Control Number: TAC-16-35998

JUSTIFICATION
FOR AN EXCEPTION TO FAIR OPPORTUNITY

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

2. Description of Action: The proposed action is for a firm-fixed price (FFP) delivery order (DO) to procure one brand name Cisco Sourcefire FirePOWER 8350 network security Intrusion Prevention System (IPS) appliance inclusive of maintenance and software licenses for VA Office of Information and Technology, Service Delivery and Engineering, Enterprise Operations (EO), Security Division to be 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's Continuous Readiness Information Security Program (CRISP) requires system security monitoring of all system logs and its network connectivity to provide event and log correlation, security event alerting and information security threat intelligence, and reporting of all network intrusion attempt activity. EO Security Division uses an existing Security Information and Event Management (SIEM) solution for data center systems and networks combined with SIEM Intrusion plug-in data feeds from Cisco Sourcefire, collectively referred to as Cisco Sourcefire brand name IPS appliance and software to meet these CRISP requirements. EO data centers support websites, email servers, databases, file servers, and VistA requirements for all of VA: Veterans Health Administration, Veterans Benefits Administration, National Cemetery Administration, and VA Central Office. The infrastructure needs to support Federal Information Security Management Act (FISMA) of 2002 High Impact Level for all EO data centers. In order for EO to manage an expanding user base, the current EO IT SIEM security tools and processes have required expansion. EO currently has six active data centers with Cisco Sourcefire IPS equipment in place and FISMA High capability. In early calendar year 2016 a need to further expand EO Security Division SIEM, including Cisco Sourcefire IPS, was identified, and EO was instructed to provide the same SIEM capability including Cisco Sourcefire IPS at one additonal data center, which also requires FISMA High security controls.

The proposed action is for one Cisco Sourcefire IPS to facilitate the planned expansion to one additonal data center. The additional Cisco Sourcefire IPS will extend security controls required for FISMA High into that additional data center. The brand name item required is one Cisco Sourcefire physical appliance, along with associated maintenance and software licenses to be perpetually assigned to the appliance. The appliance configuration requirements include Cisco AMP FirePOWER 8350 Chassis and Bundle; SMARTnet 8x5xNBD FirePOWER AMP 8350; AAC Power Cord (North America), C13, NEMA 5-15P, 2.1m; Cisco FirePOWER 1000W AC Power Supply; Cisco FirePOWER Software v5.3; Cisco FirePOWER 8350 Control License; Cisco FirePOWER Malware Storage, 8200&8300 Series, SSD 480GB, firePOWER 2-Port 10 Gbps SR Fiber

Network Module with Bypass; SMARTNET 8X5XNBD NetMod 2-Port 10Gbps SR Fiber with Bypass; Cisco AMP8350 IPS Apps and AMP Service Licenses and Service Subscription. VA will be adding to the existing infrastructure, placing the Cisco Sourcefire IPS into one additional data center. Currently this location does not have this capability, and the capability is needed to assist with remediation efforts for national plan of actions. As part of the procurement, a 12-month warranty and perpetual software license requirement is included. The required warranty and maintenance includes 24 hours per day, 7 days per week telephone and email support, software updates, patches and defect support for one year. The period of performance for maintenance under the resulting DO shall be 12 months from date of award. Delivery of the IPS is required within 30 days from receipt of order. 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) 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 extensive market research, as described in paragraph eight of this document, it was determined that limited competition is available for the aforementioned brand name items and services.

Only Cisco Sourcefire can meet all of the Government's requirements. Cisco Sourcefire appliances and software are currently in use providing 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; however, as the user population has grown, additional capacity is needed to accommodate that growth across VA. Only Cisco Sourcefire is compatible with the existing SIEM architecture, and it is the only product capable of supporting the required expansion to EO Security Division's existing Cisco Sourcefire IPS. 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. Therefore, no other brand name intrusion prevention solutions researched are able to integrate with the currently fielded Cisco Sourcefire architecture and Cisco Sourcefire-based intrusion prevention software licensing to support the needed expanded capacity. Additionally, no other brand name IPS has been determined to be interoperable or compatible with the currently fielded Sourcefire-based IPS and Sourcefire brand name architecture.

EO's current Cisco Sourcefire brand name security appliance inventory includes twelve Sourcefire IPS appliances and licenses already implemented over nine EO data centers and three more recently acquired IPS are in process of being racked and stacked (two at new unique locations and one to supplement capacity at an existing data center). All of these either already meet FISMA High requirements or are in the process of being updated to meet them. In addition to the VA's continuous monitoring requirements, this new requirement for one additional Cisco Sourcefire IPS is needed to support the VA's

Information Technology (IT) visibility to the Network initiative, and VA will install install it in one additional VA regional data center location. Specifically, only Sourcefire brand name security appliances can provide upstream forwarding of any localized network intrusion activity data into the existing EO Sourcefire architecture. The upstream forwarding of intrusion activity data is critical to produce a single view collective status of all security related activity over the network. This provides EO a single interactive view that displays the monitored EO network's security posture of all network elements providing malware protection. Furthermore, any other brand name appliance and software cannot provide this functionality because another product cannot communicate, nor integrate with the architecture and licensing supporting the existing Enterprise Operations Console, and thus will not allow security visibility of malware activity on the network. Additionally, data monitored and provided by another vendor will not integrate with the existing toolset, which is based on Sourcefire brand name security architecture and software licensing.

