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

26 April 2017

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

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

- *Certification Practice Statement For the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Access Certificates for Electronic Services (ACES)Public Key Infrastructure (PKI) Version 4.0.1, 23 June 2016*
- *Certificate Policy for Access Certificates for Electronic Services, January 4, 2017, Version 3.1*

WidePoint operates several Public Key Infrastructure systems collectively referred to as the Information Assurance/Identity Management System (IA/IDM). These systems include the following certificate authorities, asserting the identified policy OIDs:

- CN = ORC ACES 4, O=ORC PKI, C=US
  - 2.16.840.1.101.3.2.1.1.1

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 with additional support from two additional sites. The compliance audit reviewed findings from the previous year. Findings that were identified previously are identified in the audit report. There have been no major changes to the system.

The audit also evaluated conformance to the requirements of the Memorandum of Agreement between GSA Federal Acquisition Services ACES PMO and WidePoint Cybersecurity Solutions Corporation signed July 2016.

The compliance audit was performed via interviews, documentation reviews and site visits performed on 8-17 March 2017.

The Audit was performed by first conducting a CP-to-CPS traceability analyses.

The Certification Practice Statement For the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Access Certificates for Electronic Services (ACES) Public Key Infrastructure (PKI) Version 4.0.1, 23 June 2016 was evaluated for conformance to the following policy:

- Certificate Policy for Access Certificates for Electronic Services, January 4, 2017, Version 3.1

Findings of the CP-to-CPS traceability analysis are categorized as follows:

- Complies – the practices documented in the CPS address the policy,
- Disparate – the practices documented in the CPS do not address the policy,
- Recommendation - the practices documented in the CPS address the policy; however, suggestions are made to clarify or improve the CPS.

The audit was performed by using a requirements decomposition methodology. The CPS was reviewed and decomposed into requirements. The requirements were divided in a manner to facilitate the audit. In cases where items could easily be evaluated together they were retained as a single requirement; where items required separate evaluation, they were divided.

The requirements were then evaluated to determine the general methodology for their evaluation; this may include system configuration checks, facility inspections, interviews, documentation review, or other types of evaluation. In some cases "no action" may be identified for requirements that are not auditable. "Non-auditable" requirements include text in the CPS that provides introductory or background information or requirements that were more fully specified in other parts of the CPS.

After the identification of auditable requirements, each requirement was examined to derive activities ("audit steps") that should be taken by the auditor to fulfill the audit of that requirement. Where appropriate, documentation required to support these activities was identified.

The audit step activities are performed during the site visits and documentation reviews. Observations and recommendations are identified and may be included. Recommendations may include suggestions on how a failed requirement might be put into compliance or suggestions on how a passed requirement might be improved.

Initial finding are also determined during the site visits, and documentation reviews. Findings 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, other "best practices" 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 2001 and has 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) 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 Practice Statement For the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Access Certificates for Electronic Services (ACES)Public Key Infrastructure (PKI) Version 4.0.1, 23 June 2016*
- *Certificate Policy for Access Certificates for Electronic Services, January 4, 2017, Version 3.1*
- *Memorandum of Agreement between GSA Federal Acquisition Services ACES PMO and WidePoint Cybersecurity Solutions Corporation signed July 2016*
- *ACES Monthly Report February 2017*
- *Information Assurance Continuity of Operations & Disaster Recovery Plan, Version 1.4, October 4 2010 - Operational Research Consultants, Inc*
- *Information Assurance/Identity Management Contingency Plan, version 1.8, February 24, 2016*
- *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*
- *Certification Authority User Recertification 2015, 7/10/2015*
- *ORC Configuration Management Plan, 17 December 2014*
- *ORC Information Assurance/ Identity Management, Roles Manual, Revised February 5, 2014*
- *Key Compromise Plan Version 1.0, March 28, 2017*
- *Operational Research Consultants, Inc. Key Recovery Practice Statement (KRPS), Version 2.0, September 2, 2012*
- *Advanced Surveillance Group Background Check Description, March 2017*
- *WidePoint Incident Response Plan version 1.4 May 19, 2016*
- *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*
- *Annual Archive Checklist, verified 15 September 2016*
- *WidePoint Trusted Role List SSP August 2016*
- *Personal Identity Verification Interoperable (PIV-I) Test Report for ORC July 2016*
- *WidePoint IA IDM Contingency Plan Test Report April 29, 2016*

The Certification Practice Statement For the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Access Certificates for Electronic Services (ACES)Public Key Infrastructure (PKI) Version 4.0.1, 23 June 2016 was evaluated for conformance to the following policy:

- Certificate Policy for Access Certificates for Electronic Services, January 4, 2017, Version 3.1

The analysis identified 45 instances where policy description and the practice description were disparate. These discrepancies between the ACES CP and WidePoint ACES CPS often are the result of misused terms (e.g., renewal versus rekey and trusted roles, including officers and administrators) or simply not

providing a practice description as a level of detail appropriate for the CPS. None of these discrepancies have led to an operational vulnerability in the practices.

The audit included a compliance audit of the practices described in:
The Certification Practice Statement For the WidePoint (formerly Operational Research Consultants, Inc. (ORC)) Access Certificates for Electronic Services (ACES)Public Key Infrastructure (PKI) Version 4.0, 15 April 2016.

- 9 instances of non-compliance with the identified CPS,

No failures were found that suggested that the system had been compromised or operated in an overtly insecure manner. It is the lead auditor's opinion that the WidePoint PKI systems provided reasonable security control practices. Discrepancies with the stated CPS practices are identified in this report. WidePoint has identified Plans of Actions and Milestone (POA&Ms) to address these findings. It is the lead auditor's opinion that, with the implementation of the items identified in the POA&M, the WidePoint PKI systems will be in compliance with the policy and practices of the WidePoint PKI systems for those items evaluated during the audit.

4/26/2017

X James Walker Jung DIGITALLY SIGNED

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

James Walker Jung DIGITALLY SIGNED

Digitally signed by Jung.James.W.ORC3010006689.ID
DN: c=US, o=U.S. Government, ou=ECA, ou=ORC, ou=The Slandala Company, cn=Jung.James.W.ORC3010006689.ID
Date: 2017.04.26 07:13:48 -04'00'