Subject: 2019 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:

- 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), 10 December 2018 Version 4.11,
- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019

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

  - Thumbprint: 90 5f 94 2f d9 f2 8f 67 9b 37 81 80 fd 4f 84 63 47 f6 45 c1
- CN = Federal Bridge CA 2016, OU = FPKI, O = U.S. Government, C = US
  - Thumbprint: 7c 6d 0d 47 11 d0 eb ab 46 a0 78 81 3a 04 74 6a 73 a8 b3 2b
- CN = SHA-1 Federal Root CA G2, OU = FPKI, O = U.S. Government, C = US
  - Thumbprint: bd bd ab 2a 1a 9f 27 6d ee 21 37 ca fe 59 da 6b 20 f3 e7 62

The compliance audit evaluated the Federal PKI system 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 system has not changed significantly since the previous audit. The Federal PKI system has established Memorandums or Agreement (MOAs) with the organizations with which they operate (typically via cross certification). The compliance audit evaluated their compliance with these MOAs.

The compliance audit was performed via interviews, documentation reviews and site visits performed during July 2019. This audit covers the following period.

- Audit Period Start: June 8, 2018
- Audit Period Finish: July 10, 2019
Audit site visits were performed at the primary and secondary sites in Northern Virginia. Findings from the previous year were reviewed.

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,
- Does Not Comply – 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 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), SHA-1 Federal Root Certification Authority (SHA1 FRCA), 1 August 2018, Version 4.10 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

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.

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 30 years’ experience in the design, implementation and certification of information assurance systems. He is certified by the International Information Systems Security Certification Consortium (ISC)³ 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), SHA-1 Federal Root Certification Authority (SHA1 FRCA), 10 December 2018 Version 4.11,
- DRAFT 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), Version 4.12,
- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.35, 15 April, 2019
- Memorandum - Decision for Standard Assessment & Authorization for Federal Public Key Infrastructure (FPKI), November 9, 2017
- Federal Public Key Infrastructure (FPKI) Trust Infrastructure Security Incident Response Plan V2.0.4, April 27, 2017
- Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, July 17, 2017
- Configuration Management Plan For The Federal Public Key Infrastructure (FPKI) Trust Infrastructure, V 2.0.1, August 16, 2018
- Federal Public Key Infrastructure (FPKI) Trust Infrastructure Security Categorization: Moderate Information System Contingency Plan V2.2, July 2018
- U.S. General Services Administration Federal Public Key Infrastructure (FPKI) Trust I Infrastructure System Security Plan Version 6.0.4, November 02, 2017
- Federal PKI Trust Infrastructure Monthly Statistical Reports
- 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 SOP 011- Archive Management, V3.6, November 1, 2018

The operations of the Federal PKI systems were also evaluated for conformance to the FPKI responsibilities identified in the MOA 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), SHA-1 Federal Root Certification Authority (SHA1 FRCA), 10 December 2018 Version 4.11, 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

The traceability analysis identified three (3) 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), SHA-1 Federal Root Certification Authority (SHA1 FRCA), 10 December 2018 Version 4.11:

The evaluation of operational conformance to the CPS identified one item 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. Discrepancies with the stated CPS practices are identified in the report. An Action Plan was provided to address the identified discrepancy.

8/29/2019

X Jung.James.W.ORC3010006689.ID

Lead Auditor
Signed by: Jung.James.W.ORC3010006689.ID

Digitally signed by Jung.James.W.ORC3010006689.ID
Date: 2019.08.29 13:35:57 -04'00'