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 delivery order to be issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Governmentwide Acquisition Contract (GWAC) for FireEye, Inc. (FireEye) malware protection appliances, software licenses, warranty and maintenance support.

3. Description of the Supplies or Services: The proposed action is to acquire six FireEye malware protection appliances, software licenses, warranty and maintenance support for VA, Office of Information and Technology, Service Delivery and Engineering, Enterprise Operations (EO). EO has a requirement to expand its existing FireEye architecture and infrastructure with additional malware protection appliances to provide network monitoring capabilities. EO also requires warranty and maintenance support for the additional FireEye malware protection appliances. The required warranty and maintenance support includes 24/7 telephone and web support, firmware updates, software updates, patches, and defect support for one year. The period of performance for delivery of malware protection appliances shall be 30 days after contract award. Warranty and maintenance support shall be provided for 12 months following acceptance of the malware protection appliances. The total estimated value of the proposed action is [redacted].

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) 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 the market research described in section 8 of this justification, it has been determined that limited competition is available for the aforementioned FireEye malware protection appliances, software licenses, warranty and maintenance support among authorized resellers. The existing EO network monitoring architecture and infrastructure consists of FireEye malware protection appliances located at five EO data centers, and EO requires additional appliances that are compatible with the existing infrastructure. No other malware protection appliances are interoperable or compatible with the existing FireEye-based malware protection systems and architecture. The current appliances and associated software communicates through a proprietary source code, and no other software can provide this communication capability without this proprietary source code. Specifically, only FireEye security appliances can provide upstream forwarding of any localized malware activity data into the existing FireEye architecture. The upstream forwarding of malware data produces a single view collective status of all security-

related activity over the network and displays the security posture of all elements operating on the network. No other brand name hardware and software appliance can accomplish this functionality, because no other product can communicate or integrate with the existing FireEye architecture, infrastructure and licensing with the single collective view EO Console, and thus will not allow monitoring and visibility of malware activity on the network.

While other devices such as International Business Machine's (IBM) Security Network Intrusion Prevention System, Cisco IronPort, and PaloAlto WildFire provide malware protection and monitoring, no other products are interoperable with EO's existing FireEye architecture. Therefore, no other product can operate in VA's FireEye architecture. Additionally, data monitoring and malware activity captured by another vendor will not integrate with the existing EO FireEye infrastructure components. Acquisition of different network monitoring devices and support would require a completely separate infrastructure to support a new malware protection appliance, resulting in duplication of cost previously expended in the existing infrastructure that would not be recovered through competition.

Additionally, the required software licenses, warranty and maintenance support, which consists of software updates, firmware updates, patches, and defect support can only be provided by FireEye or an authorized reseller. FireEye software is proprietary; no other vendor can access the necessary source code or capability to perform fixes and updates of the FireEye products. The proprietary source code is not available to third-party vendors; therefore, no other vendor other than an authorized reseller is capable of providing the required software and firmware updates for FireEye products.

6. Efforts to Obtain Competition: Market research efforts did not yield any additional sources that can meet the Government's requirements. Although the Government is limiting competition as a result of specifying brand name products and services, there are multiple authorized resellers of FireEye products and services on the NASA SEWP V GWAC. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), this action will be synopsized upon award on the Federal Business Opportunities Page page within 14 days after award, and this justification will be made publicly available. In accordance with FAR 16.505(a)(4)(iii)(A)(2), this justification will be provided with the solicitation to all contract awardees on the NASA SEWP V GWAC.

7. Actions to Increase Competition: The Government will continue to conduct market research to ascertain if there changes in the market place that would enable future requirements for the required malware protection appliances described herein to be competed.

8. Market Research: The Government's technical experts conducted market research by reviewing similar malware protection full packet capture systems that consists of appliances with pre-loaded software including IBM Security Network Intrusion Prevention System, Cisco IronPort, and PaloAlto WildFire. This market research is an ongoing process that started in 2012 and is continuously being conducted, as recently as April 2015. As a result of this market research, the Government's technical experts

confirmed that only FireEye malware protection appliances are interoperable with the existing EO FireEye architecture and infrastructure. No other vendor has the ability to provide the malware protection appliances, software licenses, and warranty and maintenance support. Additional market research was conducted in May 2015, wherein the Government's technical experts utilized the NASA SEWP V GWAC manufacturer lookup tool and identified several sources capable of meeting VA's needs. Therefore, VA anticipates limited competition for this action.

9. Other Facts: None.