FPKIPA

Federal Public Key Infastructure Policy Authority

Federal Public Key Infrastructure (FPKI) Incident Management Plan

Federal PKI Policy Authority

Version 3.0

September 4, 2020

Revision History

Document Version	Document Date	Revision Details
1.0	February 21, 2012	Final based on CPWG review and comment period
2.0 (draft)	May 1, 2017	**Draft** update incorporating: ● include the FPKI Non-Compliance Management framework ● add notification requirements from Public Trust Store Programs ● remove references to the E-Governance Certification Authorities ● align Incident Management Process with NIST SP 800-61 Revision 2 – *Computer Security Incident Handling Guide* Note: Additional updates were requested during the comment period, and version 2.0 was not finalized.
3.0	September 4, 2020	Document updated to: ● adjudicate comments made to draft version 2.0 ● focus scope on incident management, rather than vulnerability management ● change title from *Incident Management Process For The Federal Public Key Infrastructure (FPKI) Community*

Table of Contents

1 INTRODUCTION

OMB Circular A-130 established requirements for the General Services Administration (GSA) to ensure effective controls are in place to protect and monitor Federal Public Key Infrastructure (FPKI) components. The FPKI provides the U.S. Government with a common baseline to administer digital certificates and public-private key pairs used to support federated trust of government devices and persons.

Incidents[1] are events that adversely affect the confidentiality, integrity, or availability of FPKI systems, or the validation of the certificates issued. Examples of incidents include:

- a compromised FPKI certification authority (CA)
- a compromised Personal Identity Verification (PIV) credential content signing private key
- a denial of service attack
- the unavailability of FPKI components (e.g., Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP) Responder, Authority Information Access (AIA) repository, etc.) and
- certificate mis-issuance (i.e., any certificate issued in a manner that violates the applicable Certificate Policy or Certification Practice Statement).

1.1 Purpose

This document provides guidance on the roles and responsibilities applicable to the FPKI Policy Authority (FPKIPA), FPKI Management Authority (FPKIMA), and FPKI affiliates in the event of an incident. Additionally, this document supplements each FPKI affiliate's Incident Management Process (IMP) with guidance related to incident reporting and response.

1.2 Audience

This document is intended for use by the Federal PKI Authorities, described in Section 2.1.

1.3 Scope

The scope of this document is limited to FPKI incident management as implemented by the FPKI Authorities and FPKI affiliates, collectively known as the "FPKI Community". This includes roles and responsibilities, incident impact analysis, communications planning, and coordination of response activities.

Specific approaches used for incident root cause identification and resolution are out of scope.

[1] FISMA defines "incident" as "an occurrence that - (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

2 Roles and Responsibilities

2.1 Federal PKI Authorities

2.1.1 Federal PKI Policy Authority (FPKIPA)

The FPKIPA must consider technical, policy, and mission business impacts when responding to incidents. While the FPKIPA Co-chairs have authority to coordinate immediate action in emergency situations (e.g., a certificate revocation due to a CA compromise), the FPKIPA, as the governing body for the FPKI, approves longer-term actions in response to incidents.

FPKIPA responsibilities related to the incident management process include:

1. Communicating specific incidents, planned responses, statuses, and resolutions to the FPKI Community and federal agencies
2. Initiating response plans by:
    a. Directing working groups to perform analyses of issues related to existing incidents or their recurrence
    b. Approving Certificate Policy changes as a result of analysis and remediation of incidents
    c. Publishing guidance related to or resulting from incidents
    d. Authorizing revocation of a certificate issued by the FPKIMA
    e. Coordinating with the FPKIMA
3. Approving the Remediation Action Plan (see Appendix A) and tactics

If an incident's root cause is not known or well-understood, the FPKIPA may request working groups to determine its origin. Working groups may also be asked to research preventative measures, or identify policy enhancements to prevent similar incidents in the future.

