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

14 June 2023

Caroline Godfrey
Chief Security Officer
WidePoint Cybersecurity Solutions Corporation
11250 Waples Mill Road
South Tower, Suite 210
Fairfax, VA 22030

The Slandala Company conducted a compliance audit of the WidePoint Cybersecurity Solutions Corporation Public Key Infrastructure (PKI) to verify that the PKI was being operated in accordance with the security practices and procedures described in the following Practices and Policies:

- *Certification Practices Statement for the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Shared Service Provider (SSP) Public Key Infrastructure (PKI), Version 4.2.5, September 2021*
- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.3, December 1, 2021*

WidePoint operates several Public Key Infrastructure systems collectively referred to as the Information Assurance/Identity Management System (IA/IDM), including the following certificate authorities:

- CN=ORC SSP 4, O=ORC PKI,C=US
- CN=WidePoint ORC SSP 5 ,O=ORC PKI,C=US

The Compliance Audit evaluated the Certificate Authority, Directory Server, Certificate Status Servers and Card Management Systems components associated with these CAs. Registration Authority functions are performed by WidePoint staff at their primary site. SSP registration are being performed by client staff at the agency site. The compliance audit reviewed findings from the previous year. There have been no major changes to the system.

The audit also evaluated conformance to the requirements of the Memorandum of Agreement (MOA) between Widepoint and the FPKIPA covering interoperability between the WidePoint SSP PKI and the FPKI, signed June 2020.

The compliance audit was performed via interviews, documentation reviews and site visits performed in May 2023. This audit covers the following period:

- Audit Period Start: March 2022
- Audit Period Finish: April 2023

The operational compliance audit was performed using a requirements decomposition methodology and was initiated by first performing a direct CP-to-CPS traceability analysis. The Certification Practices Statement for the WidePoint SSP PKI was evaluated for conformance to the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

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 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,
- 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, who acted as the lead auditor. 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 Certified Information Systems Auditor (CISA). He has implemented or operated PKI systems for the Department of State, the Department of Energy, 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 and several of the Department of Defense (DoD) agency Registration Authorities, Local Registration Authorities and External Certificate Authorities. Mr. Jung has been the lead auditor for the Department of Defense Certification Authorities the Department of Treasury Public Key Infrastructure (PKI) and Shared Service Provider (SSP) and the Federal PKI (FPKI) Trust Infrastructure, including the Federal PKI Common Policy Framework (FCPF) Certification Authority and the Federal Bridge Certification Authority (FBCA).

Mr. Jung has not held an operational role or a trusted role on the WidePoint PKI systems, nor has he had any responsibility for writing the Certificate Practices Statements. The Slandala Company and Mr. Jung are independent of the WidePoint PKI and its operations and management.

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

- *Certification Practices Statement for the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Shared Service Provider (SSP) Public Key Infrastructure (PKI), Version 4.2.5, September 2021*

- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.3, December 1, 2021*
- *Memorandum of Agreement between The United States Federal Public Key Infrastructure Policy Authority ("Policy Authority") and WidePoint Cybersecurity Solutions Corporation [Personal Identity Verification Shared Service Provider], signed June 2020*
- *Public Key Infrastructure Interoperability Test Report: May 2018 – WidePoint SSP*
- *Federal Election Commission Registration Practice Statement, version 3.1 July 2019*
- *ORC Personal Identification Verification Card Issuance (PCI) Operations Plan, February 5, 2014, Version 1.4*
- *Federal Election Commission (FEC) Registration Authority (RA) Compliance Audit Report For The WidePoint Cybersecurity Solutions Corporation Shared Service Provider (SSP) Public Key Infrastructure (PKI), Date: 16 March 2020*
- *WidePoint HSPD-12 Roles and Responsibilities*
- *WidePoint Shared Service Provider Configuration Management Plan Widepoint PIV SSP CMP, Version 2.2, May 6, 2019*
- *Information Assurance/ ID Management Local Registration Authority (LRA) Appointment Letter Template*
- *WidePoint Information Assurance/ Identity Management (IA/IDM) Procedure # 4-6.1, Information Assurance/Identity Management Disaster Recovery Site Safe Procedure, approved 4/5/2016*
- *WidePoint Information Assurance/ Identity Management (IA/IDM) Procedure # 4-5, Information Assurance/Identity Management System Backup Procedure, approved 4/5/2016*
- *WidePoint Information Assurance/ Identity Management (IA/IDM) Procedure # 7-0, Information Assurance/Identity Management Disaster Recovery (DR) Site Access, approved 4/5/2016*
- *Key Compromise Plan Version 1.0, March 28, 2017*
- *Advanced Surveillance Group Background Check Description*
- *WidePoint Cybersecurity Solutions Corporation Incident Response Plan, June 28, 2019, version 1.6*
- *WidePoint Rules of Behavior*
- *ORC Information Assurance/ Identity Management Roles Manual, February 5, 2014, Version 2.0.8*
- *Information Assurance/Identity Management Privacy Policies and Procedures Policy*
- *WidePoint Information Assurance/Identity Management (IA/IDM) System Risk Management Plan, April 5, 2016, Version 1.4*
- *WidePoint Trusted Role List - November 19, 2021*
- *WidePoint Information Assurance / Identity Management (IA/IDM) Contingency Plan Test Report 20 August 2020*
- *WidePoint Cybersecurity Solutions Corporation Incident Response Plan Test Report, June 28, 2019*

The Certification Practices Statement for the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Shared Service Provider (SSP) Public Key Infrastructure (PKI),

Version 4.2.5, September 2021 was evaluated for conformance to the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.3, December 1, 2021.

The analysis identified nineteen instances where policy description and the practice description were disparate.

The audit included a compliance audit of the practices described in the Widepoint SSP CPS. Three items did not comply with the policy or practice statements. This includes one finding from the previous audit related to the virtual host audit processes.

SSP RA operations were audited at the Federal Election Commission (FEC) in Washington DC. No items were identified that did not comply with the policy or practice statements

No failures were found that suggested that the system had been compromised or operated in an overtly insecure manner. Discrepancies with the stated practices are identified in this report. A Plan of Actions and Milestone (POA&Ms) has been identified to address these findings. 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.

6/14/2023

X James Walker Jung DIGITALLY SIGNED The Slandala Company

James Jung
Lead Auditor
Signed by: Jung.James.W.ORC3011047256.ID

Jung.James.W.ORC3011047256.ID Digitally signed by Jung.James.W.ORC3011047256.ID Date: 2023.06.14 09:57:46 -04'00'