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

19 October 2022

United States Patent and Trademark Office
Policy Management Authority
Madison West (MDW)
600 Dulany Street
Alexandria, Virginia 22314

Subject: Compliance Audit for United States Patent and Trademark Office Public Key Infrastructure 2022

A compliance audit of The United States Patent and Trademark Office Public Key Infrastructure was conducted by Mr. James Jung of The Slandala Company. USPTO operates a Public Key Infrastructure (PKI) whose hierarchy is cross certified with the Federal Bridge PKI and issuing Personal Identity Verification (PIV) cards. The audit was conducted to verify that the USPTO PKI is operating in accordance with the security practices and procedures described by the following documents:

- Certification Practices Statement for the United States Patent and Trademark Office, June 3, 2022, Version 4.2,
- Certificate Policy for the United States Patent and Trademark Office, June 3, 2022, Version 4.1,
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.2, December 1, 2021.

USPTO operates the following Certification Authority (CA):

- CN = USPTO_INTR_CA1, CN = AIA, CN = Public Key Services, CN = Services, CN = Configuration, DC = uspto, DC = gov
    - Subject Key Identifier= 8d474ad15e45eaee2f515847214f12ebca7aa15f

The compliance audit evaluated the certificate authority, registration authority functions, repositories, certificate status servers, identity management systems (IDMS) and ancillaries associated with the CA. As part of the audit, findings from the previous year were reviewed, and have been corrected. The Memorandum of Agreement between the United States Federal Public Key Infrastructure (PKI) Policy Authority (Federal PKI Policy Authority) and USPTO, was also reviewed for compliance. The previous audit letter is not posted as called for by the MOA.

The compliance audit was performed via interviews, documentation reviews and site visits performed during September 2022. Two of the five USPTO RA sites were assessed. An on-site

review of the RA in Alexandria Virginia was performed. A remote audit of the RA site in Denver Colorado was performed. This audit covers the following period.

- Audit Period Start: 15 September 2021
- Audit Period Finish: 15 September, 2022

The 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 with or address the requirements of the applicable policies are categorized as Disparate.

- Disparate – CPS practices found to not comply or address the requirements of the applicable policies.

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. 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. James Jung and The Slandala Company meet the Federal PKI Compliance Auditor requirements for qualifications and independence. 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); 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 in the USPTO PKI operations, nor has he had any responsibility for writing the "*Certification Practices Statement for the United States Patent and Trademark Office."* Mr. Jung and The Slandala Company are independent of the USPTO PKI and the RA operations and management.

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

- Certification Practices Statement for the United States Patent and Trademark Office, June 3, 2022, Version 4.2,
- Certificate Policy for the United States Patent and Trademark Office, June 3, 2022, Version 4.1.
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.2, December 1, 2021
- X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.36, 6 May 2022
- Memorandum of Agreement between The United States Federal Public Key Infrastructure Policy Authority and the United States Patent and Trademark Office, signed December 2020
- Private Key Recovery Request of a USPTO PIV Subscriber Draft Form
- IPKI Master Training Record
- Information System Contingency Plan (ISCP), Version 4.8, 10 August 2022
- United States Patent and Trademark Office Personal Identification Verification (PIV) Credential/Card Issuance Acknowledgement Form
- Privacy Impact Assessment for the Identity Management Authenticator (ID-AUTH)
- Privacy Threshold Analysis for the Identity Management Authenticator (ID-AUTH)
- PKI Monthly Audit Log Examination Report, January 27, 2022

A direct CP-to-CPS traceability analysis evaluated the following the *Certification Practices Statement for the United States Patent and Trademark Office, June 03, 2022, Version 4.2* for compliance with the following policies:

- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.2, December 1, 2021,*
- *Certificate Policy for the United States Patent and Trademark Office, June 3, 2022, Version 4.1.*

Thirty-seven disparate items were identified.

PKI operations were evaluated for conformance to the "*Certification Practices Statement for the United States Patent and Trademark Office, June 03, 2022, Version 4.2."* Eight requirements were found to not comply.

No failures were found that suggested that the system had been operated in an overtly insecure manner. Discrepancies with the stated practice statements are identified in the report and it is the lead auditor's opinion that the USPTO Registration Authorities have maintained effective controls.

10/19/2022

X James Walker Jung DIGITALLY SIGNED The Slandala Company

James Jung
Director, The Slandala Company
Signed by: Jung.James.W.ORC3011047256.ID

Jung.James.W.ORC3011047256.ID Digitally signed by Jung.James.W.ORC3011047256.ID Date: 2022.10.19 15:10:43 -04'00'