FBCA Certificate Policy Change Proposal Number: 2007-01

To: Federal PKI Policy Authority

From: Certificate Policy Working Group

Subject: Proposed modifications to the Federal Bridge Certificate Policy

Date: December 7, 2006

Title: Harmonization between Federal Bridge and Common Policy Framework

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Federal Bridge Certificate Policy Version 2.2, September 28, 2006.

Change Advocate's Contact Information:

Name: Judith Spencer
Organization: GSA
Telephone number: 202-208-6576
E-mail address: judith.spencer@gsa.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: The Federal PKI Policy Authority has recognized the requirement that the policies of the Federal Bridge and the Common Policy Framework be harmonized to ensure consistency across the Federal PKI, particularly in light of HSPD-12 and FIPS 201. The changes incorporated in this change proposal satisfy the need to harmonize the policies.

Background: Federal Agency legacy PKIs may continue to operate within the HSPD-12 framework through their relationship with the FBCA. However, it is important that the FBCA and Common Policy be harmonized to protect the security integrity of the Federal PKI as a whole. A line-by-line comparison was conducted between the FBCA Policy and the proposed reformatted Common Policy. From this comparison several areas for improvement were identified in the Federal Bridge Policy.

Issue

The Certificate Policies of the Federal PKI are evolutionary documents that will continue to grow and change as new understanding and insight is gained by the federal sector. The Federal Bridge CA was revised and reformatted over a year ago. A similar exercise on the Common Policy has yielded additional language changes not present in the current Federal Bridge Policy. This change will rectify this situation and bring the policies into closer harmony with each other.

Specific Changes:

Specific changes are made to the following sections:

2.3	4.1.2	4.4	4.5.1	4.6	4.7	4.9.5	4.9.6	4.9.7
4.9.8	4.9.11	4.9.12	4.12.1	5.1	5.1.2.3 (new)		5.1.4	5.1.6
5.1.7	5.4.8	5.5.1	5.5.3	5.7.2	6.1.1.1	6.1.1.2	6.1.5	6.2.4.1
6.2.4.2	6.2.4.3(new)		6.2.6	6.2.7	6.2.9	6.5.1	6.7	7.1.7
7.3	9.4.2	9.7	9.10.3	9.11	9.12.2	9.15	11	12

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

2.3 FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly available within ~~one week~~ thirty days of approval.

4.1.2 Enrollment Process and Responsibilities

Entities applying for cross-certification are responsible for providing accurate information on their certificate applications. Upon issuance, each certificate issued by the FBCA shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the Entity.

~~For Entity CAs, this CP makes no stipulations regarding enrollment process and responsibilities.~~

For Entity CAs, all communications among PKI authorities supporting the certificate application and issuance process shall be authenticated and protected from modification.

4.4 CERTIFICATE ACCEPTANCE

Before a subscriber can make effective use of its private key, a PKI Authority shall convey to the subscriber its responsibilities as defined in Section 9.6.3.

4.5.1 Subscriber Private Key and Certificate Usage

For High, Medium Hardware, Medium, and Basic Assurance, subscribers shall protect their private keys from access by other parties. For Rudimentary assurance, no stipulation

Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs.

After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required in Section 3.3.1.

After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.9.5 Time within which CA must Process the Revocation Request

The FBCA and Entity CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published.

~~For the FBCA, all revocation requests must be processed within six hours of receipt of request.~~
~~For Entity CAs, revocation request processing time shall be as specified below:~~

~~**Assurance Level**~~	~~**Processing Time for Revocation Requests**~~
~~Rudimentary~~	~~No Stipulation~~
~~Basic~~	~~Within 24 hours of receipt of request~~
~~Medium (all policies)~~	~~Within 18 hours of receipt of request~~
~~High~~	~~Within six hours of receipt of request~~

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation

Practice Note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

For this CP, CRL issuance encompasses both CRL generation and publication.

For the FBCA, the interval between CRLs shall not exceed 24 hours. ~~In the case of revocation of a certificate, the FBCA shall issue an emergency CRL within six hours.~~

For Entity CAs, see the table below for issuing frequency of routine ~~and emergency~~ CRLs. ~~For Basic, Medium, Medium Hardware, and High, Emergency CRLs shall be issued whenever a CA certificate is revoked, or any certificate is revoked because of key compromise.~~ CRLs may be issued more frequently than specified below.

Table 1 Entity CA CRL issuance Frequency

Assurance Level	Maximum Interval for Routine CRL Issuance	~~Maximum Interval for Emergency CRL Issuance~~
Rudimentary	No Stipulation	~~No stipulation~~
Basic	24 hours	~~24 hours after notification~~
Medium (all policies)	24 hours	~~18 hours after notification~~
High	24 hours	~~Six hours after notification~~

For Entity Principal CAs that are operated in an off-line manner, ~~only issue CA certificates and~~ routine CRLs may be issued less frequently than specified above if the CA ~~are operated in an off-line manner~~ only issues:

- CA certificates
- (optionally) CSS certificates, and
- (optionally) end user certificates solely for the administration of the principal CA.

