

JUSTIFICATION FOR OTHER THAN FULL AND OPEN COMPETITION

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 the issuance of a sole source Firm-Fixed Price contract for the procurement of Eagle 6 modeling software licenses and services in support of the Veterans Information System and Technology Architecture (VistA) Security Remediation (VSR) and VistA Standardization and Virtualization (VSV) projects under the VistA Evolution Program.
3. Description of the Supplies or Services: VA Office of Information & Technology, Enterprise Program Management Office (EPMO) has a requirement for the procurement of up to 2,400 licenses of brand name Eagle 6 modeling software. Ancillary services such as maintenance, warranty, and technical support are also needed along with extended software development and engineering services. Technical support includes installation and configuration of the software, development of the VistA model, and creation of reports and dashboards. Extended services encompass enhancement of data modeling, continuous enhancement of rules, creation of reports and dashboards, mentoring and regular periodic training of VA staff and operation of the software modeling tool by subject matter experts to accomplish project objectives. The contractor will also provide continuing engineering services to update and maintain the model.

VistA is an enterprise-wide system developed using the Massachusetts General Hospital Utility Multi-Programming System (MUMPS) programming language. The Eagle 6 software will provide tools to the VSR and VSV projects to model and analyze VistA's MUMPS software and configuration. Eagle 6 software identifies vulnerabilities in VistA MUMPS code, VistA Delphi code and Class III code along with VistA business processes that may degrade the performance and security of the VistA system. It is also able to compare different versions of VistA MUMPS code (M code), such as from multiple sites to determine variations in software and configuration to prevent interoperability issues and to ensure security patches have been updated at multiple sites. For VSR, the tool will identify vulnerabilities in the software, provide reporting and dashboards to manage those vulnerabilities and determine which routines, libraries, applications and business processes make use of the vulnerable software. VA's Assessment and Authorization Standard Operating Procedures for systems and applications requires VA to scan code for vulnerabilities and compliance with federal laws, regulations and security guidelines. Critical to managing the resolution of vulnerabilities is the ability to identify the underlying laws, regulations, standards or guidelines that are related to the vulnerabilities. This allows vulnerabilities to be prioritized for remediation and provides necessary information to guide technical experts remediating the vulnerability. For VSV, the tool will compare the 130 product VistA instances operations across the VA enterprise against the model to identify variations in

deployed applications and local configuration to enable the standardization of all systems. In addition to identifying vulnerability and standardization issues, the tool will support the remediation of the identified issues by mapping affected MUMPS routines to programmatic interfaces and business processes allowing VA to determine what business processes are affected by the issue. Further, the tool will identify all issues associated with a business process so that all issues can be remediated as a single work effort thus minimizing disruption to that operating instance of VistA.

The contract period of performance is one base year and two option years. Under the base period VA may procure up to 2,400 licenses with associated support services. The two option years will allow VA to renew only these licenses and continue associated support services. The total estimated value of the proposed action is (inclusive of options).

4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 3304(a)(1) as implemented by the Federal Acquisition Regulation (FAR) Subpart 6.302-1, entitled "Only one responsible source and no other supplies or services will satisfy agency requirements."

5. Rationale Supporting Use of Authority Cited Above: The proposed source for this action is Rivera Consulting Group, 7060 SR311, Sellersburg, IN, 47172. Based on market research, as described in section 8 of this document, it was determined that Rivera Consulting Group, a VA verified Service-Disabled Veteran-Owned Small Business (SDVOSB), and the developer of Eagle 6 software is the only source capable of providing a product meeting VA's requirements as described in section 3 above for vulnerability and standardization scanning of MUMPS software code in VistA.

Eagle 6 is the only modeling software that can scan VistA MUMPS software code, VistA Delphi code, Class III code against VA coding security standards and identify where Class I and Class III code violates VA's security standards and meets all of the VA functional requirements. Specifically, VA requires software that can identify vulnerabilities, assign vulnerability identifiers and correlate those identifiers with compliance with federal laws (e.g. Federal Information Security Management Act and Health Insurance Portability and Accountability Act), regulations, standards and guidelines (e.g. National Institute of Standards and Technology Special Publication 800 series). Eagle 6 is the only software that can meet the VA's requirement to identify vulnerabilities and correlate those identified vulnerabilities specifically to the applicable federal laws, regulations, standards and guidelines.

