

JUSTIFICATION
FOR EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

2. Description of Action: This proposed action is for a firm-fixed-price delivery order (DO) issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Governmentwide Acquisition Contract (GWAC).

3. Description of Supplies or Services: The proposed action is to procure Red Seal software licenses and associated maintenance for VA's Layer 3 network devices for VA, Office of Information and Technology, Office of Information Security. Red Seal software licenses provide seamless integration into Risk Vision, which is VA's Governance, Risk, and Compliance (GRC) tool used for security continuous monitoring, as demonstrated by VA's initial pilot completed in November 2014. Red Seal delivers real-time network visualization that can detect, document and provide actionable intelligence to information system owners on critical risks located on networked equipment. Additionally, the Red Seal integration into Risk Vision allows critical risk reviews and responses to take place enabling VA to understand potential threats to VA systems. Red Seal also provides Federal regulatory compliance with the Federal Information Security Management Act requirements as well as Secure Technical Implementation Guides both required by VA. Additionally, Red Seal is deployed without Credential Authentication on Layer 3 network devices, which reduces the deployment effort and maintenance on VA's network appliances. Maintenance is also required to ensure the software remains operational. The period of performance is for 12 months from date of award, with one, 12 month option period. Delivery of licenses shall be within 30 days of delivery order award.

4. Statutory Authority: The statutory authority permitting this exception to fair opportunity is Section 41 U.S.C 4106(c)(2) as implemented by Federal Acquisition Regulation (FAR) 16.505(b)(2)(i)(B) entitled, "Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized."

5. Rationale Supporting Use of Authority Cited Above: Based on extensive market research, as described in section 8 of this document, it was determined that limited competition is viable among authorized resellers of the Red Seal software licenses and associated maintenance. Only Red Seal software can meet all of VA's functional requirements. Specifically, Red Seal is the only product that can be integrated, supported, and deployed with VA's existing Risk Vision GRC tool. Also, only Red Seal can import files directly to the Layer 3 devices without deploying a software configuration file to the routers. VA cannot allow a vendor to deploy a software

configuration file to the routers as this would introduce unknown risk to network security. Additionally, Red Seal is the only product that can be used without the requirement to provide a credentialed, monitoring agent deployed on the network device (authentication access) for use in traversing communication paths across VA's network. Allowing authentication access to network devices increases the risk of threats and vulnerabilities on the device and may require re-accreditation of those infrastructure systems. The impact to VA not using Red Seal will result in an increased susceptibility to threat agents being introduced into VA's Layer 3 devices. These devices allow all communication capabilities enterprise-wide and would cripple VA network operations, impact the ability to deliver patient care and benefits administration due to network connectivity issues. VA requires the capability to deploy network visualization and compliance capability that does not require deployment of Layer 3 configuration files or separate authenticated access to Layer 3 devices to perform. Red Seal is the only software that meets this requirement and does not require separate authenticated agents or processes to run on Layer 3 devices. As a result, there is no chance of threat agents or vulnerabilities being introduced on VA's network. Red Seal integrates with other security services deployed in VA and any Layer 3 configuration and compliance data used by Red Seal can be obtained without access to the Layer 3 device.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in the market research section of this document. This effort did not yield any additional sources, other than authorized resellers, that can meet the Government's requirements. It was determined, however, that limited competition is viable among authorized resellers for this software license. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), the award synopsis and the justification will be made publicly available on the Federal Business Opportunities Page within 14 days of award. The justification will also be posted to the NASA SEWP V GWAC website along with the Request for Quotation.

7. Actions to Increase Competition: The Government will continue to conduct market research to ascertain if there are changes in the market place that would enable future actions to be competed.

8. Market Research: The Government's technical experts conducted market research in March 2015 by reviewing possible software products that provide network visualization and proactive security intelligence. VA conducted market research on Red Seal, FireMon Security Manager, Core Insight, and Tuffin. Based upon reviewing publicly available information, Core Insight and Tuffin could not meet VA's functional requirements and could not support organizations that deploy greater than 10,000 Layer 3 devices. VA representatives met with Red Seal and FireMon to provide an overview of their capabilities. VA requires a capability to be deployed and integrated with the Risk Vision GRC tool, the capability to provide network visualization and mapping, and to be deployed without additional constraints and efforts on VA staff. Red Seal is the only product that can be integrated with Risk Vision and deployed without additional constraints on VA staff. FireMon Security Manager cannot be deployed as it would require a separate supporting, hosted environment and would require the deployment of additional resources on network

devices to support credentialed authentication access. FireMon would require a third party authentication access to the Layer 3 devices which is not allowed within VA. During the meeting, FireMon was made aware that VA could not support their solution. FireMon is not capable of providing an out of the box solution as the GRC tool would have to be re-architected to allow authenticated access to VA network devices. Based on the product descriptions, the functional overviews, and the supporting architecture requirements, it was determined that Red Seal is the only product that can support VA's requirements and current operating environment.

Additional market research was conducted in July 2015 utilizing the NASA SEWP V GWAC Quick Request for Information Tool. It was determined that there is adequate competition for the Red Seal software licenses and associated maintenance on the NASA SEWP V GWAC.

9. Other Facts: None.