The Slandala Company
203 North Lee Street
Falls Church, Virginia, 22046
703 851 6813
jimmy.jung@slandala.com

28 February 2012

Darlene K. Gore
Federal PKI Management Authority
PKI Program Manager
Security Services Division

Subject: Federal PKI Auditor Letter of Compliance

Attached please find the results of the Compliance Audit for the Legacy Federal Public Key Infrastructure (FPKI) Systems. This audit was performed to evaluate the operations of the FPKI systems for conformance to the following Federal PKI Practices and Policies: e security practices and procedures described the following Federal PKI Practices and Policies:

- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.25, dated December 13, 2011
- X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.16, dated September 23, 2011
- X.509 Certificate Policy For The E-Governance Certification Authorities, Version 2.0, dated September 9, 2011
- United States Federal PKI X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI) Trust Infrastructure Federal Bridge Certification Authority (FBCA), Federal Common Policy Certification Authority (FCPCA), SHA-1 Federal Root Certification Authority (SHA1 FRCA), Version 4.0, dated 28 November 2011
- United States Federal PKI X.509 Certification Practice Statement – X.509 Certification Practice Statement (CPS) For The E-Governance Certification Authorities (EGCA), Version 4.0, dated 28 November 2011

The compliance audit evaluated the Federal PKI systems. The compliance audit was performed via interviews, documentation reviews and site visits performed during January of 2012. The Federal PKI includes CAs issuing certificates under the following names:

- CN = eGovernance App CA, OU = FPKI, O = U.S. Government, C = US
- CN = eGovernance CSP2 CA, OU = FPKI, O = U.S. Government, C = US
- CN = eGovernance Trust Services CA, OU = FPKI, O = U.S. Government, C = US
- CN = Federal Bridge CA, OU = FPKI, O = U.S. Government, C = US
- CN = Federal Common Policy CA, OU = FPKI, O = U.S. Government, C = US
- CN = SHA-1 Federal Root CA, OU = FPKI, O = U.S. Government, C = US

The audit was performed by Mr. James Jung of The Slandala Company. Mr. Jung has performed audits of PKI systems for more than 9 years and has 27 years of experience in the design, implementation and certification of information assurance systems. He is certified by the International Information Systems Security Certification Consortium (ISC)^2 as Certified Information Systems Security Professionals (CISSP) and is certified by the Information Systems Audit and Control Association (ISACA) as Certified Information Systems Auditors (CISA). He has designed, installed or operated PKI systems for the Department of State, the Department of Energy, the Department of Treasury, the Federal Bureau of

Investigation, the Department of Homeland Security, the United States Patent and Trademark Office (USPTO) and other agencies and commercial companies. He has provided PKI audit and compliance support for the Department of State, the Department of Labor, the Department of Commerce (DoC) and has been the lead auditor for the Department of Defense Certification Authorities and auditor of several of the DoD agency Registration Authorities, Local Registration Authorities and External Certificate Authorities. Mr. Jung has not held an operational role or a trusted role on the Federal PKI systems, nor has he had any responsibility for writing the Federal PKI Certificate Practices Statements. Mr. Jung and The Slandala Company are independent of the Federal PKI Management Authority and the operations and management of the Federal PKI.

The Audit was performed by first performing a direct CP-to-CPS traceability analysis comparing the United States Federal PKI X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI) Trust Infrastructure Federal Bridge Certification Authority (FBCA), Federal Common Policy Certification Authority (FCPCA), SHA-1 Federal Root Certification Authority (SHA1 FRCA), 28 November 2011, dated Version 4.0 to the following CPs:

- The X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.25, dated December 13, 2011
- X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.16, dated September 23, 2011

Seventeen (17) items were found to not comply or address the requirements of the applicable policies.

A direct CP-to-CPS traceability analysis was performed, comparing the United States Federal PKI X.509 Certification Practice Statement – X.509 Certification Practice Statement (CPS) For the E-Governance Certification Authorities (EGCA), Version 4.0, dated 28 November 2011 to the:

- X.509 Certificate Policy For The E-Governance Certification Authorities, Version 2.0, dated September 9, 2011

Sixteen (16) items were found to not comply or address the requirements of the applicable policies.

The operations of the Federal PKI systems were evaluated for conformance to the FPKI responsibilities identified in the MOA established between the Federal PKI Policy Authority and other Entities for Cross-Certifying. Several of these were very old and could be updated. The Federal PKI operates in compliance with these MOAs.

The Federal PKI audit was performed using a requirements decomposition methodology. The two CPSs were reviewed and decomposed into requirements, and the requirements were then evaluated to determine the general methodology for their evaluation and the activities that should be taken by the auditor to fulfill the audit of that requirement. Findings and data are recorded during these activities, and are categorized as follows:

- Complies – operations comply with the practices documented in the CPSs,
- Does Not Comply – operations do not comply with the practices documented in the CPSs,
- Recommendation (Complies) - operations comply with the practices documented in the CPSs; however, other "best practices" could be considered.

The Federal PKI Architecture Certification Practice Statements were decomposed into 336 requirements for which the following results apply:

- 10 requirements were found to not comply

  an additional

- 36 requirements complied, but a recommendation is made regarding potential improvements to the implementation or the policy and practices documentation.

Details of these findings are given in the Compliance Audit Report.

The following documentation was reviewed as part of the Compliance Audit:

- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.25, dated December 13, 2011
- X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.16, dated September 23, 2011
- X.509 Certificate Policy For The E-Governance Certification Authorities, Version 2.0, dated September 9, 2011
- United States Federal PKI X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI) Trust Infrastructure Federal Bridge Certification Authority (FBCA), Federal Common Policy Certification Authority (FCPCA), SHA-1 Federal Root Certification Authority (SHA1 FRCA), Version 4.0, dated 28 November 2011
- United States Federal PKI X.509 Certification Practice Statement – X.509 Certification Practice Statement (CPS) For The E-Governance Certification Authorities (EGCA), Version 4.0, dated 28 November 2011

No failures were found that suggested that the system had been operated in an overtly insecure manner. It is the lead auditor's opinion that the GSA FPKI provided reasonable security control practices. The discrepancies with the stated CPS practices are identified in this report. A Plan of Actions and Milestones (POA&M) was provided to address the identified discrepancies. However, two of the discrepancies could not be addressed. The FPKI Policy Authority allowed the issuance of two (2) SHA-1 certificates from the legacy Common Policy at SHA-1 after 12/31/2010. This action was performed in support of a transition in algorithms and to support interoperability. The following discrepancies resulted:

- The Key Size requirements of the CPS state that, "All FBCA and FCPCA certificates are issued by a UniCert CA, which signs certificates and CRLs using SHA-256. "

- The CPS Approval procedures in the applicable policies state that "The FPKI PA will not issue waivers."

2/27/2012

X

James Walker Jung
Lead Auditor
Signed by: Jung.James.W.ORC1000023399.ID