

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 delivery order issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Government-wide Acquisition Contract (GWAC) for brand name ForeScout CounterAct appliances, associated software licenses, software maintenance, training vouchers and technical support services.
3. Description of the Supplies or Services: VA, Office of Information and Technology (OI&T), Enterprise Program Management Office (EPMO) has a requirement for brand name ForeScout CounterAct appliances (quantity of five ForeScout CounterAct CT4000 servers and 98 ForeScout CounterAct CT10000 servers); ForeScout End-Point Centralized software licenses; 24 hours a day, 7 days a week (24x7) maintenance for the appliances and software; software maintenance; vouchers for training support, and technical support. The effort also includes optional tasks for additional ForeScout CounterAct appliances (quantity of 50 ForeScout CounterAct CT4000 Servers and 75 ForeScout CounterAct CT10000 Servers), software, software maintenance, training and technical support in order to meet the continuously evolving and expanding cyber-security and network infrastructure high availability requirements. VA currently has 195 ForeScout appliances providing hardware asset management across the enterprise. This effort provides an additional 103 ForeScout CounterAct appliances, upgrades, maintenance support for all devices from 8 hours/day, 5 days/week to 24x7, training to VA engineers, and technical support to implement the new devices to meet VA Continuous Diagnostics and Mitigation program (CDM) requirements. The appliances, software and services are required in support of the joint Department of Homeland Security (DHS) and VA CDM program. DHS has a mission to safeguard and secure cyberspace in an environment where cyberattack threats are continuously growing and evolving. The CDM program seeks to defend Federal Information Technology (IT) networks from cyber-security threats by providing continuous monitoring sensors, diagnosis, mitigation tools, dashboards, and Continuous Monitoring as a Service to strengthen the security posture of Government networks. Congress established the CDM program to provide adequate, risk-based, cyber-security while more efficiently allocating Federal cyber-security resources. Based on the requirements provided to VA by DHS, VA requires additional ForeScout CounterAct appliances, software licenses, training vouchers and technical support in order to implement the necessary cyber-security capabilities. These capabilities include identifying cyber-security risks on an ongoing basis, the ability to prioritize these risks based upon potential impacts to VA infrastructure and mitigating the most critical cyber-security risks first. ForeScout software maintenance shall consist of unlimited phone and email support for software and technical issues 24x7. This support shall also consist of advanced-level software

maintenance which includes any and all manufacturer-released software updates, patches and versions. The Contractor shall provide technical support consisting of subject matter expertise and a ForeScout service account manager to provide project management oversight for deployment services, conduct operational risk mitigation reviews, drive customer escalations as needed, best practice reviews, and deliver insight and planning to VA. The Contractor shall also provide training services. Delivery of the appliances and software items are required within 30 days after receipt of order. The VA has an anticipated need for the aforementioned appliances, software and services for a period of at least five years. The period of performance for the support services shall be 12 months from date of acceptance by VA of the appliances and software. This acquisition will include four 12-month option periods for software maintenance; vouchers for training support, and technical support and an optional task for an additional 125 ForeScout CounterAct appliances, software, software maintenance training and technical support. The total estimated price of the proposed action, inclusive of options, is \$ [REDACTED]

4. Statutory Authority: The statutory authority permitting this exception to fair opportunity is 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 8 of this document, it was determined that limited competition is viable amongst authorized resellers of ForeScout CounterAct appliances, associated software licenses, software maintenance, training, and technical support services. The required ForeScout CounterAct appliances, software and support are an integral part of the CDM solution. These devices fortify the cybersecurity of Government networks and systems. This effort is to acquire additional ForeScout CounterAct appliances, associated software licenses, software maintenance, training, and technical support services to meet the evolving needs of VA. These items must be able to work within the existing VA CDM infrastructure. Due to the proprietary nature of the asset monitoring and management hardware and software code in the existing EPMO CDM environment, which is comprised of ForeScout CounterAct appliances and the associated software licenses, only ForeScout appliances and software will meet VA's requirements due to compatibility and interoperability constraints within the existing infrastructure. The existing infrastructure is comprised of ForeScout appliances and software that has been configured, integrated and tested to provide VA with the ability to maintain an integrated, seamless view of network data and network performance across the VA IT infrastructure as well as to monitor cyber-security threats. The ForeScout appliances identify any internet protocol addressable device connected to the VA network and to determine if it is authorized or unauthorized on the network. This complete view of the network is necessary to support the VA mission due to multiple incomplete streams of data requiring separate management and integration, which could result in an inability to triage and troubleshoot cyber-security threats across the entire infrastructure. Only ForeScout or an authorized reseller can provide the necessary ForeScout appliances, software and support services. No other manufacture's appliances or software licenses