Since Fiscal Year 2013, VA has invested in excess of $3.48 million to develop the existing Cisco Sourcefire IPS architecture. To replace the existing Cisco Sourcefire infrastructure would require a redesign of the entire SIEM, considering not only the SIEM integration with the IPS, but potentially a cascading effect of required redesign of other IT security solutions that are also integrated into the SIEM. This could result in an even greater cost to VA for materials and equipment, and VA staff training to learn how to use the new IT Security systems. Furthermore, VA IT Security Specialists estimate it would require at least 2 years of effort to replace/retool the current CISCO Sourcefire IPS and International Business Machines (IBM) QRadar SIEM production architecture. Introducing alternate products into the existing CISCO and IBM infrastructure would cause system incompatibilities with proprietary licensing/functionality, compromising VA's network security, generate additional VA material weakness remediation deliverable failures, and cause existing approved systems and authority to operate to cease. The entire accreditation process would have to be repeated.

This also aligns with the data center IT Security standard that has been vetted and recorded by regional and national groups. Making a change to IT security architecture at this point would result in a catastrophic outcome to running standards, processes and system controls local within EO and nationally across the regional data centers.

This need for IPS for one additional EO data center was identified early in calendar year 2016. There is no option for transition because of the operational and IT security impact a change like this would cause. The impact would be changes across multiple data centers that are not in the change window for expansion having a critical negative impact on project, staff, VA material weakness remediation, system Accreditation controls, and current yearly VA OIG audit control deliverables. This would impact VA ability to continue to meet Federal Information System and Management Activity (FISMA) High control needs. Failure to procure the required appliances with associated maintenance and software will render VA vulnerable to cyber attacks. Furthermore, there would be delayed incident response, resulting in VA inability to timely understand threats against such cyber attacks as Advanced Persistent Threat, Zero Day, and Command and Control IT Threats. This harms VA's security posture to protect data

centers, networks, and systems, and Veteran personal health and personal identifier information. Based on the above, it has been determined that no other brand hardware, software, or maintenance services can meet the Government's requirements.

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 that can meet the Government's requirements. It was determined however that limited competition is viable among authorized resellers for the required brand name security appliances, maintenance and software. In accordance with FAR 5.301 and 16.505(b)(2), the award notice for this action will be synopsized at award on the Federal Business Opportunities Page (FBO) and this justification will be made publicly available.

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 actions to be competed.

8. Market Research: The Government's technical experts continually conducted market research from October 2015 to February 2016. Market research was completed by reviewing other similar IPS. The other similar software reviewed included International Business Machines (IBM) Proventia Network IPS, Hewlett Packard (HP) 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 with the existing Sourcefire-based infrastructure, nor the upstream forwarding requirement and other requirements discussed in section five above. Cisco Sourcefire has a proprietary management console which coordinates all communication between Cisco devices, and doesn't support non-Cisco devices. The same is true of each of these alternative products the technical experts investigated. If one of these other products were selected to meet the need for expansion of IPS services, then VA would need to procure another proprietary management console for that different brand name product, which could not be synced with the existing Sourcefire appliances. Both solutions would have to run in parallel and would not sync. VA would not be able to receive automated reporting and correlation between the two systems. Based on current infrastructure no other vendor can provide the needed services without stripping out and replacing the entire existing infrastructure and repacing it entirely. This would create a vulnerability in terms of a lapse in EO Security Division's ability to monitor the logs and system. Taking this approach would not only add significantly to the cost of providing these services, but would also require substantially greater manpower to support. Additionally, VA networking Subject Matter Experts regularly review industry trade publications and conduct internet research to ascertain if any other brand name appliances and software are available to meet VA's requirements. Based on all of these market research efforts, the Government's technical experts have determined that only Cisco Sourcefire brand name security appliances, maintenance and software can meet all of EO's needs.

Additional market research was conducted in February 2016, utilizing the NASA SEWP V GWAC provider lookup tool. Based on this research, there are 72 authorized

resellers that offer Cisco Systems, Inc. products. Of the 72, 9 are service-disabled Veteran-owned small business (SDVOSB) Value Added Resellers (VARs) and 8 of the 9 are VA-verified SDVOSBs. The market research results suggest there is a reasonable expectation that two or more quotes will be received from SDVOSB VARs; therefore there is an expectation for limited competition at the reseller level.

9. Other Facts: None.

10. Technical and Requirements Certification: I certify that the supporting data under my cognizance, which are included in this justification, are accurate and complete to the best of my knowledge and belief.

[redacted]

11. Fair and Reasonable Cost Determination: I hereby determine that the anticipated price to the Government for this action will be fair and reasonable. Pricing for products awarded on NASA SEWP V GWAC have already been determined to be fair and reasonable and more competitive pricing is anticipated from competition and discounts among GWAC holders who are resellers of the required brand name Cisco Sourcefire security appliances, maintenance and software. Finally, price analysis shall be conducted by comparing the successful quote to the Independent Government Cost Estimate.

[redacted]

12. Procuring Contracting Officer Certification: I certify that this justification is accurate and complete to the best of my knowledge and belief. As this action does not exceed $500,000, the certification below required by FAR 16.505(b)(2)(ii)(C)(1) and VA Acquisition Regulation 806.304 serves as approval.

[redacted]