Common Policy Framework Certificate Policy Change Proposal Number: 2017-02

To: Federal PKI Policy Authority (FPKIPA)

From: Chi Hickey, Co-chair, FPKIPA

Subject: Proposed modifications to the Common Policy Framework Certificate Policy

Date: April 3, 2017

Title: Notification of Issue Resolution and Remediation

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.25, September 22, 2016

Change Advocate's Contact Information: chi.hickey@gsa.gov

Organization requesting change: FPKI Policy Authority

Change summary: Implementation of this change proposal will require CAs issuing under the COMMON Policy Framework to publish information pertaining to resolved incidents on their websites.

Background:

Situations have surfaced that require members in the PKI to make changes in their infrastructure to remedy a violation of policy or operational vulnerability. This change will require that these actions be reported on the affected CA's website along with an explanation and additional remedial action, if any.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The FPKIPA shall be notified if any CAs operating under this policy experience the following:

- suspected or detected compromise of the CA systems;

- suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension);
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

The FPKIPA will take appropriate steps to protect the integrity of the Federal PKI.

The CA's Management Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

In the event of an incident as described above, the organization operating the CA shall notify the FPKIPA within 24 hours of incident discovery, along with preliminary remediation analysis.

Within 10 business days of incident resolution, the organization operating the CA shall post a notice on its publically available web page identifying the incident and provide notification to the FPKIPA The public notice shall include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident.
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

The notification provided directly to the FPKIPA shall also include detailed measures taken to remediate the incident. The FPKIPA will post the notices to idmanagement.gov and provide an announcement to all Federal Agencies and Bridge Affiliate PKIs.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
- If the CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

The Agency PMA shall be notified as soon as possible.

In the event of an incident as described above, the organization operating the CA shall post a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations must be performed.

The FPKIPA shall be immediately informed, as well as any superior or cross-certified CAs and any entities known to be distributing the CA certificate (e.g., in a root store).

The CA must generate new keys in accordance with section 6.1.1.1.

If the CA distributed the private key in a Trusted Certificate, the CA shall perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in section 6.1.4.
- Initiate procedures to notify subscribers of the compromise.

Subscriber certificates may be renewed automatically by the CA under the new key pair (see section 4.6), or the CA may require subscribers to repeat the initial certificate application process.

The organization operating the CA shall post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

Estimated Cost:

There may be a cost to the infrastructure to update documentation and train personnel in this procedure.

Implementation Date:

This change will be effective immediately upon the date of approval by the FPKIPA and incorporation into the Federal Common Policy Framework Certificate Policy.

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	April 3, 2017
Date change released for comment:	May 17, 2017
Date comment adjudication published:	June 1, 2017