~~, routine CRLs may be issued less frequently than specified above.~~ However, the interval between routine CRL issuance shall not exceed 31 days. Such CAs must meet the requirements specified ~~above~~ in section 4.9.12 for issuing Emergency CRLs. (Note: such CAs will also be required to notify the FPKI Operational Authority upon Emergency CRL issuance. This requirement will be included in the MOA between the FPKIPA and the Entity.)

4.9.8 Maximum Latency of CRLs

~~No stipulation. (See Section 4.9.7)~~ CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.11 Other Forms of Revocation Advertisements Available

~~Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.~~

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS.

- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

In the event of an Entity Principal CA private key compromise or loss, the cross-certificate shall be revoked and a CRL shall be published at the earliest feasible time by the FPKI Operational Authority.

For Entity CAs, ~~no stipulation.~~ when a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued as specified below:

Assurance Level	**Maximum Latency for Emergency CRL Issuance**
Rudimentary	No stipulation
Basic	24 hours after notification
Medium (all policies)	18 hours after notification
High	Six hours after notification

4.12.1 Key Escrow and Recovery Policy and Practices

~~For the FBCA, no stipulation.~~

~~Entity CAs that support key recovery shall identify the document describing the key recovery policy in the applicable CP.~~

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. CAs that support private key escrow for key management keys shall document their key recovery practices.

Practice Note: Escrowed keys must be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

Under no circumstances will a subscriber signature key be held in trust by a third party.

5.1 PHYSICAL CONTROLS

All CA equipment including CA cryptographic modules shall be protected from unauthorized access at all times.

~~The FBCA and Entity CAs shall impose physical security requirements that provide similar levels of protection as those specified below.~~ All the physical control requirements specified below apply equally to the FBCA and Entity CAs.

NEW SECTION:

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.4 Water Exposures

~~No stipulation~~

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.6 Media Storage

FBCA and Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Sensitive FBCA and Entity CA media shall be stored so as to protect it from unauthorized physical access.

5.1.7 Waste Disposal

~~Sensitive waste material shall be disposed of in a secure fashion.~~ Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.4.8 Vulnerability Assessments

FBCA personnel shall routinely assess whether the CA system or its components have been attacked or breached.

For Entity CAs, personnel shall perform routine assessments for evidence of malicious activity.

Practice Note: The security audit data should be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors should check for continuity of the security audit data.

5.5.1 Types of Events Archived

FBCA or Entity CA archive records shall be sufficiently detailed to establish the proper operation of the FBCA or Entity CA, or the validity of any certificate (including those revoked or expired) issued by the FBCA or Entity CA.

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

Data To Be Archived	Rudimentary	Basic	Medium	High
CA accreditation (if applicable)	**X**	**X**	**X**	**X**
Certificate Policy	**X**	**X**	**X**	**X**
Certification Practice Statement	**X**	**X**	**X**	**X**
Contractual obligations	**X**	**X**	**X**	**X**
Other agreements concerning operations of the CA	**X**	**X**	**X**	**X**
System and equipment configuration	**X**	**X**	**X**	**X**
Modifications and updates to system or configuration	**X**	**X**	**X**	**X**
Certificate requests	**X**	**X**	**X**	**X**
Revocation requests		**X**	**X**	**X**
Subscriber identity Authentication data as per Section 3.~~1.9~~2.3		**X**	**X**	**X**
Documentation of receipt and acceptance of certificates (if applicable)		**X**	**X**	**X**
Subscriber Agreements		**X**	**X**	**X**
Documentation of receipt of tokens		**X**	**X**	**X**
All certificates issued or published	**X**	**X**	**X**	**X**
Record of CA Re-key	**X**	**X**	**X**	**X**
All CRLs issued and/or published		**X**	**X**	**X**
All Audit Logs	**X**	**X**	**X**	**X**
Other data or applications to verify archive contents		**X**	**X**	**X**
Documentation required by compliance auditors		**X**	**X**	**X**

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. For the FBCA, archived records may be moved to another medium when authorized by the FPKI Operational Authority Administrator. The contents of the archive shall not be released except in accordance with Sections 9.3 & 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the FBCA or Entity CA itself.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, an Entity may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA).

Prior to the end of the archive retention period, the FPKI Operational Authority shall provide archived data and the applications necessary to read the archives to a Federal PKI Policy Authority approved archival facility, which shall retain the applications necessary to read this archived data.

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 1.
- 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.

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information by the FBCA shall be generated in FIPS 140 validated cryptographic modules. Cryptographic keying material used to sign certificates, CRLs or status information by Entity CAs shall be generated in FIPS 140 validated cryptographic modules or modules validated under equivalent international standards.

For the FBCA, the modules shall meet or exceed Security Level 3. For Entity CAs, the modules shall meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Basic, Medium, or Medium Hardware), or Security Level 3 (for High). Multiparty control is required for CA key pair generation for the FBCA and for Entity CAs operating at the Medium, Medium Hardware, or High levels of assurance, as specified in Section 5.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

For High, Medium Hardware, and Medium Assurance, ~~the process shall be validated by~~ an independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation shall be performed using a FIPS approved method or equivalent international standard.

