U.S. General Services Administration

MEMORANDUM FOR	Nicolas Popp System Owner SVP, Information Protection Symantec
FROM:	Dominic K. Sale Authorizing Official Deputy Associate Administrator General Services Administration
THRU:	Kurt Garbars Chief Information Security Officer General Services Administration
THRU:	Joseph Hoyt Information System Security Manager General Services Administration
SUBJECT:	Decision for Standard Assessment & Authorization
DATE:	December 12, 2016

A security controls assessment of the Symantec environment has been conducted at the Federal Information Processing Standards (FIPS) 199 Moderate Impact level in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* and General Services Administration (GSA) IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA), CIO-IT Security-06-30.

The security controls listed in the System Security Plan (SSP) have been assessed by Telos using the assessment methods and procedures described in the Security Assessment Report (SAR) to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome for meeting the security requirements of the system. A Plan of Action and Milestones (POA&M) has been developed describing the corrective measures implemented or 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 SSP, and the planned actions in the POA&M, I recommend authorization of the Symantec information system.

RECOMMEND AUTHORIZATION:

12/12/2016

X Joseph Hoyt

Joseph Hoyt
Information System Security Manager
Signed by: JOSEPH HOYT

After reviewing the results in the SAR, and the supporting evidence provided in the security authorization package, I have determined the risk to GSA's Federal systems, 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 Symantec Shared Service Provider Public Key Infrastructure Symantec information system in its current environment and configuration. This authorization is valid for Three (3) years from the Authorizing Official's signature on this letter or until a significant change in the system or threat/risk environment, as described in CIO-IT Security 06-30, necessitates re-assessment and re-authorization. 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 under the following conditions:

1) Symantec shall conduct and submit RA audits on their customers that they service under the: VeriSign SSP Intermediate CA - G3 and Symantec SSP Intermediate CA - G4, which are included in this ATO System Boundary, within 6 months of the signed date of this ATO. All issues identified with the audits shall be addressed and resolved by 3 months from receipt of the audit report from the third party auditor.

2) Provide a mapping of Symantec's Certificate Policy (CP) and Certificate Practice Statement (CPS) of VeriSign SSP Intermediate CA - G3 and Symantec SSP Intermediate CA - G4 to the Federal Common Policy (CP) and CPS and resolve all issues within 2 months of the signed date of this ATO.

3) Submit one populated, representative sample card for each PIV issuer configuration used to the FIPS 201 Evaluation Program for testing for all customers under the VeriSign SSP Intermediate CA - G3 and Symantec SSP Intermediate CA - G4 within six months of receipt of this signed ATO letter. Symantec shall correct all errors identified from testing. In addition, Symantec and their associated issuers shall work with the agencies

to issue the correct updated PIV cards to the federal agencies within three months after errors are identified from Testing.

4) Submit sample production end-entity certificates currently in use for all types of certificates issued from the Symantec PKI. Resolve all issues identified within three months of receipt of feedback.

5) Review and sign the Memorandum of Agreement between the FPKIPA and Symantec Shared Service Provider PKI for the Federal Government within one week of this signed ATO.

APPROVED:

12/12/2016

X Dominic K. Sale

Dominic Sale
Authorizing Official
Signed by: DOMINIC SALE

CONCURRENCE:

12/12/2016

X Kurt Garbars

Kurt 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.