Depending on the scope of an incident, the FPKIPA may coordinate with federal executive branch agencies, or other organizations to include:

- the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS);
- the Office of Management and Budget (OMB);
- the National Institute of Standards and Technology (NIST);
- the National Security Agency (NSA) and/or U.S. Cyber Command;
- a specific FPKI Community member or product vendor

Depending on the incident's event domain, described more in Section 3.2.2.2.2, additional incident reporting requirements such as those included in the US-CERT Federal Incident Notification Guidelines must be followed.

2.1.2 Federal PKI Management Authority (FPKIMA)

The FPKIMA is responsible for the operations of the Federal Common Policy CA and the Federal Bridge CA, to include issuance and revocation of cross certificates at the direction of the FPKIPA. The FPKIMA coordinates the execution of the incident management plan on behalf of the FPKI Community, monitors incident sources, and assists with impact assessments and associated remediation activities.

The FPKIMA maintains a knowledge base of reported incidents to assist in developing responses for future incidents and responds to FPKIPA requests to investigate newly discovered incidents that may impact the FPKI Community.

FPKIMA responsibilities related to the incident management process include:

1. Facilitating communications with affected affiliates on behalf of the FPKI Authorities
    a. Confirming receipt of incident notification
    b. Updating the FPKIPA regarding any additional incident information and providing input to operational impacts
2. Preparing and finalizing the Security Event Report (Appendix A)
3. Providing initial guidance on issue resolution provided historical or internal knowledge regarding PKI operations
4. Performing certificate issuance or revocation activities at the request of the FPKIPA

2.2 Federal PKI Affiliates

FPKI affiliates include federal agencies and commercial service providers operating a certification authority certified by the Federal PKI Policy Authority.

FPKI affiliate responsibilities related to the incident management process include:

1. Communicating security incidents involving infrastructures or services to the FPKI Authorities, users/customers, and known relying parties.
2. Providing additional investigation support and/or information about incidents to the FPKI Authorities as they become known, and
3. Conducting remediation activities once an incident is confirmed.

Each FPKI affiliate should have internally defined processes in place for detecting and responding to incidents, in accordance with NIST SP 800-61 and US-CERT reporting guidelines. This document provides additional guidance that FPKI affiliates should incorporate into their incident planning procedures. In particular, FPKI affiliates should plan for reports and communications with the FPKI Authorities, as outlined by this document.

3 Incident Management Process

All participants in the FPKI Community have responsibility for the incident management process, which is divided into four (4) phases:

1. Detection

2. Diagnosis

3. Resolution
4. Post-Resolution Activity

3.1 Phase 1: Detection

FPKI Community members share responsibility for detecting incidents.

The FPKIMA monitors internal sensors and public data sources available from industry groups and other consortiums to identify suspected or confirmed incidents that may affect the FPKI Community.

3.1.1 Detection Communication

FPKI affiliates must report incidents to the FPKI Authorities at fpki@gsa.gov. Upon receipt of incident discovery, the FPKIPA is responsible for determining what information should be communicated throughout the FPKI Community and with other government stakeholders, and by what means.

Once identified, the FPKI affiliate responsible for the incident (hereinafter referred to as "responsible FPKI affiliate") will do the following:

1. Immediately confirm with the FPKI Authorities at fpki@gsa.gov that an incident has occurred.
2. Submit an initial Security Event Report (Appendix A) to the FPKI Authorities within 24 hours of event detection/notification.
3. Provide stakeholder updates consistent with guidance from the FPKI Authorities.

Communications pertaining to the reporting of an incident are distinct from normal operational communications. Incident reporting supports the overall security of the FPKI. The submission of an incident report does not imply an admission of guilt or fault.

3.1.2 Receipt and Distribution

Upon receiving an initial communication from the detecting organization that an incident has occurred, the FPKI Authorities will execute the following steps:

1. FPKIMA - Assign an action officer to work with the responsible FPKI affiliate. The action officer will be responsible for maintaining an event record to include all communications between the FPKI Authorities, and:
    a. the detecting organization,
    b. the responsible FPKI affiliate, and
    c. other government or external organizations, if applicable.
2. FPKIMA - Action officer will confirm the submission of the Security Event Report and share relevant updates with the FPKIPA.
3. FPKIMA - Provide the responsible FPKI affiliate with initial guidance, if applicable.
4. FPKIPA - Communicate status with the FPKI Community, as appropriate.

