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

2 October 2020

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

Subject: 2020 Federal PKI Auditor Letter of Compliance

A compliance audit of the General Services Administration (GSA) Federal Public Key Infrastructure (FPKI) was conducted to verify that the FPKI was being operated in accordance with the security practices and procedures described by the following Federal PKI Practices and Policies:

- 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), Version 5.1, 05 May 2020,
- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, Version 1.32 April 14, 2020.

General Services Administration (GSA) Federal Public Key Infrastructure (FPKI) operates three Certification Authorities (CAs):

- CN = Federal Common Policy CA, OU = FPKI, O = U.S. Government, C = US
  - Subject Key Identifier: ad0c7a755ce5f398c479980eac28fd97f4e702fc
- CN = Federal Bridge CA 2016, OU = FPKI, O = U.S. Government, C = US
  - Subject Key Identifier: 23b0b37d1654d4025676eb3abea96b2f437b2816
- CN = Federal Bridge CA G4, OU = FPKI, O = U.S. Government, C = US
  - Subject Key Identifier: 79f00049eb7f77c25d410265348a90239b1e076f

The compliance audit evaluated the Federal PKI and evaluated the operations and management of the certificate authorities, repositories, and related security-relevant components. No subscriber registration authority functions are performed by the system. (The Federal PKI dies not operate Credential Status Services, Registration Authorities, Key Recovery or Card Management Systems.) The Federal PKI system has not changed significantly since the previous audit. The Federal PKI Policy Authority has established Memorandums of Agreement (MOAs) with the organizations with which they operate (typically via cross certification). The compliance audit evaluated their compliance with these MOAs. Findings from the previous year were reviewed.

This audit covers the following period.

- Audit Period Start: July 10, 2019
- Audit Period Finish: August 30, 2020

The audit was performed in August of 2020, at which time precautions to protect against the Covid-19 virus were in place. The report identifies with notes where methods used to evaluate the practice were modified as part of these precautions. In general:

- Interviews were conducted remotely.
- The assessment of the physical protections was based on interviews with both FPKI staff and data center staff, log reviews and documentation.
- System configuration assessments of the offline systems were based on screen captures rather than direct observation.

The Federal PKI audit was initiated by first performing a direct CP-to-CPS traceability analysis.

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), Version 5.1, 05 May 2020 was evaluated for conformance to the following CPs:

- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, Version 1.32 April 14, 2020

CPS practices found to not comply or address the requirements of the applicable policies, as part of the traceability analysis are categorized Disparate.

- Disparate – CPS practices found to not comply or address the requirements of the applicable policies.
- Recommendation – suggestions to improve the CPS description of practices could be considered.

The X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework is being extensively updated. Recommendations were made where the CPS might be improved based on draft versions of the updated policy.

The Federal PKI operational compliance audit was performed using a requirements decomposition methodology. The CPS was 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 CPS,
- Discrepancy – operations do not comply with the practices documented in the CPS,
- Noted – Methods used to evaluate the practice were modified as part of the precautions to protect against the Covid-19 virus
- Recommendation – operations comply with the practices documented in the CPS; however, improvements to the implementation could be considered.

The audit was performed by Mr. James Jung of The Slandala Company. Mr. Jung has performed audits of PKI systems since 2002 and has more than 35 years' 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 a Certified Information Systems Security Professional (CISSP) and is certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (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 Certification 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.

Information from the following documents was used as part of the compliance audit.

- 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), Version 5.1, 05 May 2020
- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, Version 1.32 April 14, 2020
- DRAFT X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, Version 2.0 1 September 2020
- GSA IT Security Procedural Guide: Media Protection CIO-IT Security -06-32, Revision 3, April 15, 2012
- Federal Public Key Infrastructure (FPKI) Trust Infrastructure Security Incident Response Plan V2.0.4, April 27, 2017
- FPKIMA Standard Operating Procedure (SOP) 025 Administrative tasks, v3.0 October 16, 2017
- FPKIMA Standard Operating Procedure (SOP) Records Archive Management, V3.4, November 6, 2017
- FPKIMA Standard Operating Procedure (SOP) 006 Gather Audit Logs V3.14, 03 August 2020
- FPKIMA Standard Operating Procedure (SOP) 007 Review System Audit Logs V4.2, 30 July 2020
- IT Security Procedural Guide: Media Protection (MP) CIO-IT Security-06-32, Revision 5 June 6, 2018
- FPKIMA SOP 011- Archive Management, V3.6, November 1, 2018
- IT Security Procedural Guide; Media Protection (MP) CIO-IT Security-06-32, revision 5, April 3, 2020
- Federal Public Key Infrastructure (FPKI) Trust Infrastructure Penetration Test Report October 1st, 2019, Version: 1
- Information System Contingency and Incident Response Plan Test Report Functional Test, April 2020
- Federal Public Key Infrastructure (FPKI) Trust Infrastructure Security Categorization: Moderate Information System Contingency Plan (ISCP) V2.3.1, May 2020
- Federal Public Key Infrastructure (FPKI) Trust Infrastructure Security Incident Response Plan V2.1.1, 22 May 2020
- U.S. General Services Administration Federal Public Key Infrastructure (PKI) Trust Infrastructure (FPKITI) FIPS 199 Moderate System Security Plan August 10, 2020

The operations of the Federal PKI systems were also evaluated for conformance to the FPKI responsibilities identified in the MOAs established between the Federal PKI Policy Authority and other Entities for Cross-Certifying. The Federal PKI operates in compliance with these MOAs.
A direct CP-to-CPS traceability analysis was performed, 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), Version 5.1, 05 May 2020 was evaluated for conformance to the following CPs:

- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, Version 1.32 April 14, 2020

The traceability analysis identified two (2) items that were disparate.

Federal Public Key Infrastructure (FPKI) operations of the following CAs were evaluated for conformance to 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), Version 5.1, 05 May 2020.

The evaluation of operational conformance to the CPS identified two (2) items that did not comply.

No failures were found that suggested that the system had been operated in an overtly insecure manner and it is the lead auditor's opinion that the GSA FPKI provided reasonable security control practices. An Action Plan was provided to address the identified discrepancies. Discrepancies with the stated CPS practices are identified in the report. The report identifies, as a discrepancy, a cross-certificate that does not meet the FPKI Certificate Profile. This deviation in the profile was requested by an Entity CA to support the operations of a specific application and directed by an approved Letter of Authorization (LOA) from the FPKI Policy Authority chair.

10/2/2020

X James Walker Jung DIGITALLY SIGNED The Slandala Company

Lead Auditor
Signed by: Jung.James.W.ORC3011018685.ID

Jung.James.W.ORC3011018685.ID

Digitally signed by Jung.James.W.ORC3011018685.ID
Date: 2020.10.02 15:59:02 -04'00'