

JUSTIFICATION
FOR AN EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
1701 Directors Blvd
Austin, TX 78744
2. Description of Action: This proposed action is for the award of a brand name firm-fixed-price delivery order 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: VA requires the renewal of six WildFire license subscriptions for Department of Veterans Affairs Office of Information Technology (OIT), in support of Palo Alto 5060 (PA-5060) devices for malware detection and prevention. To meet the challenge of modern-day malware, Palo Alto Networks has developed WildFire, a service that integrates with our next-generation firewalls and provides detection and prevention of modern malware. WildFire identifies unknown or zero-day malware by directly executing files in a virtual environment and observing malicious behavior. This enables Palo Alto Networks to identify malware quickly and accurately, even if the malware has never been seen before. The period of performance shall run from September 5, 2018, through September 4, 2019, with four 12-month option years.
4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 4106(c)(2) as implemented by the Federal Acquisition Regulation (FAR) Subpart 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 paragraph eight of this document, it was determined that limited competition is viable among authorized resellers for brand name WildFire license subscriptions. From the initial installation to the current state, WildFire has identified over 2000 variants of malware unique to the VA environment. To meet the challenge of modern-day malware, Palo Alto Networks WildFire service integrates with VA's next-generation firewalls and provides detection and prevention of modern malware. WildFire identifies unknown or zero-day malware by directly executing files in a virtual environment and observing malicious behavior. Even if the malware has never been seen before, the Palo Alto Networks is enabled to identify malware quickly and accurately,. No other product is capable of meeting the requirements of native Secure Socket Layer (SSL), Transport Layer Security(TLS), and Secure Shell (SSH) decryption/inspection capability to decrypt sessions to analyze their content, inline threat detection and blocking, inline ability to drop traffic related to discovered threats, full virtual system emulation for behavioral analysis of unknown threats,

adaptable and updateable logic within virtual test system, and port-agnostic inspection of well-known protocols. Additionally, unlike any other similar solution Wildfire provides detection of malware on non-standard ports and within application tunnels, the ability to decompress, analyze, and defend against all threats within compressed files, protects against lateral threat movement when deployed at the gateways and datacenter WAN, with minimal processing overhead/impact on email delivery and other business services. Wildfire natively identifies infected systems by IP address, active directory username, analysis environment automatically scales to meet the needs of the network, requires the implementation of no additional hardware or virtual servers by the VA, provides extensive integrated reporting and search functionality, provides comprehensive views into internal threat database, and can be implemented on currently installed VA infrastructure and platforms without the need for additional hardware.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in section 8 of this justification. This effort did not yield any additional sources that can meet the Government's requirements. However, it was determined that limited competition is viable among resellers for this brand name item. In accordance with 16.505(b)(2)(ii)(D), this action will be synopsized, and the justification will be made publicly available within on the Federal Business Opportunities Page due to the total estimated price exceeding the simplified acquisition threshold.

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: VA technical personnel conducted market research in January 2018 by issuing a Request for Information (RFI) on NASA SEWP to identify potential providers of the WildFire software. Also, research was conducted using publicly available technical specifications on similar products to identify if another solution could meet the needs of the VA. These similar solutions include FireEye by FireEye, SourceFire by Cisco, Checkpoint by ThreatCloud, and Fortinet by FortiSandbox. However no other solution provided full compatibility with the other software currently installed and in use within the same network. WildFire is a commercial off-the-shelf (COTS) software package currently in use on other projects within VA as a contracted product. WildFire is the only software capable of fulfilling all of the Government's requirements at this time while meeting the compatibility and interoperability requirements allowing them to work with existing, fielded software packages. Also, WildFire is the only product that will cost the VA no additional funds as it is the only product that will not require the implementation of additional hardware or virtual servers by the VA. Based on the above, only WildFire meets all the of the Government's requirements.

The contract specialist (CS) conducted market research in April 2018 by using the NASA SEWP V GWAC Provider Lookup and Market Research tools to determine what vendors are capable of providing the full requirement. Based on this market research, the CS found multiple vendors capable of meeting the full requirement through NASA SEWP.

9. Other Facts: None