3.2 Phase 2: Diagnosis

In Phase 2: Diagnosis, the FPKI Authorities will work with members of the FPKI Community, as needed, to diagnose the incident. This activity will result in an impact analysis and assignment of a Total Impact Rating, described in Section 3.2.2.2.

3.2.1 DIAGNOSIS COMMUNICATION

As part of the Diagnosis phase, the responsible FPKI affiliate will:

- Continue mitigation actions and communications consistent with internal policy and established agreements (e.g., FPKI Memorandums of Agreement, customer service level agreements, etc.).
- Collaborate with FPKI Authorities in their security event investigation.
- Act on guidance provided by the FPKI Authorities, or other government authority.

3.2.2 IMPACT ANALYSIS AND RISK RATING

Upon receipt of the Security Event Report, the FPKI Authorities will coordinate the following steps with the responsible FPKI affiliate:

1. Conduct a security event investigation.
2. Conduct a security event impact assessment.
3. Develop remediation recommendations and an action plan.
4. Notify the FPKI Community of the incident.

Additional federal stakeholders may be involved in the above steps.

The results of the security event investigation, security event impact assessment, and remediation recommendations, detailed below, shall be documented in the consolidated Security Event Report. The Security Event Report will be a living document until the incident has been remediated, and all post-resolution activity has been completed. The FPKI Authorities will determine when the report is complete.

3.2.2.1 SECURITY EVENT INVESTIGATION

The purpose of the security event investigation is to determine the root cause of the incident. In addition to providing input to the security event impact assessment, the investigation helps determine the actual or potential future impacts of the incident on the FPKI Community.

3.2.2.2 SECURITY EVENT IMPACT ASSESSMENT

Regardless of the incident’s origin, an assessment shall be performed to determine the extent of any current or potential future impacts on the FPKI Community. This assessment shall be performed by the FPKI Authorities in consultation with the responsible FPKI affiliate, and may include other relevant federal stakeholders. Figure 1 describes the security event impact assessment criteria and rating methodology.

Figure 1 shows factors used in determining a Total Impact Rating (R). The rating is the sum of the ratings (r) for each of the event type, event domain, time to impact, and impacted community factors. The following provides a description for each of these factors.

