Cyber Security Operations Center Next Generation (CSOC-NG) Support Extension

Control Number VA-23-00066196

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 sole source action is for a modification to a Firm-Fixed-Price (FFP) Task Order (TO) 36C10B18N10020010 issued under Transformation Twenty-One Total Technology Next Generation (T4NG) Contract VA118-16-D-1002 with Science Applications International Corporation (SAIC), 12010 Sunset Hills Rd, Reston, VA 20190. The purpose of this modification is to extend the period of performance of Option Period Four and Optional Tasks One through 12 for three months for the continuation of Cyber Security Operations Center Next Generation (CSOC-NG) Support. This extension will serve as a bridge of support until a new competitive TO is awarded.

3. Description of the Supplies or Services: The scope of the CSOC NG Support TO is to provide comprehensive information and cyber security support services to the Department of Veterans Affairs (VA) CSOC to assist in developing and providing enterprise wide information and cybersecurity and network defense services, as aligned with the VA Office of Information & Technology (OI&T) security configuration and interoperability of VA CSOC managed tools/devices and information security privacy goals, and to provide expert advice on the best utilization of the software, tools, and procedures used to perform all functions in this TO. This support consists of over 145 contractor staff supporting 5 core teams responsible for enterprise cybersecurity, incident response and investigation, analytics, security modeling, reporting, assessing and network monitoring. The work provides a substantial portion of the VA CSOC teams composition including a 24/7/365 presence for incident response. The scope of VA CSOC NG also includes functions of threat intelligence, technical services, research and development, data analytics, metrics and reporting, scanning and assessments across the enterprise. The overall support for CSOC NG as outlined in the TO Performance Work Statement (PWS) is critical to ensure the confidentiality, integrity and availability of VA information, systems and applications to the staff that utilize them and the Veterans who rely on VA for continued care. CSOC requires that the current services outlined above and in the PWS, Option Period Four and Optional Tasks One through 12, under TO 36C10B18N10020010 continue without interruption to prevent a negative impact to CSOC, VA's overall cybersecurity posture, and Veterans. The overall period of performance shall be extended from 60 months to 63 months and will commence September 4, 2023 and go through December 3, 2023. The total estimated value of the proposed action is $[redacted]. However, there are unused months in Optional Tasks One through 12 from the original TO award that will cover the three month extension cost for the optional tasks. As such, the overall TO value is estimated to only increase by $[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) 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: The proposed source for this action is SAIC, 12010 Sunset Hills Rd, Reston, VA 20190. SAIC is the current Contractor on the CSOC-NG Support TO. On August 31, 2018 the TO was awarded with a 12-month Base Period beginning on September 4, 2018, with four 12-month Option Periods and twelve Optional Tasks. Subsequently, on August 1, 2022 the final option period and optional tasks were exercised and currently expire on September 3, 2023. VA is in the process of competitively awarding a new TO. The requirement development for the competitive TO began in the first quarter of Fiscal Year (FY) 2023, however, solicitation release is anticipated by mid-August with award currently projected by late September/early October 2023. This is at least three weeks beyond the current TO expiration date. This projection is a best case scenario which assumes a manageable number of proposals being received, no significant additional questions on the solicitation requirements, no proposal extension requests, limited or no discussions, etc. Once the competitive contract is awarded, there is also a need for at least 45 days of overlap to support a seamless transition of the services to a new vendor. For these reasons, CSOC requires support provided by SAIC beyond its current end date of September 3, 2023. SAIC is currently performing all the cybersecurity support services, as described in Section 3 above, for CSOC-NG under this effort and is currently meeting the requirements of the TO. Without this continuation of services, VA faces a gap in service for the critical cybersecurity support provided under the current TO, 36C10B18N10020010, which would negatively impact VA’s cybersecurity posture and detection and response actions while the new TO is awarded. This extension will ensure continuity of VA’s cybersecurity defenses, monitoring, investigation, remediation support, as well as continued compliance with Federal mandates and mandatory Federal reporting and a seamless transition to a new vendor. Any interruption of these tasks executed by the SAIC CSOC-NG Support team supporting VA would immediately result in Federal reporting non-compliance and direct impacts to the VA network which would allow adversarial access, and degradation of systems, services and applications VA-wide which would severely and negatively affect the confidentiality, integrity, and availability of VA information, systems, and applications, ultimately impacting VA’s public image and care to Veterans. CSOC is responsible for the monitoring, analysis, and action on over 2.1 trillion events per month, leading to 15,912 alerts per month, which result in 266 cyber investigation tickets per month. Any impact to the ability to review and analyze these alerts presents an imminent threat to VA and Veterans who rely on the security of VA’s information, systems, and applications for continued and quality care.

