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

14 August 2024

India Donald
Program Manager Federal PKI Management Authority
Identity, Credential, and Access Management (ICAM) Division

Subject: 2024 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), 2 November 2023, Version 6.4
- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), May 8, 2024, Version 3.5
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, May 8, 2024, Version 2.8.

General Services Administration (GSA) Federal Public Key Infrastructure (FPKI) operates two 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

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 and had been corrected.

This audit covers the following period.

- Audit Period Start: August 22, 2023
- Audit Period Finish: 1 August 2024

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) was evaluated for conformance to the applicable certificate policies. 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 40 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), 2 November 2023, Version 6.4
- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), May 8, 2024, Version 3.5
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, May 8, 2024, Version 2.8
- 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
- U.S. General Services Administration Federal Public Key Infrastructure (FPKI) Incident Response Plan and Contingency Plan Functional Test Report March 29, 2024
- U.S. General Services Administration Federal Public Key Trust Infrastructure (FPKI) Configuration Management Plan June 6, 2024 v2.15
- U.S. General Services Administration Federal Public Key Infrastructure (FPKI) Trust Infrastructure Information System Contingency Plan (ISCP) (FIPS 199 Moderate) V2.3.6 March 29, 2024
- Federal PKI Trusted Infrastructure Change Request Form Tracking Number: FY2024-3
- FPKIMA Operations Trusted Role List, February 20, 2024
- Decision for a Standard Assessment & Authorization for Federal Public Key Infrastructure (FPKI) SYSTEM TYPE: Contractor System DATE: March 15, 2024
- U.S. General Services Administration Incident Response (IR) Plan Federal Public Key Infrastructure (FPKI) Trust Infrastructure March 29, 2024 Version 2.2.1

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) was evaluated for conformance to the following CPs:

- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA),
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework.

The traceability analysis identified no items that were disparate.

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

- 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),
- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA),
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework.

The evaluation of operational conformance to the CPS did not identify any 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. No discrepancies were identified.

8/14/2024

X James Walker Jung DIGITALLY SIGNED The Slandala Company

James Walker Jung DIGITALLY SIGNED The Slandala Company 2024.08.14 08:19:09 -04'00'

James Jung
Lead Auditor
Signed by: Slandala

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