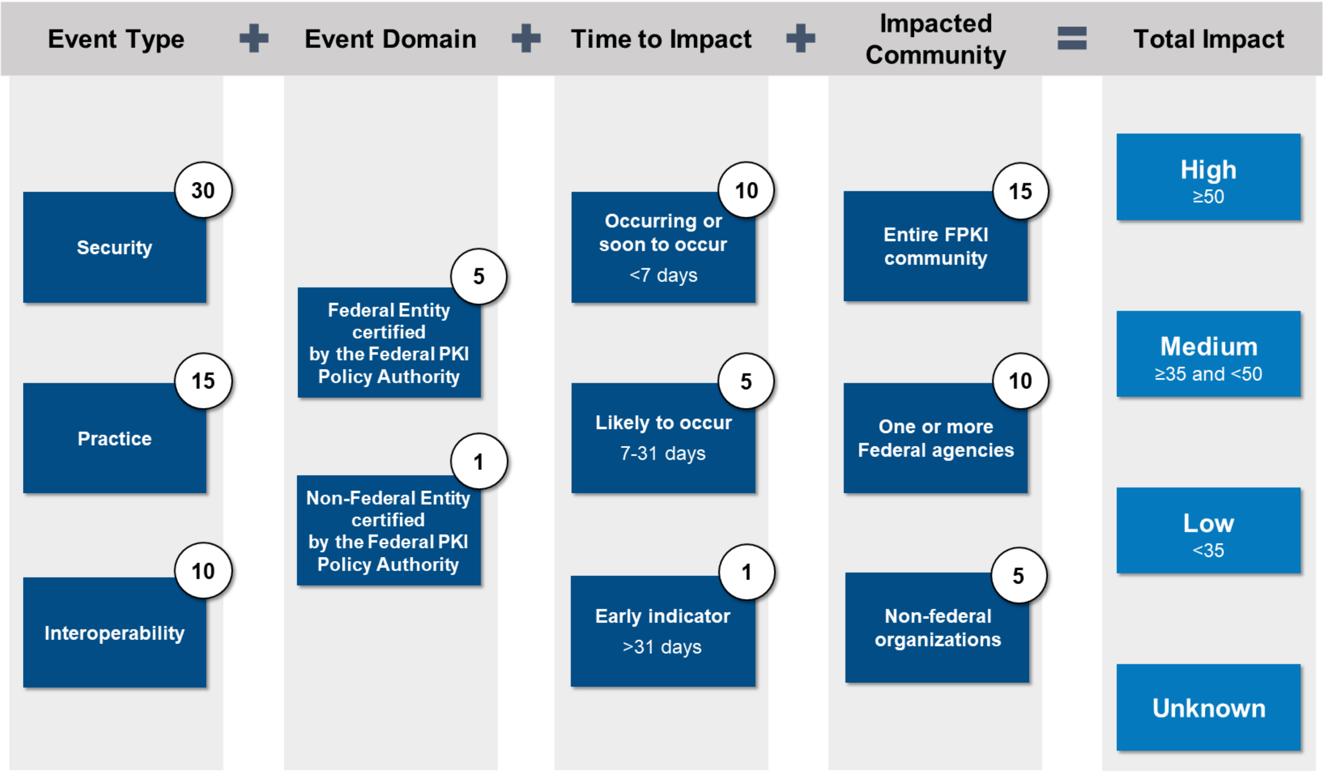
Event Type
Event Domain
Time to Impact
Impacted Community
Total Impact
30
Security
15
Practice
10
Interoperability
5
Federal Entity certified by the Federal PKI Policy Authority
1
Non-Federal Entity certified by the Federal PKI Policy Authority
10
Occurring or soon to occur <7 days
5
Likely to occur 7-31 days
1
Early indicator >31 days
15
Entire FPKI community
10
One or more Federal agencies
5
Non-federal organizations
High ≥50
Medium ≥35 and <50
Low <35
Unknown

Figure 1: Security Event Impact Assessment Calculation

3.2.2.2.1 Event Type

All reported incidents are assigned an event type, allowing the FPKI Authorities to categorize each incident. Event categories include security, practice, and interoperability.

Table 1: Event Type

Event Type	Description	Example	Rating (r)
Security	A compromise, attack, or other event that impacts the confidentiality, integrity, or availability of associated FPKI services.	● CA system key compromise ● Denial of service attack on a public repository (e.g., CRL Distribution Point)	30

Event Type	Description	Example	Rating (r)
Practice	An operational practice that impacts the confidentiality, integrity, or availability of associated FPKI services.	● Failure to maintain multi-party control over CA signing key activation data ● Certificate mis-issuance (e.g., issuing a certificate without validating the identity or authority of the requestor)	15
Interoperability	An event that causes problems with data exchange or usage between members of the FPKI Community.	● Certificate or CRL profile misconfiguration (e.g., invalid Key Usage) ● Failure to publish necessary CA certificates in an Authority Information Access extension bundle to facilitate Path Discovery and Validation	10

3.2.2.2.2 Event Domain

The domain of the incident is an important factor in the incident management plan as it correlates to risk acceptance and liability for the U.S. Government.

Table 2: Event Domain

Event Domain	Description	Rating (r)
Federal entity certified by the Federal PKI Policy Authority	These CAs are operated by or on behalf of federal agencies (e.g., federal shared service provider CAs).	5
Non-Federal entity certified by the Federal PKI Policy Authority	These CAs are operated by and on behalf of commercial entities (e.g., commercial CAs).	1

3.2.2.2.3 Time to Impact

This factor is strictly a measure of how long it will take for an incident to affect the FPKI Community. For example, time frames are categorized as: Occurring or Soon to Occur (<7 days), Likely to Occur (7-31 Days), and Early Indicator (>31 Days).

