the current personnel security:
   1. Policy [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI 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 CP/CPS. *[5.3 Personnel Controls]*

CP Section(s):

5.3

PS-3 Personnel Screening

Base Control

Controls:

a. Screen individuals prior to authorizing access to the system; and
b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].

PKI Specific Requirements Guidance/FPKI Parameter

PS-3 (PKI-1)

In addition to local Personnel screening requirements, the organization follows Personnel screening/citizenship requirements in the PKI CP/CPS.

CP Section(s):

5.3.2

PS-6 Access Agreement

Base Control

Controls:

a. Develop and document access agreements for organizational systems;
b. Review and update the access agreements [*Assignment: organization-defined frequency*]; and
c. Verify that individuals requiring access to organizational information and systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

PKI Specific Requirements Guidance/FPKI Parameter

PS-6 (PKI-1)

The organization e nsures that individuals in PKI Trusted Roles acknowledge operational and security responsibilities upon appointment to the role.

FPKI Parameter:

PS-6b.

Replaced by PS-6 (PKI-1)

PS-6b.

[Assignment: organization-defined frequency]

Parameter: Not Applicable

CP Section(s):

5.3

RA: Risk Assessment

RA-1 Risk Assessment Policy and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [*Assignment: organization-defined senior management official*] to manage the risk assessment policy and procedures;

c. Review and update the current risk assessment:
   1. Policy [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency];.

PKI Specific Requirements Guidance/FPKI 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 CP/CPS *[8 Compliance Audit and Other Assessments]*

CP Section(s):

1.4.1

RA-5 Vulnerability Monitoring and Scanning

Base Control

Controls:

a. Monitor and scan for vulnerabilities in the system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

PKI Specific Requirements Guidance/FPKI Parameter

RA-5 (PKI-1)

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-2)

The organization ensures that detailed rules of engagement are agreed upon by Trusted Roles before the commencement of any vulnerability scanning.

CP Section(s):

5.4.8

SA: System Acquisition

SA-1 System and Service Acquisition Policy and Procedures

Base Control

Control:

- a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
  - 1. [Selection (one or more): organization-level; mission/business process-level; system level] system and services acquisition policy that:
    - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    - (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
  - 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;
- b. Designate an [*Assignment: organization-defined senior management official*] to manage the system and services acquisition policy and procedures;
- c. Review and update the current system and services acquisition:
  - 1. Policy [Assignment: organization-defined frequency]; and
  - 2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI Parameter

SA-1 (PKI-1)

In addition to local System and Services Acquisition policy and procedures, the organization specific System and Services Acquisition policy and procedures will be documented in the PKI CP/CPS.

CP Section(s):

6.6.1

SC: System and Communications Protection

SC-1 Policy and Procedures
Base Control
Control: d. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; e. Designate an [*Assignment: organization-defined senior management official*] to manage the system and services acquisition policy and procedures; f. Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency];
PKI Specific Requirements Guidance/FPKI 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 CP/CPS. **CP Section(s):** 6.7

SC-7 Boundary Protections Security Control Enhancements		
(21)	BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	**FPKI Parameters:** [Assignment: organization defined information system components] Parameter: [PKI System components] [Assignment: organization-defined missions and/or business functions] Parameter: [PKI] **CP Section(s):** 6.7

SC-8 Transmission Confidentiality and Integrity
Base Control
Control: Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
PKI Specific Requirements Guidance/FPKI Parameter
SC-8 (PKI-1) The use of unencrypted protocols such as HTTP or LDAP is permitted by policy when exchanging public data contained in digitally signed objects such as certificates or CRLs. **FPKI Parameters:** [Assignment: Selection (one or more): confidentiality; integrity] [Parameter: integrity] **CP Section(s):** 2.2.1

SC-13 Cryptographic Protection

Base Control

Control:

a. Determine the [Assignment: organization-defined cryptographic uses]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

PKI Specific Requirements Guidance/FPKI Parameter

FPKI Parameters:

[Assignment: organization-defined cryptographic uses and type of cryptography required for each use]

Parameter: [PKI cryptography and algorithms]

CP Section(s):

6.1.5, 7.1.3

SC-15 Collaborative Computing Devices and Applications

Base Control

Control:

c. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and

d. Provide an explicit indication of use to users physically present at the devices.

PKI Specific Requirements Guidance/FPKI Parameter

SC-15 (PKI-1)

The organization ensures that collaborative computing devices are prohibited on PKI System Components

FPKI Parameters:

SC-15 (PKI-1) replaces SC-15 (1), (3), (4)

CP Section(s):

N/A

SI: System and Information Integrity

SI-1 System and Information Integrity and Procedures

Base Control

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): organization-level; mission/business process-level; system level] system and information integrity policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures;

c. Review and update the current system and information integrity:
   1. Policy [Assignment: organization-defined frequency]; and
   2. Procedures [Assignment: organization-defined frequency];

PKI Specific Requirements Guidance/FPKI 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 for PKI Systems in the PKI CP/CPS.

CP Section(s):

6.6

SI-2 Flaw Remediation

Base Control

Control:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time-period*] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

PKI Specific Requirements Guidance/FPKI Parameter

SI-2 (PKI-1)

The organization ensures that any Flaw Remediation mechanisms are under control of PKI Trusted Roles

CP Section(s):

5.4.8, 6.6

SI-2 Flaw Remediation Security Control Enhancements

(5)	FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].	**FPKI Parameters:** Prohibited. Patches must be reviewed and approved by Trusted Role Personnel prior to installation on PKI Systems. **CP Section(s):** N/A

SI-3 Malicious Code Protection

Base Control

Control:

a. Implement [*Selection (one or more): signature based; non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
    1. Perform periodic scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and
    2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization- defined personnel or roles] in response to malicious code detection.
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

PKI Specific Requirements Guidance/FPKI Parameter

SI-3 (PKI-1)

The organization ensures that any Malicious Code Protection update mechanisms for the PKI CA components are under control of PKI Trusted Roles.

CP Section(s):

6.6.1

SI-4 System Monitoring

Base Control

Control:

a. Monitor the system to detect:
    1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization- defined monitoring objectives*]; and
    2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:
    1. Strategically within the system to collect organization-determined essential information; and
    2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

PKI Specific Requirements Guidance/FPKI Parameter

SI-4 (PKI-1)

The organization ensures that Information System Monitoring tools for the PKI CA components are under the control of PKI Trusted Roles.

CP Section(s):

5.4.2

SI-6 Security and Privacy Functionality Verification

Base Control

Control:

a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];
b. Perform the verification of the functions specified in SI-6a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];
c. Notify [*Assignment: organization-defined personnel or roles*] of failed security and privacy verification tests; and
d. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

PKI Specific Requirements Guidance/FPKI Parameter

SI-6 (PKI-1)

Systems verify that audit logging is turned on at startup and notifications are received for any audit logging that fails.

CP Section(s):

5.4.6

SI-7 Software, Firmware, and Information Integrity

Base Control

Control:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [*Assignment: organization-defined software, firmware, and information*]; and
b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [*Assignment: organization-defined actions*].

PKI Specific Requirements Guidance/FPKI Parameter

SI-7 (PKI-1)

The organization ensures that Software, Firmware and Information Integrity tools for the PKI system are under the control of Trusted Roles.

FPKI Parameter:

SI-7.a.

[Assignment: organization-defined software, firmware, and information]

Parameter: [PKI Systems]

CP Section(s):

6.6

APPENDIX B: REFERENCES

SP 800-53 NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

SP 800-53B NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

COMMON X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, September 2020

https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-common.pdf