are compatible, functional, or interoperable within the existing ForeScout based infrastructure. Specifically, any other brand name items will not communicate with the existing infrastructure due to the aforementioned proprietary constraints.

Additionally, the ForeScout appliances and software are proprietary products; therefore, only ForeScout or its authorized resellers have the access to the proprietary data and source code necessary to provide maintenance and technical support services required to sustain this system. The proprietary code is required to ensure the appliances and software are properly operational and defects properly resolved. Access to ForeScout proprietary data and source code is required to provide the required maintenance and technical support services. Only ForeScout or an authorized reseller can provide the support services due to the proprietary source code required to develop and implement software upgrades and updates.

If the ForeScout appliances, software and support services are not acquired, there will be an immediate risk to the EPMO applications operating across the enterprise. ForeScout appliances, software and support services are vital to VA for the sustainment of the VA's cyber-security monitoring and to continue to meet the needs of current and planned DHS and VA CDM program 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 brand name appliances, software and support services. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), this action will be synopsisized and the justification will be made publicly available on the Federal Business Opportunities Page within 14 days of award of the order, and this justification will also be posted to the NASA SEWP V GWAC website along with the Request for Quotation.

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 perform additional market research in a timely manner so that alternate solutions can be considered should they become available.

8. Market Research: The Government's technical experts conducted market research in March 2017 to ascertain the ability of any other source to provide the aforementioned appliances, software and support services. The research consisted of reviewing various applications, software and maintenance plans including those offered by Cisco, Aruba and Portnox. All of these applications, software and support services lack the compatibility and interoperability with the ForeScout products within the existing infrastructure. Based on the market research conducted by the Government's technical experts, it has been determined that no other brand of appliances, software and support services can meet the Government's requirements due to the need to access the source code and other proprietary data of the existing ForeScout appliances, software and support services. Unauthorized software providers do not have access to the proprietary data of the software to be able to provide troubleshooting, updates, fixes,

patches, and upgrades. Only ForeScout or its authorized resellers have access to the source code of the software to provide the necessary support.

Additionally, the Government's technical experts conducted market research through the issuance of a Request for Information (RFI) on NASA SEWP V GWAC website. The RFI was released on March 16, 2017 and closed on March 23, 2017. Seven responses were received. Six responses were from Service-Disabled Veteran-Owned Small Business (SDVOSB) concerns in Group B(2) and one response was received from a Small Business in Group C. The technical experts performed an analysis of the quotes received and determined that all of the quotes met the requirements detailed in the draft Product Description. Additional market research was conducted through the utilization of the NASA SEWP V GWAC Provider Lookup Tool. The Provider Lookup Tool yielded 57 contract holders that can provide the required ForeScout appliances, software and support services. Of the 57 contract holders, 13 are SDVOSBs. A search was performed to confirm that there were two or more from Group B(2) SDVOSB that were registered and verified in Vendor Information Pages (VIP) database (<http://www.va.gov/OSDBU/index.asp>). The results of that search identified that there were two or more SDVOSBs that are registered and verified in VIP. Based on the results of the market research, there is reasonable expectation that limited competition exists among SDVOSB concerns in Group B(2). Therefore, the request for quotation for this requirement will be submitted to Group B(2) SDVOSB GWAC holders under North American Industry Classification System code 541519.

9. Other Facts: None.