

JUSTIFICATION  
FOR AN 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: The proposed action is for a firm fixed-price order to be issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise Wide Procurement (SEWP) V Government Wide Acquisition Contract (GWAC) for the procurement of premium support for a quantity of 18 brand name Palo Alto networked firewall devices, Palo Alto threat prevention license subscriptions for a quantity of 28 Palo Alto networked firewall devices (10 high availability firewalls and 18 backup firewalls), and Palo Alto Panorama License renewal for a quantity of 1 Palo Alto Lab firewall.
3. Description of the Supplies or Services: VA, Office of Information Security, Network Security Operations Center (NSOC) requires premium support for a quantity of 18 brand name Palo Alto networked firewall devices, Palo Alto threat prevention license subscriptions for a quantity of 28 Palo Alto networked firewall devices (10 high availability firewalls and 18 backup firewalls), and Palo Alto Panorama License renewal for a quantity of 1 Palo Alto Lab firewall. VA NSOC currently has a Palo Alto firewall Intrusion Prevention Systems/Intrusion Detection System (IPS/IDS) hardware/ software solution in-place. This solution consists of firewalls, which manage network traffic. Premium support consists of maintaining and supporting the current list of releases on the Palo Alto Network Support Website, access to maintenance releases, minor releases, and major releases, verifying and correcting defects in software for currently supported maintenance releases, access to online support via the Palo Alto Network Support website, return and repair service for hardware defects, after hours telephone support (24x7x365 for severity one critical issues, and next business day ship advance for hardware defects).

The Palo Alto Panorama software manages the firewall device. It allows the network professional to manage all firewall traffic, manage all aspects of device configuration, push global policies, and generate reports on traffic patterns or security incidents. The Panorama software support for the one lab firewall device will consist of software upgrades and updates to include major releases, point releases, service releases, and security releases of applicable software. The Panorama software support for the one lab firewall device will consist of software upgrades and updates to include major releases, point releases, service releases, and security releases of applicable software on a quarterly basis, and/or within 48 hours in cases in which a high risk vulnerability fix becomes available. The upgrades and updates are necessary for the firewall hardware to operate successfully.

The Palo Alto threat prevention subscriptions for the one lab firewall device are add-on services on the firewall that enhance performance and features. Activating this add on

subscription assists in protecting the VA network from advanced threats by identifying and scanning all traffic applications, users, and content across all ports and protocols. This add on feature must be activated through a license subscription. Each account allows a certain number of authorized users to access the device. The period of performance is 12 months with three, 12-month option periods to be exercised at the discretion of the Government.

[REDACTED]

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 market research, as described in section eight of this justification, it was determined that limited competition is available among resellers for the aforementioned brand name requirements. The Palo Alto firewall IPS/IDS hardware/software solution in-place at the NSOC Palo Alto software releases and updates cannot be accessed without this premium support renewal. Without updated software releases and updates firewall hardware will have security holes and risks and will lack functionality. Any source that provides this premium support must have access to the Palo Alto's proprietary source code in order to ensure that the services provided are properly configured and that all release and updates made are pushed through the devices proprietary constraints. In order to provide Palo Alto Panorama software maintenance support, including software updates and upgrades, access to Palo Alto's proprietary source code is required. This code is required to ensure the services provided are properly configured.

Furthermore, no other firewall management software maintenance is compatible with or interoperable with the existing Palo Alto software licenses due to Palo Alto's proprietary software application programming interfaces, database structures and protocols. Palo Alto software releases and updates cannot be accessed without this software renewal, as only Palo Alto software can be used to update Palo Alto software. It is a proprietary software product and no other firewall management tool is capable of seamlessly integrating with the existing Palo Alto firewall management tool. The upgrades and updates are necessary for the firewall hardware to operate successfully. Only Palo Alto or an authorized reseller can provide the necessary software updates because of the proprietary source code required to develop and implement software updates.

In addition, Palo Alto threat prevention software is the only threat prevention software that will operate in a Palo Alto device. The device has proprietary constraints that only for Palo Alto brand name software to run on them and cannot be configured to allow another brand name software add-on onto the machine. It is a proprietary software product and no other threat prevention software is capable of integrating with the existing Palo Alto threat prevention software. Without the threat prevention software, the firewall hardware will have security holes and put the network at serious risk.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in section eight of this justification. This effort did not yield any additional sources that can meet the Government's requirements. It was determined, however, that limited competition is viable among authorized resellers for this brand name software maintenance, subscriptions, and premium support. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), the award notice for this action will be synopsisized on the Federal Business Opportunities page and the justification will be made publicly available within 14 days of award

7. Actions to Increase Competition: The Government will continue to conduct market research to ascertain if there are changes in the marketplace that would enable future actions to be fully competed. Specifically, the Government's technical experts will continue to research other brand name software and the potential ability to integrate with the existing firewall log management tool in place and the costs associated with the configuration, integration and implementation.

8. Market Research: Market research was conducted by the Government's technical experts in March 2017 by reviewing similar services and products from Jupiter Networks. Specifically, the VA technical experts contacted Jupiter Networks, a provider of firewalls and firewall software. It was determined that Jupiter Networks, while similar in service to Palo Alto, was not able to meet requirements. Jupiter Networks agreed that they could not support Palo Alto devices or provide software that could operate on the Palo Alto devices. Only Palo Alto software providers are capable of providing the software and required maintenance and upgrades for Palo Alto software, as the software is proprietary.

The Government's technical experts also conducted market research in March 2017 via a Request for Information (RFI) posted to NASA SEWP V GWAC requesting Palo Alto premium software maintenance, Palo Alto threat prevention license subscriptions and Palo Alto Panorama License renewal. Two vendors responded to the RFI and proposed utilizing Palo Alto brand products. Also, market research was conducted in June 2017 by utilizing the NASA SEWP Product LookUp Tool and there are multiple resellers of these brand services and products. Limited competition is therefore anticipated.

Further market research was conducted on June 13, 2017 by the Government's technical experts contacting Palo Alto directly. Palo Alto indicated maintenance and support on the Palo Alto Networks devices is proprietary and manufactured by Palo Alto Networks and no other maintenance can be applied to the devices. In addition, on July 19, 2017, Palo Alto indicated the source code was not available for purchase. The Palo Alto networks maintenance and support can be sold through a 3<sup>rd</sup> party via a Government contract.

9. Other Facts: None.