Table 3: Time to Impact

Time to Impact	Example	Rating (r)
Occurring or Soon to Occur	Loss of critical infrastructure that impacts availability.	10

Time to Impact	Example	Rating (r)
Likely to Occur	Loss of Hardware Security Module activation data (e.g., operator cards) could prevent future signing operations if the module becomes deactivated.	5
Early Indicator	Offline Root CA hardware failure could prevent future signing operations	1

3.2.2.3 *IMPACTED COMMUNITY*

This factor concentrates on the type and number of stakeholders impacted by the incident. Identifying the impacted community will also aid in determining which stakeholders are necessary for subsequent communications.

Table 4: Impacted Community

Impacted Community	Example	Rating (r)
Entire FPKI Community	Federal Common Policy CA key compromise	15
One or more federal agencies, but not the entire FPKI Community	Successful denial of service attack on an issuing CA's CRL Distribution Point and /or OCSP services	10
Non-Federal Organizations	Non-Federal Root CA signing or status services unavailable	5

3.2.2.3.1 TOTAL IMPACT RATING

Determining a Total Impact Rating (R) is subjective and dependent on expert analysis and judgment. The calculations and factors described in Figure 1 can be used in this analysis. Specifically, the Rating is the sum of the ratings (r) for each of the event type, event domain, impacted community, and time to impact factors. However, this analysis should only be used as a guide.

In analyzing the potential impacts, the potential direct and indirect results of the incident must be considered, including the possibility that there will be additional instances of the incident. Table 5 provides meaning to each of the impact ratings[2]. Table 5 also includes criteria for each Total Impact Rating, in support of the four impact ratings.

When a Total Impact Rating is determined, the FPKIPA Co-chairs will determine whether it is necessary to communicate the information and to whom.

[2] It contains some relative terms, like "severe," "serious," and "limited," whose meaning will depend on context. The FPKI Authorities must consider the context and the nature of the incident impacts, to decide the relative significance.

Table 5: Total Impact Ratings

Impact Ratings	
Criteria	**Total Impact Rating**
The incident has significant potential of a severe effect on the Federal Government's security posture, operations, legal standing, or financial standing. A severe effect means the incident will likely: 1. Present threats to invalidate the FPKI's confidentiality, integrity, non-repudiation, or authentication services; 2. Cause a severe degradation in or loss of mission capability to an extent and duration that the FPKI is not able to perform one or more of its primary functions; 3. Result in major legal liability; or 4. Result in major financial loss.	High (R ≥50)
The incident could have a serious adverse effect on the FPKI Community's security posture, operations, legal standing, or financial standing. A serious adverse effect means the incident will likely: 1. Present significant threats to the level of confidentiality, integrity, non-repudiation, or authentication services provided by the FPKI; 2. Cause a significant degradation in mission capability to an extent and duration that the FPKI is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 3. Result in significant legal liability; or 4. Result in significant financial loss.	Medium (R ≥35 and R <50)
The incident could have a limited adverse effect on the FPKI Community's security posture, operations, legal standing, or financial standing. A limited adverse effect means the incident might: 1. Present minor threats to the level of confidentiality, integrity, non-repudiation, or authentication services provided by the FPKI; 2. Cause a degradation in mission capability to an extent and duration that the FPKI is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 3. Result in minor legal liability; or 4. Result in minor financial loss.	Low (R <35)
At least one impact criteria element is unknown and the Total Impact Rating cannot be defined.	Unknown

While Figure 1 analysis can be used to determine the Total Impact Rating, the FPKI Authorities have the ability to make a Rating determination based on criteria described in Table 5.

3.2.2.4 REMEDIATION RECOMMENDATIONS AND ACTION PLAN

The FPKI Authorities will develop high-level remediation recommendations based on the security event investigation and impact assessment. This effort will culminate with a Remediation Action Plan that will be included as part of the completed Security Event Report.

The Remediation Action Plan is intended to stop an incident from causing future negative impacts on the FPKI Community. Depending on the incident's root cause and impact assessment, immediate action may be warranted to eliminate the effects of the incident and restore the service to proper operating status.