At the High and Medium Hardware assurance levels, subscriber key generation shall ~~must~~ be performed using a validated hardware cryptographic module. For ~~all other~~ Medium and Basic assurance ~~levels~~, either validated software or validated hardware cryptographic modules shall ~~may~~ be used for key generation.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire after 12/31/~~08~~10 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 12/31/08 and expire after 12/31/2010 shall be generated using, at a minimum, SHA-224.

Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates that expire before ~~12/31/08~~ 12/31/10 shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. End-entity certificates that expire on or after ~~12/31/08~~ 12/31/10 shall contain public keys that are at least 2048 bit for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through ~~12/31/08~~ 12/31/10. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after ~~12/31/08~~ 12/31/10.

6.2.4.1 Backup of FBCA & Entity CA Private Signature Key

FBCA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.

Backup of Entity CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, Entity CA private signature keys shall be backed up under multi-person control.

~~No more than a single copy of the signature key shall be stored at the FBCA or Entity CA location. Additional copies may exist off-site provided that accountability for them is maintained.~~ At least one copy of the FBCA or Entity CA private signature key shall be stored off site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

6.2.4.2 Backup of subscriber private signature key

At the Medium Hardware and High assurance levels, Subscriber private signature keys may not be backed up or copied.

At the Rudimentary, Basic, or Medium levels of assurance, Subscriber private signature keys may be backed up or copied, but must be held in the Subscriber's control.

Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

NEW SECTION

6.2.4.3. Back up of Subscriber Key Management Private Keys

Backed up subscriber private key management keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.6 Private Key Transfer into or from a Cryptographic Module

FBCA and Entity CA private keys ~~shall be generated by and remain in a cryptographic module. The CA private keys may be backed up in accordance with Section 6.2.4.1.~~ may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1. At no time shall the CA private key exist in plain text outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

~~For subscriber private keys, no stipulation.~~

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS-140.

6.2.9 Methods of Deactivating Private Keys

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. CA Hardware cryptographic modules shall be removed and stored in a secure container when not in use. ~~If cryptographic modules are used to store subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access.~~

6.5.1 Specific Computer Security Technical Requirements

For the FBCA, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The FBCA and its ancillary parts shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to FBCA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use or require separation for FBCA random access memory
- Require use of cryptography for session communication and database security
- Archive FBCA history and audit data
- Require self-test security related FBCA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the FBCA system
- Enforce domain integrity boundaries for security critical processes

For Entity CAs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Entity CA and its ancillary parts shall include the following functionality:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For Certificate Status Servers, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

6.7 NETWORK SECURITY CONTROLS

Network security controls shall be employed to protect the FBCA and the FBCA Internal Directory. Networking equipment shall turn off unused network ports and services. Any network software installed on the FBCA equipment shall be necessary to the functioning of the FBCA.

The FBCA Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup).

Any boundary control devices used to protect the Border directory or FBCA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

Entity CAs, ~~and~~ directories, and certificate status servers shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

7.1.7 Usage of Policy Constraints Extension

~~No stipulation~~. The CAs may assert policy constraints in CA certificates.

7.3 OCSP PROFILE

~~No stipulation.~~ If implemented, Certificate Status Servers (CSS) shall sign responses using algorithms designated for CRL signing.

9.4.2 Information treated as Private

The FBCA shall protect all subscriber personally identifying information from unauthorized disclosure. The FBCA shall also protect personally identifying information for Entity personnel collected to support cross-certification and MOA requirements from unauthorized disclosure. The contents of the archives maintained by the FPKI OA shall not be released except as required by law.

For Entity CAs, no stipulation.

9.7 DISCLAIMERS OF WARRANTIES

~~No stipulation~~. The FPKI OA may not disclaim any responsibilities described in this CP.

9.10.3 Effect of Termination and Survival

~~None~~. The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

~~None.~~ The Federal PKI PA shall establish appropriate procedures for communications with Entity CAs via contracts or memoranda of agreement as applicable.

For all other communications, no stipulation.

9.12.2 Notification Mechanism and Period

Proposed changes to this CP shall be distributed electronically to Policy Authority members and observers in accordance with the Charter and By-laws. ~~This CP and any subsequent changes shall be made publicly available~~ .

9.15 COMPLIANCE WITH APPLICABLE LAW

~~No stipulation~~. The FBCA and Entity CAs are required to comply with applicable law.

11. ACRONYMS & ABBREVIATIONS

NSA	National Security ~~Entity~~ Agency

12. GLOSSARY

~~Employee~~	~~Any person employed by an Entity as defined above.~~
Entity	~~Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.~~ For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, or government agency with operational control of a CA.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.

Estimated Cost:
No cost.

Implementation Date:
This change will be implemented immediately upon approval by the FPKIPA and incorporation into the FBCA CP.

Prerequisites for Adoption:
There are no prerequisites.

Plan to Meet Prerequisites:
There are no prerequisites.

Approval and Coordination Dates:
Date presented to CPWG: December 7, 2006
Date Presented to FPKI PA: December 12, 2006
Date of approval by FPKI PA: March 9, 2007