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

30 August 2021

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

Subject: 2021 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), 28 June 2021, Version 6.0
- 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 2.1, May 18, 2021.

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

- CN = Federal Bridge CA G4, OU = FPKI, O = U.S. Government, C = US
  - Subject Key Identifier: 79f00049eb7f77c25d410265348a90239b1e076f
- CN = Federal Common Policy CA G2, OU = FPKI, O = U.S. Government, C = US
  - Subject Key Identifier: f4275ca9c37c47f4faa6a7b05997aadd352617e3
- CN = Federal Common Policy CA, OU = FPKI, O = U.S. Government, C = US
  - Subject Key Identifier: ad0c7a755ce5f398c479980eac28fd97f4e702fc

The Federal Common Policy Certificate Authority G2 CA was stood up on 14 October. The Federal Common Policy CA was decommissioned during the audit period. Beginning prior to the audit period, the Federal PKI has been transitioning to Redhat Certificate Services PKI and to an offline operation. This transition was completed with the decommissioning of the CN = Federal Common Policy CA. 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 does not operate Credential Status Services, Registration Authorities, Key Recovery or Card Management Systems.) 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: August 30, 2020
- Audit Period Finish: August 3, 2021

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), 28 June 2021, Version 6.0 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 2.1, May 18, 2021.

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 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,
- 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.

- 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), 28 June 2021, Version 6.0
- 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 2.1, May 18, 2021.
- FPKIMA Standard Operating Procedure (SOP) 006 Gather Audit Logs V3.2, 27 July 2021
- FPKIMA Standard Operating Procedure (SOP) 007 Review System Audit Logs V4.5, 30 July 2021
- FPKIMA Standard Operating Procedure (SOP) 054 Update CRLs Review System Audit Logs V4.5, 30 July 2021
- 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), 28 June 2021, Version 6.0 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 2.1, May 18, 2021.

The traceability analysis identified one item that was disparate.

Federal Public Key Infrastructure (FPKI) operations of the following CAs were evaluated for conformance to the following:

- 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), 28 June 2021, Version 6.0
- The X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019
- The X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, Version 2.1, May 18, 2021

The evaluation of operational conformance to the CPS identified one item that did not comply. Two additional items did not comply, but were corrected during the audit. Evidence for their correction was reviewed and they were identified as mitigated.

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. Discrepancies with the stated CPS practices are identified in the report. It is the lead auditor's opinion that the GSA FPKI is in compliance with the applicable policies and practice statements.

8/30/2021

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: 2021.08.30 16:25:58 -04'00'