

JUSTIFICATION
FOR AN EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Procurement, 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 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 brand name Trustwave Holding Inc. (Trustwave) DbProtect Vulnerability Management software licenses and maintenance support.

3. Description of the Supplies or Services: Office of Information and Technology, Network Security Operations Center (NSOC) requires an additional 2,000 brand name Trustwave DbProtect Vulnerability Management software licenses with maintenance support. DbProtect software is currently implemented in combination with Trustwave's AppDetective Pro (ADP) as part of VA's database threat protection platform to audit database security across the enterprise. Trustwave ADP is limited in its ability to scale to large enterprises, is decentralized in its stored data design, and can only audit a finite number of databases, and therefore, VA previously procured 7,000 DbProtect Vulnerability Management software licenses in 2016. DbProtect is a database security, risk and compliance platform designed to meet the needs of large enterprises. DbProtect risk management framework, security controls, controls monitoring, and governance make it a comprehensive database security solution. DbProtect Vulnerability Management software also provides for real-time/overall risk assessment across all VA database management systems; continuous security monitoring; a console with an enterprise vulnerability management view; centralized report management; enterprise scalability for multiple users; centralized scan management and creation; centralized user role based access and management; load balancing; a centralized repository; and credentialed management. DbProtect is licensed based on the number and type of database applications to be protected, and the Government requires an additional 2,000 Vulnerability Management software licenses to support an increase in applications across the enterprise. The required maintenance support shall provide product code/vulnerability database updates, monthly updates to DbProtect's Shatter Knowledge database, and technical support during normal business hours. A complete license file shall be delivered upon renewal of all required licenses and maintenance support within seven (7) days of award and the period of performance for the required software maintenance shall be 12-months. [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 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 among authorized resellers for the brand name Trustwave DbProtect Vulnerability Management software licenses and maintenance support. VA's existing database threat protection platform consists of an unlimited license of Trustwave's ADP Vulnerability Assessment software and 7,000 DbProtect licenses. The VA-NSOC and its IT security partners' database scanning infrastructures are based upon this existing Trustwave proprietary software and VA requires additional Vulnerability Management software licenses that are compatible and interoperable with VA's existing Trustwave infrastructure to allow for seamless integration with existing database scanning protocols. No other brand product is interoperable with the existing Trustwave database structures and software application programming interfaces utilized by the existing ADP and DbProtect Vulnerability Management software due to proprietary constraints. Introducing any alternative software would not permit the seamless integration of years of vulnerability data collected by NSOC and its IT security partners in support of database security audits across the enterprise, and will compromise the integrity of the database scan results. A new alternative solution would necessitate the total reconstruction of VA's database threat prevention platform, and would result in replacing the existing 7,000 DbProtect licenses and ADP licenses, which is estimated to take 3 to 5 years and \$40 million to complete. Specifically, a new solution would require requirements analysis and replacement of the existing hardware infrastructure and software licenses including installation, configuration, testing and deployment across the enterprise. In addition, various applications that currently interface with the software, including the Nessus Enterprise Web Tool which monitors password vulnerabilities, are only coded to work with the Trustwave software. Use of any other brand name software would result in extensive delivery days in addition to duplicative costs that would not be recovered through competition.

Additionally, to provide the required updates, patches, and bug fixes, access to Trustwave's proprietary software code is required. Failure to acquire the maintenance support for the new licenses could cause system failures, and put enterprise data currently being backed up and restored, including internal VA information, at risk of being compromised.

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. It was determined that limited competition is viable among authorized resellers for the required brand name Trustwave DbProtect Vulnerability Management software licenses and maintenance support. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), notice of award for this action will be synopsized and this justification will be made publicly available on the Federal Business Opportunities Page within 14 days of award. In accordance with FAR 16.505(a)(4)(iii)(A), this justification will be posted with the request for quotation on the NASA SEWP V GWAC to notify interested parties.

7. Actions to Increase Competition: In order to remove or overcome barriers to competition on future acquisitions for this requirement, the agency will continue to

perform market research to consider and ascertain if there are changes in the marketplace that would allow other brand products to work with the existing Trustwave infrastructure, thus enabling future actions to be fully competed.

8. Market Research: The Government's technical experts conducted market research in June 2018 by reviewing similar software to ascertain if these items could meet or be modified to meet VA's requirements. Specifically, the Government's technical experts conducted web-based research of vulnerability software available from Imperva, IBM, McAfee, and Tenable Network Security products. The market research confirmed that no other software is compatible and interoperable with VA's existing Trustwave infrastructure to allow for seamless integration with VA's existing database threat protection platform. Further, only Trustwave or an authorized reseller can access the proprietary source code in order to provide the required maintenance support.

Additionally, market research was conducted in June 2018 utilizing the NASA SEWP V GWAC Provider Look-up tool to ascertain the extent of limited competition among resellers. The results of the search found that there are numerous resellers of Trustwave products that could possibly meet VA's needs, including seven (7) Service-Disabled Veteran-Owned Small Businesses. Therefore, limited competition is anticipated.

9. Other Facts: None.