United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

Memorandum

To: Martha D. Eichenbaum, System Owner
Chief, End User System Administration
Office of the Chief Information Officer, Service Delivery Division

From: Karen Matragrano, Authorizing Official
Director, Service Delivery
Office of the Chief Information Officer

1-12-17

Subject: Authorization to Operate (ATO) for the Symantec Validation and Protection (S-VIP) Cloud Software as a Service (SaaS)

Authorization of the S-VIP Cloud SaaS and its application-level components in the production environment has been performed in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, "*Security of Federal Automated Information Resources,*" and the Department of the Interior (DOI) Assessment and Authorization (A&A) Program. The DOI A&A Program is based on the requirements set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and the DOI Security Control Standards. As the Authorizing Official, I approve the request for the ATO with conditions.

The ATO is effective for eight (8) months and is contingent upon continued application of security controls in place and the conditions designated below:

a.) Symantec must proceed with pursuing FedRAMP Compliance as follows:
- Review the "Guide to Understanding FedRAMP" at www.fedramp.gov;
- Download the FedRAMP Templates;
- Determine the systems security categorization level;
- Compile policies, risk assessments, and internal and external security assessments;
- Map system inventories and boundaries;
- Map existing controls to FedRAMP requirements and note gap analysis;
- Submit the System Security Plan and supplemental documentation to DOI OCIO;
- Engage and accredited 3rd Party Assessment Organization (3PAO) to perform the FedRAMP assessment.

b.) Symantec must comply with the DOI IT Security and Privacy Requirements for the duration of the conditional ATO and during the FedRAMP process.

c.) The requirements set forth in the DOI IT Security and Privacy Requirements documents must be fully met by the end of the initial contract period of performance and in advance of award or use of S-VIP, Symantec must, at a minimum, contractually confirm that all DOI data and information are protected in accordance with the DOI IT Security and Privacy Requirements.

The Information System Security Officer should retain a copy of this conditional ATO letter with all supporting documentation as a permanent record.