



June 15, 2015

MEMORANDUM FOR: CHI HICKEY
PROGRAM MANAGER, PUBLIC KEY INFRASTRUCTURE
(PKI) SYSTEM
OFFICE OF GOVERNMENTWIDE POLICY

FROM: DOMINIC SALE
AUTHORIZING OFFICIAL
OFFICE OF GOVERNMENTWIDE POLICY

THRU: KURT D. GARBARS
CHIEF INFORMATION SECURITY OFFICER
OFFICE OF GSA INFORMATION TECHNOLOGY (IT)

THRU: JONATHAN WALLICK
INFORMATION SYSTEMS SECURITY MANAGER
OFFICE OF GSA INFORMATION TECHNOLOGY (IT)

Subject: SECURITY ASSESSMENT AND AUTHORIZATION FOR
VERIZON SHARED SERVICE PROVIDER FOR THE PUBLIC
KEY INFRASTRUCTURE SYSTEM

A security controls assessment of the Verizon Shared Service Provider (SSP) Public Key Infrastructure (PKI) Information System has been conducted at the Federal Information Processing Standards (FIPS) 199 Moderate Impact level. This assessment was conducted in accordance with the requirements of Federal Information Security Modernization Act of 2014; the Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; the National Institute of Standards and Technology (NIST) Special Publication 800-37 R1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; and the General Services Administration (GSA) Security Authorization Process.

The Verizon Shared Service Provider (SSP) Public Key Infrastructure (PKI) Information System security assessment and authorization package includes the following:

- The Security Security Plan (SSP);
- The System Security Assessment Report (SAR);



- The Privacy Impact Assessment (PIA);
- The Plan of Action and Milestones (POA&M);
- The Penetration Testing Report;
- The Contingency Plan with Business Impact Analysis; and
- The Contingency Plan Test Report.

The security controls listed in the System Security Plan have been independently tested and assessed by Telos Corporation using the assessment methods and procedures described in the Security Assessment Report. The purpose of this controls assessment was to determine the extent to which system security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The POA&M describes the corrective measures that have been implemented or are planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

Based on the security configuration defined in the System Security Plan, and the planned actions reported in the POA&M, I recommend authorization of the Verizon Shared Service Provider (SSP) Public Key Infrastructure (PKI) Information System.

RECOMMEND AUTHORIZATION:

6/15/2015

X Jonathan Wallick

Jonathan Wallick
Information System Security Manager
Signed by: JONATHAN WALLICK

After reviewing the results Security Assessment Report and the supporting evidence provided in the security authorization package, I have determined that the risk to Federal agency operations, data, and/or assets resulting from the operation of the information system is acceptable.

Accordingly, I am issuing an Authorization to Operate (ATO) for the Public Key Infrastructure information system. This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.



The security authorization of the information system will remain in effect for three (3) years from the date of this memorandum.

APPROVED:

6/15/2015

X Dominic K. Sale

Dominic Sale
Authorizing Official
Signed by: DOMINIC SALE

CONCURRENCE:

6/15/2015

X Kurt Garbars

Kurt D. Garbars
Chief Information Security Officer
Signed by: KURT GARBARS

Copies of the authorization package are available for review at the GSA facilities in the Washington, D.C. metropolitan area. If you have any questions or comments regarding this authorization to operate, please contact Man Lau, Director, ISSO Support Division, at (202) 219-7982.