A Request for Information (RFI) was posted on the Contract Opportunities site via SAM.gov on May 11, 2023. On June 2, 2023, 25 responses were received as well as 63 questions and recommendations on the Performance Work Statement (PWS). While addressing the questions, there were numerous changes required to the PWS and

IGCE to better refine the Government's requirements to maximize potential competition for a FFP type order. Additionally, there were several changes due to work being incorporated into the recompete PWS for VA Cybersecurity Center Next Generation II (CSOC NG II) Support that was not in the current TO, and will not be part of the bridge extension modification. The combination of addressing the RFI questions and recommendations, carrying over the resultant answers to the PWS, and updating the applicable acquisition package documentation due to the unanticipated changes in CSOC NG II took much longer than originally anticipated, causing delays in completing the acquisition package. As such, the recompete TO will not be awarded prior to the current TO with SAIC ending, which would result in a gap of critically required services. Loss of SAIC support during this gap will result in an enterprise-wide security compromise to all information systems. Therefore, VA requires continued support with SAIC to ensure all VA networks are compliant and prevent any adversarial access. VA anticipates award of a competitive TO in late September/early October of 2023 which would encompass the services detailed in Section 3.

Based on market research which can be found in Section 8 of this document, it was determined that SAIC remains the only responsible source capable of satisfying VA CSOC-NG Support requirements within the required timeframe, until a follow-on TO is awarded and an orderly transition can occur. No other source can provide the aforementioned support or continuity of services required as a result of the delays in the award and execution of the new TO. This extension will provide for the timely continuance of this critically needed support in order to ensure there is no gap in service, where this continuance is crucial to ensuring continued daily operations of VA's cybersecurity capabilities.

Additionally, there are critical custom enterprise-wide dashboards and reports which require elevated privileges and in some cases tokens for access, which is not available with any immediacy, that rely upon the technical expertise and VA specific knowledge of a subset of SAIC contractors in order to maintain functionality and provide maintenance; any impact to the level of support for these dashboards and reports would result in VA failing to comply with Cybersecurity and Infrastructure Security Agency reporting requirements and other Federal and VA Mandates. Over the years VA CSOC has developed a very specific toolset in order to maintain operations and meet the mission, a new vendor, without intimate VA knowledge would not be able to correctly utilize the toolset (e.g.: Splunk, Tenable, Swimlane, and Microsoft Defender for Endpoint) and apply the outputs to the appropriate processes/procedures until after a lengthy timeframe, which will have cascading negative effects across VA, resulting in adversarial infiltration, loss of VA data and impacts to patient care. Interruption of any of the above mentioned critical operational activities and essential service tasks executed under the existing TO with SAIC would immediately prevent VA CSOC from having the 24/7/365 support necessary to remain operational. Any source, other than SAIC, would require a ramp-up period of approximately 45 days to onboard and/or transition appropriate staff, obtain necessary permissions and access to VA systems, recruit and train staff with the appropriate skill sets and properly transition all required tasks and workloads. This 45 day onboarding time period is based on past experience on this effort and similar Office of Information Security support contracts. Failure of VA