Table 6 correlates Total Impact Rating to example remediation actions. These potential actions are subjective and may be employed at the discretion of the FPKI Authorities to best ensure the overall security and trust in the FPKI:

Table 6: Total Impact Rating and Example Remediation Actions

Total Impact Rating	Example Remediation Action
High	● Revocation of the associated cross certificate(s) ● Termination of a commercial shared service provider's FISMA Authority to Operate ● Share guidance to the FPKI Community to ensure that a compromised CA's certificate has been removed from trusted root stores and repositories and added to untrusted certificate stores, where applicable. ● Share recommendation that all end-entity certs should also be revoked by the affiliate and CRLs be updated.
Medium	● For a security event, potential revocation of a cross certificate based on the discretion of governing bodies and associated stakeholders ● For a practice or interoperability event, notification issued with remediation deadline ○ Notification/consultation with shared service provider customer agencies, if warranted ○ Brief/final determination by FPKIPA Note: Remediation timelines for practice and interoperability events will be shorter in duration than policy events
Low	● For a practice or interoperability event, notification issued with remediation deadline ○ Notification/consultation with shared service provider customer agencies, if warranted ○ Brief/final determination by FPKIPA Note: Though example remediation actions are the same as some "medium" events, remediation timelines for "low" events will be longer in duration due to a lower total impact to the FPKI Community.
Unknown	● At the discretion of the FPKI Authorities

The Remediation Action Plan will include a resolution and response due date, within the timeframe detailed in the corresponding impact rating. Once complete, the Remediation Action Plan is presented to the FPKIPA Co-chairs for approval.

The FPKI Authorities will evaluate each incident individually and determine whether to approve the current remediation plan or modify it consistent with policy. The FPKIPA Co-chairs will determine whether the Remediation Action Plan requires approval from other FPKIPA federal agency stakeholders. Any remediation plan associated with incidents affecting the federal community and a medium or high Total Impact Rating may require communication to the voting members of the FPKIPA for additional comment. Depending on the feedback from the FPKIPA members and the incident urgency, the FPKIPA Co-chairs may choose to hold an FPKIPA vote on the approval of the Remediation Action Plan.

3.2.2.5 NOTIFY THE FPKI COMMUNITY

The FPKI Authorities will inform the FPKI Community of an incident and its potential impact within 24 hours of developing remediation recommendations, as appropriate.

3.3 Phase 3: Resolution

The FPKIMA, the affected FPKI affiliates, and others that may be described in the Remediation Action Plan may be responsible for executing the approved Remediation Action Plan, in accordance with their change management procedures.

3.3.1 RESOLUTION COMMUNICATION

All action(s) recommended and approved as part of a Remediation Action Plan shall be implemented by the applicable FPKI affiliate(s) in accordance with documented policies, practices, and procedures. The results of these actions shall be analyzed, and a determination made as to whether the remediation has resolved the incident, or if further action is required. This determination will be made by the FPKI Authorities with the cooperation of the FPKI affiliate.

The FPKI affiliate shall communicate the status of implementing the Remediation Action Plan to the FPKI Authorities on a daily basis or as otherwise indicated.

3.3.2 RESOLUTION TRACKING

The FPKIPA will track the progress and status of the remediation action(s) and ensure adherence to the implementation timeline. If a remediation action is not implemented within the designated time frame, the FPKIPA may choose to approve an extension or reassess the incident and approve an alternative remediation plan. For example, if a CA vulnerability is not resolved within the designated time frame, the FPKIPA may extend the date for remediation or choose to revoke a certificate issued to that CA. The FPKI Authorities will communicate remediation progress information it deems appropriate to the FPKI Community within 24 hours of Remediation Action Plan completion or earlier depending on the impact assessment factors.

3.4 Phase 4: Post-Resolution Activity

The FPKIMA is responsible for finalizing the Security Event Report within 24 hours of incident resolution. The report tracks the incident from detection through resolution and becomes a data source for knowledge management in support of future incident management investigations.

