

The Slandala Company
203 North Lee Street
Falls Church, Virginia 22046

28 August 2026

Paul Newton
Department of the State PKI Management Authority

The Slandala Company conducted a compliance audit of the Department of State Public Key Infrastructure (PKI) Certification Authorities to verify that the PKI was being operated in accordance with the security practices and procedures described by the following applicable policies and practice statements.

- Department of State (DoS) Public Key Infrastructure (PKI) X.509 Certificate Policy Version 3.0, April 2025
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.13 December 16, 2025
- Department of State (DoS) Public Key Infrastructure (PKI) X.509 Certification Practices Statement, Version 2.5, February 2025

The following Certification Authorities (CAs) were assessed in the audit:

- CN = U.S. Department of State AD Root CA, CN = AIA, CN = Public Key Services, CN = Services, CN = Configuration, DC = state, DC = sbu
- CN = U.S. Department of State AD High Assurance CA, CN = AIA, CN = Public Key Services, CN = Services, CN = Configuration, DC = state, DC = sbu
- OU = U.S. Department of State PIV CA2, OU = Certification Authorities, OU = PIV, OU = Department of State, O = U.S. Government, C = US
- OU = U.S. Department of State PIV CA3, OU = Certification Authorities, OU = PIV, OU = Department of State, O = U.S. Government, C = US
- CN = U.S.-Department-of-State-DPC-CA, DC = derived, DC = state, DC = sbu

The Compliance Audit evaluated the associated Certificate Authority, Directory, Card Management Systems (CMS) and OCSP server components. Registration Authority (RA) sites in Arlington, Va; Springfield, Va and Washington, D.C. were included. As part of the audit, the Memorandum of Agreement between the Federal Public Key Infrastructure (PKI) Policy Authority and the Department of State was reviewed. The Department of State is operating in accordance with this MOA. The compliance audit reviewed findings from the previous audit. Two findings; one related to suspended certificates and one related to the id-fpki-common-cardAuth certificate being asserted on non-PIV certificates were previously identified.

This audit covers the following period.

- Audit Period Start: September 2022
- Audit Period Finish: April 2026

The operational compliance audit was performed using a requirements decomposition methodology and was initiated by first performing a direct CP-to-CPS traceability analysis. CPS practices found to not comply or address the requirements of the applicable policies, as part of the traceability analysis are categorized as “Disparate.”

The CPS was then 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. The audit step activities are performed during the site visits and documentation reviews. Observations and recommendations are identified and may be included. 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 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); is certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA) and GIAC Security Essentials (GSEC) certified by the SANS Institute. 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. Since 2010, Mr. Jung has been performing the audit for the Federal PKI Trust Infrastructure, including the Federal Bridge and Common CAs.

Mr. Jung has not held an operational role or a trusted role on the Department of State PKI systems, nor has he had any responsibility for writing the practice statements. Mr. Jung and The Slandala Company are independent of the Department of State PKI operations and management.

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

- *Department of State (DoS) Public Key Infrastructure (PKI) X.509 DoS OpenNet Certificate Policy Version 3.0, April 2025*
- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.13, December 16, 2025*
- *Department of State (DoS) Public Key Infrastructure (PKI) X.509 DoS OpenNet Certification Practices Statement, Version 2.5 February 2025*

- *Memorandum of Agreement, between the United States Federal Public Key Infrastructure Policy Authority and United States Department of State, executed 2020*
- *Department of State Bureau Of Diplomatic Security Dos One Badge PIV Card Issuer (PCI) Operations Plan, 14 February 2019, Version 1.25*
- *United States Department of State Bureau Of Information Resource Management (IRM) Derived PIV Credential Issuer (DPCI) Operations Plan, Version 1.7, May 2022*
- *FIPS 201 / FICAM Evaluation Program Remote PIV Card Annual Testing Report, Version 1.1 Department Of State (PKI Shared Service Provider) & Department Of State (Issuing Organization), May 6, 2026*
- *Federal PKI Activity Report Updated: April 3, 2023.*

A direct CP-to-CPS traceability analysis was performed. The *Department of State PKI X.509 Certification Practices Statement*, was evaluated for conformance to the following policies:

- *Department of State (DoS) Public Key Infrastructure (PKI) X.509 Certificate Policy*
- *X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework*

A direct CP-to-CPS traceability analysis was performed. The Department of State PKI X.509 Certification Practices Statement, was evaluated for conformance to the following policies:

- Department of State (DoS) Public Key Infrastructure (PKI) X.509 Certificate Policy
- X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework

Eleven (11) disparate items were found to not address the requirements of the applicable policies.

The operations of the Department of State PKI systems were evaluated for conformance to “*Department of State PKI X.509 Certification Practices Statement*”

The evaluation of operational conformance to the CPS identified sixteen items that did not comply.

No failures were found that suggested that the system had been operated in an overtly insecure manner. Discrepancies with the stated practices are identified in this report. It is the lead auditor’s opinion that effective controls providing reasonable assurance that the practices defined in the applicable certification practice statements are in place and operational, as described in the Audit Report.

2026.08.28

04:50:23
-04'00'

 **X**

James Walker Jung
Lead Auditor