FBCA Certificate Policy Change Proposal Number: 2017-02

To: Federal PKI Policy Authority (FPKIPA)
From: Chi Hickey, Co-Chair, FPKIPA
Subject: Proposed modifications to the Federal Bridge 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 Federal Bridge Certification Authority (FBCA) Version 2.30, October 5, 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 participating in the FPKI 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 & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The members of the FPKIPA shall be notified if any of the following cases occur:

- suspected or detected compromise of the ~~FB~~CA systems;
- physical or electronic attempts to penetrate ~~FB~~CA systems;
- denial of service attacks on ~~FB~~CA components;
- any incident preventing the ~~FB~~CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow member entities to protect their interests as Relying Parties.

The FPKIMA or Entity PKI PMA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the ~~FBCA~~ applicable CPS.

~~Entity CAs shall provide notice as required by the applicable MOA.~~ In the event of an incident as described above, the Entity 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 web page identifying the incident and provide notification to the FPKPA. 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.

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

When computing resources, software, and/or data are corrupted, the FBCA and Entity CAs 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 4.9.7, Table 4.
- 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.

In the event of an incident as described above, the Entity 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

If the FBCA or Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The FPKIPA and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;
- A new FBCA or Entity CA key pair shall be generated by the FBCA or Entity CA in accordance with procedures set forth in the FBCA or Entity CPS; and
- • New FBCA or Entity CA certificates shall be issued to Entities also in accordance with the FBCA or Entity CPS.

If the CA distributes its key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4.

The FPKIMA or Entity CA governing body shall also investigate and report to the FPKIPA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

The Entity 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 approval by the FPKIPA and incorporation into the FBCA Certificate Policy.

Prerequisites for Adoption:

None

Plan to Meet Prerequisites:

N/A.

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