Prior to closing out the incident management process, the following actions shall be considered:

- Update the operating policies, as appropriate.
- Submit a lesson learned report including after-action documentation to the appropriate authoritative body, if applicable.
- Implement contingency actions identified during the Incident Investigation phase.
- Share previously unknown problems or effects with appropriate parties per the guidance established by this document.
- Share new best practices with appropriate parties per the guidance established by this document.

The responsible FPKI affiliate will work with the FPKIMA to finalize the Security Event Report and follow FPKIMA guidance related to the Report.

In cases of a CA compromise, the FPKIPA, after receiving notices from the applicable FPKI affiliate, may post the notices to idmanagement.gov and provide an announcement to all federal agencies and affiliates.

APPENDIX A: SECURITY EVENT REPORT

1) Contact information of incident reporter [Affiliate]:
2) Discovery source [Affiliate]: (identify your organization as the reporting organization, and identify any other sources that you relied on in gaining knowledge of the incident)
3) Date and time of reporting [Affiliate]:
4) Event as it was reported [Affiliate]: (include emails or other notification method)
5) Detailed incident description [Affiliate]:
   a. Date/time of discovery:
   b. Who detected the incident and how was it detected?
   c. Cause of incident:
   d. Physical location of the incident, if applicable:
   e. Current status of incident:
   f. Description of affected resource: (Which PKI components were affected? Include CA names, serial numbers, validation paths to the Federal PKI, and certificate samples, if necessary.)
   g. Additional mitigating factors (e.g., encryption used on lost materials):
   h. Response actions performed (e.g., isolation of networked components):
   i. Other organizations contacted (e.g., US-CERT):
   j. Reporting party and/or CAs interpretation of the incident:
   k. Partial or complete list of all certificates that were either mis-issued or not compliant as a result of the incident:
      - All certificates issued after a given date from a CA or specific RA
      - List the date and identity of mis-issued or non-compliant component
   l. Timeline of events:
6) Security Event Impact Assessment [FPKI Authorities]:
   a. Event type:
   b. Event location:
   c. Time to occurrence:
   d. Impacted community:
   e. Total Impact Rating:
7) Response lead [FPKI Authorities]:
8) Remediation recommendations [FPKI Authorities]:
9) Remediation Action Plan [FPKI Authorities]:
   a. Required remediation actions:
   b. Implementation timeline:
   c. Resolution and response due date:
10) Resolution timeline [FPKI Authorities]:

APPENDIX B: REFERENCES

BRIDGE X.509 Certificate Policy for the Federal Bridge Certificate Authority (FBCA)
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-fbca.pdf

COMMON X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-common.pdf

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

SP 800-61 Computer Security Incident Handling Guide
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

APPENDIX C: GLOSSARY

Term	Definition
Analysis	The examination of acquired data for its significance and probative value to the case.
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
Availability	Ensuring timely and reliable access to and use of information.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Federal Public Key Infrastructure (FPKI)	The FPKI facilitates secure (trusted) physical and logical access, document sharing, and communications across federal agencies, and between federal agencies and outside bodies such as universities, state and local governments, commercial entities, and other communities of interest. To provide trust services, the FPKI uses a set of digital certificate standards, processes, and a mission-critical Trust Infrastructure to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. It uses a security technique called Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure technical non-repudiation and confidentiality.
FPKI Community	The FPKI Community is comprised of government and commercial organizations, which enable trust for interoperable person entity, or non-person-entity (NPE) identity authentication.
Federal Public Key Infrastructure Management Authority (FPKIMA)	The Federal Public Key Infrastructure Management Authority is the organization responsible for operating the Federal Common Policy Certification Authority.

Term	Definition
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Management	Process for handling any event that may negatively impact the FPKI Community and/or relying parties, and therefore requires immediate attention and resolution (i.e., incident management).
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Remediation Action Plan	Plan detailing the required remediation actions and an implementation timeline based on the incident's urgency level. This plan becomes part of the Security Event Report.
Security Event Report	Documentary record that tracks an incident from discovery through resolution.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.