Additionally, Eagle 6 is the only tool with the ability to map identified vulnerability issues to business processes, which are also critical VA functional requirements. Eagle 6 maps the business process through the logical path in the MUMPS code to allow each single business process to be efficiently remediated as a logical unit of work such that business disruption does not occur during remediation (i.e. remediate all issues in an business process at one time). Eagle 6 software tools can link business processes to application (M code) behavior and when a change is made to a line of code it has the ability to identify the impact of the change to associated business processes. Eagle 6 is

the only software that supports the remediation of the identified issues by mapping affected MUMPS routines to programmatic interfaces and business processes to meet all VA requirements.

Furthermore, Rivera Consulting Group is the original developer of the Eagle 6 software and associated tools and the only source that can provide the required support services associated with the Eagle 6 tool. No other source can provide the aforementioned support services including installation, configuration, model development, training, technical support, and engineering services given that the source code for Eagle 6 is proprietary to Rivera Consulting Group. These services are required to ensure the VA can effectively apply the tool to address the complex security and standardization requirements for VistA.

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. In accordance with FAR 5.2 and 6.302-1, the pre-solicitation and award notices for this action will be synopsized on the Federal Business Opportunities Page and this justification will be made publicly available with the award notice within 14 days of award.

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 future actions to be competed.

8. Market Research: In April 2017, the Technology Acquisition Center issued a Request for Information (RFI), number VA118-17-N-2018. This RFI sought a mapping of product capabilities to three categories of VistA Evolution requirements including Data Dictionary Analysis and Remediation, Code Analysis and Convergence, and Security Analysis. The purpose of this RFI was to determine if there was one vendor who could address analysis requirements for all three categories of requirements needed across the VistA Evolution program. While there was overlap in capabilities, no single vendor could fully address more than one of these categories of the RFI, therefore, in order to enhance competition, the requirements for the Security Analysis was broken out into this separate procurement.

A second RFI was issued on July 23, 2017 under RFI number VA118-17-N-2347, titled MUMPS Security Remediation and it focused on the VA's Security Analysis requirements to elicit sources for tools to address requirements for Mumps Scanning Tools to address VSR, VSV requirements for VistA MUMPs code analysis.

Rivera Consulting Group (SDVOSB) proposed Eagle 6 software. Rivera Consulting Group stated that they met all of the requirements in the RFI. Eagle 6 has been tested and reviewed in the VA Center for Innovation laboratory. The software was installed on a test system and mapped VistA MUMPs code. It was able to identify lines of unused code which testers verified through inspection. Based on the technical analysis of the RFI response by the VA technical experts, it was determined that Rivera Consulting Group's Eagle 6 software meets VA's requirements.

Inverness Technologies (SDVOSB) did not respond to the July 23 RFI, but in its response to the April 2017 RFI, it offered the VistA Advanced Analytics (VAA) tool to meet the Security Analysis requirement. Based on the technical analysis of their response to the initial RFI, it was determined that the proposed VAA tool only partially met the stated requirements of the original RFI, but further clarification was needed. Inverness Technologies (Inverness) was contacted on August 7, 2017 to ensure that they were aware of the second RFI for the Security Analysis requirement and to provide additional clarification with regard to the two areas in the security portion of Inverness' response to the original RFI. Specifically, clarification was needed to determine if the VAA tool could possibly meet all of VA's security requirements. Inverness Technologies stated that the VAA tool did not map software components to business processes or track and update security vulnerability identifiers. Inverness stated the VAA only mapped the relationships of the software components. Therefore, it was determined that Inverness could not meet all of the VA's security requirements.

Rivera Consulting Group was the only vendor to respond to the July 23, 2017 RFI and indicated that they were able to meet all stated requirements. Therefore, based on the above market research, it was determined that only Rivera Consulting Group's Eagle 6 software fully met VA's requirement for VistA MUMPs code analysis.

9. Other Facts: Not applicable.