CSOC to provide all current functions or to be unable to fully staff those functions until such a time as a follow-on TO and an orderly and complete transition can occur between VA, SAIC, and the new TO awardee will cause undue negative impacts to VA such as an influx of uncontained cyber-attacks, Federal mandates being missed, and cyber threats going unmitigated, all of which can and will result in Congressional inquiries to the Agency. As such, it is in the best interest of the Agency to extend the current TO with SAIC to ensure continuity of services. The 3-month extension accounts for the time needed to have a new TO awarded as well as the 45 days needed for the transition period.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in Section 8 of this document. This effort did not yield any additional sources that can meet the Government's requirements. There is no competition anticipated for this acquisition. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), the award notice for this action will be synopsized on the Contracting Opportunities website, SAM.gov and the justification will be made publicly available within 14 days of award.

7. Actions to Increase Competition: No barriers to future competition are anticipated. A competitive contract is anticipated to be awarded in late September/early October 2023 and future acquisitions will be awarded on a competitive basis.

8. Market Research: This requirement is leveraging market research conducted in May 2023 as part of the competitive procurement which includes support for the same services. The Small Business Administration's Veteran Small Business Certification (VetCert) database for the identification of prospective Service-Disabled Veteran-Owned Small Businesses (SDVOSBs) and Veteran-Owned Small Businesses (VOSBs) under North American Industry Classification System code 541512, Computer Systems Design Services, was reviewed. The VetCert database search yielded 3782 SDVOSB and VOSB vendors that can potentially provide the required services under that NAICS code. As a result, further market research was conducted. On May 11, 2023, a RFI was issued on the Contract Opportunities site via SAM.gov, requesting technical information necessary to determine capable vendors of providing the required services. On June 2, 2023 the RFI closed and 25 RFI responses were received to include nine large businesses: Leidos, Inc., Raytheon Technologies, Inc., Science Applications International (SAIC) Corporation, Favor TechConsulting (FTC), International Business Machines (IBM) Corporation, General Dynamics Information Technology (GDIT), Inc., Zscaler US Government Solutions, SOS International LLC (SOSi), and ECS Federal (ECS), LLC; Ten SDVOSBs: Sapphire Innovative Solutions Inc., The JAAW Group, Insignia Technology Services, Greenbrier Government Solutions, Maveris, LLC, Sierra 7, Inc., MBL Technologies (MBL), Inc., Tangent Technologies, LLC, Information Management Resources (IMRI), Inc., and The Cyber Security Architecture Strategy Engineering (C.A.S.E) Group; Two VOSBs: CSIOS Corporation (CSIOS), and True Zero Technologies, LLC.; Four 8(a): RV Global Solutions, Inc., SRR International, Inc., EvoTech, LLC, and MSM-Net, Inc. Of the 25 responses, two SDVOSBs were found to be fully capable of performing the technical requirements, Greenbrier Government Solutions and Maveris, LLC, and 23, including SAIC, were determined not to be capable based on the capability statements provided. SAIC is currently performing the CSOC-

NG services, however, CSOC NG II PWS presented in the above referenced RFI, while similar in scope, is far more robust, complex and technically detailed than the current TO PWS and includes new tasks that SAIC is not currently performing. While Greenbrier Government Solutions and Maveris, LLC would be capable of meeting the requirements due to its similar general capabilities, they would be unable to provide seamless support by September 4, 2023 due to lack of TO award and transition in/out time.

This market research supports a VA determination that only SAIC is capable of providing continued CSOC-NG services until award of the competitive contract. Only SAIC has the technical expertise and experience that can meet VA's needs in the required timeframe for seamless continuation of cybersecurity services for VA, consisting of all technical activities described in Sections 3 and 5 above until the new contract with expanded scope is awarded. The competitive contract is currently projected to be awarded in the late September/early October 2023 timeframe. This extension will provide for the timely continuance of this critically needed support in order to ensure there is no gap in service.

9. Other Facts: None.