

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 issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Governmentwide Acquisition Contract (GWAC).
3. Description of the Supplies or Services: VA Office of Information Technology, Service Delivery and Engineering, Enterprise Operations (EO) Security Division requires nine Cisco Sourcefire intrusion prevention system (IPS) devices and associated licenses and maintenance. The licenses are to be perpetually assigned to the associated Cisco Sourcefire IPS devices, model numbers AMP8350 and DC4000. The standard licenses function as an activation key to activate the IPS devices. Without the licenses, the devices will not operate. These devices are needed to meet the VA requirements of cross information technology (IT) system integration, interoperability with currently fielded systems, as well as the need for the IPS system to permit the upstream of data in order to produce a single view collective status of all security related activity over the network. In addition, VA requires maintenance to begin once the nine new Cisco Sourcefire IPS devices are accepted. The required warranty and maintenance includes 24/7 telephone and email support, software updates, patches and defect support for one year. The 12-month warranty and maintenance period will commence upon VA's acceptance of the Cisco Sourcefire device. The Cisco Sourcefire devices and associated licenses will be delivered within 30 days after award. The period of performance for maintenance of equipment will be 12 months.
4. Statutory Authority: The statutory authority permitting this 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." As required by FAR 16.505(a)(4), this justification is in accordance with FAR 16.505(b)(2)(ii)(A), (B), and (C) and is modified to show the brand name justification.
5. Rationale Supporting Use of Authority Cited Above: Based on market research, as described in section 8 of this document, it was determined that limited competition is viable among authorized resellers. The Cisco Sourcefire uses the Snort engine that allows customized approach for IT Security protection currently allowing EO cross IT Security integration. It is essential to keep the EO cross IT Security integration to continue supporting VA's Continuous Readiness Information Security Program requirements and Federal Information Security Management Act High needs detailed under National Institute of Standards and Technology 800-53 revision 4. VA requires

system security monitoring of all system logs and network connectivity to provide event and log correlation, event alerting and information security threat intelligence, and reporting of all network intrusion attempt activity. All Cyber Security intelligence is centralized in the Security Information and Event Management (SIEM) for data center systems and networks. Using combined SIEM Intrusion plug-in data feeds from Cisco Sourcefire collectively referred to as Cisco Sourcefire brand name intrusion prevention appliance and licenses meet these requirements.

In addition, Cisco Sourcefire software is the only software that can continue to build upon EO Security's existing Cisco Sourcefire -based IPS. Other brand name IPS devices researched are unable to integrate with the currently fielded Cisco Sourcefire architecture and Cisco Sourcefire -based intrusion prevention licensing. Additionally, no other brand name IPS has been determined to be interoperable or compatible with the currently fielded Cisco Sourcefire -based intrusion prevention system and Cisco Sourcefire architecture. Specifically, the current system and software communicates through a source code that is based on Cisco Sourcefire proprietary data. No other software can provide this communication capability without this source code. Existing Cisco Sourcefire security appliance inventory includes existing ownership of five existing Cisco Sourcefire -related appliances and licenses spread over five EO data centers. Specifically, only Cisco Sourcefire security devices can provide upstream forwarding of any localized network intrusion activity data into the existing EO Cisco Sourcefire architecture, operate under the same Cisco Sourcefire licensing, and can be managed from the same Cisco Sourcefire central management console. The upstream of data is a VA functional requirement and is critical to produce a single view collective status of all security related activity over the network. This will ultimately provide EO a single interactive view that displays the monitored EO's network's security posture of all network elements of malware protection. Furthermore, any other brand name software cannot accomplish this because another product can neither communicate, nor integrate with the architecture and licensing of, the Enterprise Operations Console, and thus will not allow security visibility of malware activity on the network. Additionally, data monitored and provided by another brand name will not integrate with the existing toolset, which is based on Cisco Sourcefire security architecture and licensing.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in the market research section of this document. It was determined that limited competition is viable among authorized resellers for this effort. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), this action will be synopsisized on the Federal Business Opportunities Page and the justification will be made publicly available within 14 days of award. Additionally, in accordance with FAR 16.505(a)(4)(iii)(A) this justification will be submitted to all applicable NASA SEWP V GWAC holders along with the Request for Quotation in order to fully notify all interested parties.

7. Actions to Increase Competition: In order to remove or overcome barriers to competition in future acquisitions for this requirement, the agency will work with the program office to continue to perform market research to consider and ascertain if any other sources can provide these services in the future.

8. Market Research: The Government's technical experts conducted market research by reviewing other similar malware protection full packet capture systems. This market research is an ongoing process starting in 2012 and continuously being conducted, as recently as January 2015. The other similar software reviewed included International Business Machines Proventia Network IPS, Hewlett Packard Tipping Point IPS, and Palo Alto Networks IPS. Based on reviews of these products, the Government's technical experts determined that none of these products can meet the Government's interoperability and compatibility requirements previously discussed. None of the vendors' devices could function and interconnect with current EO production Sourcefire IPS architecture, licensing and configuration. Additionally, none of these other products can offer the upstream forwarding of localized data into the existing EO Cisco Sourcefire console architecture, which is critical in producing a single view collective status of all Sourcefire security related activity over the network. Review of these products is based on actual VA experience using the competing monitoring software. Additionally, VA networking subject matter experts regularly review industry trade publications and conduct internet research to ascertain if any other brand name software is available. Based on all of these market research efforts, the Government's technical experts have determined that only Cisco Sourcefire security appliance and licensing can meet all of EO's needs.

Additional market research was conducted by utilizing the NASA SEWP V GWAC Provider LookUp tool. There are 122 resellers of brand name Cisco products, with 26 vendors that currently have the requirements listed in their catalog. Therefore, adequate competition is expected.

9. Other Facts: None.