GENERAL SERVICES ADMINISTRATION (GSA)
ASSISTED ACQUISITION SERVICES (AAS) REQUEST FOR INFORMATION (RFI)
TO
VETS 2 CONTRACT HOLDERS

I. Introduction

General Services Administration (GSA) Assisted Acquisition Services (AAS) is releasing this Request for Information (RFI) on behalf of United States Southern Command (USSOUTHCOM). The purpose of this RFI is to assist the Government in conducting market research focused on identifying VETS 2 contract holders. This information will be used for market research only. The Government is not obligated to release a future solicitation.

This RFI does NOT constitute a Request for Proposal and is not to be construed as a commitment, implied or otherwise, by the Government that a procurement action will be issued. Response to this notice is not a request to be added to a bidders list or to receive a copy of a solicitation. No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of the submission of the requested information. No reimbursement will be made for any costs associated with providing information in response to this announcement and any follow up information requests. Responses to this RFI may be considered in the future determination of an appropriate acquisition strategy for the program. The Government may not respond to any specific questions or comments submitted in response to this RFI or information provided as a result of this request. Any information submitted by respondents as a result of this notice is strictly voluntary.

II. Invited Respondents

The Government is seeking responses from prime awardees on the VETS 2 GWAC vehicle.

III. Background

Joint Chiefs of Staff, directorate, J6 has an enduring need for the implementation and sustainment of the United States (U.S.) and partner nation Information Technology (IT) and the execution of full- spectrum operations in the USSOUTHCOM Area of Responsibility (AOR). USSOUTHCOM is one of eleven combatant commands (COCOMS) located in Doral, Florida. USSOUTHCOM is responsible for providing contingency planning, operations, and security cooperation in its assigned area of responsibility (AOR). The AOR consists of 31 countries, twelve dependencies, and areas of special sovereignty. This AOR covers Central America, South America, and select countries in the Caribbean (partner nations). USSOUTHCOM's mission is to provide force protection of U.S military resources at these locations and for ensuring the defense of the Panama Canal. Additionally, it is USSOUTHCOM's responsibility to deter aggression, defeat threats, rapidly respond to crises, and build regional capacity, working with U.S. allies, partner nations, and U.S. government (USG) team members to enhance security and defend the U.S. homeland and its

interest. J6 is responsible for the development, implementation, operation, maintenance and security of communication systems to enable USSOUTHCOM and its subordinate elements to exercise full C4I (Command, Control, Communications, Computers, and Intelligence) capabilities in execution of their assigned missions.

IV. Scope

The Government anticipates awarding a task order for IT & Cyber Services that will be solutions oriented and outcomes based. These outcomes are anticipated to be measured by successful employment of seamless, interoperable, resilient, cyber-informed information technology capabilities, in accordance with USSOUTHCOM strategic, operational, and tactical objectives. All capabilities will be expected to include robust configuration and change management through every stage of service delivery and account for all associated people, processes, and technology. Additionally, all capabilities will be expected to include cyber-informed architectures and activities including mission relevant terrain in cyberspace and mission defense plans. The contractor will be expected to use innovative technologies to reduce the total cost of ownership and increase return on investment (ROI). These efforts will be expected to include identifying, researching, testing, and recommending emergent technologies to meet identified USSOUTHCOM capability gaps, Government and DoD mandated improvements, and strategic directives. The contractor performing the USSOUTHCOM Cyber Information Technology Enterprise Services (SCITES) 2 TO will also be expected to maintain, improve, secure, defend, and provide IT services for the entirety of the DoD Information Network Area of Operations SOUTHCOM (DAO SOUTHCOM) operating environment. Finally, the contractor is expected to facilitate seamless and interoperable extension of IT and cyber capabilities through effective coordination and communication across multiple echelons of the command, mission partners, interagency, and foreign partners.

Note: Interested vendors are advised that portions of this effort require onsite availability 24 hours per day, seven days per week across the USSOUTHCOM AOR. For example, the Joint DoDIN Operations Center (JDOC) requires this type of availability.

V. Anticipated Task Areas

This requirement is anticipated to be broken into seven task areas:

TASK 1 – PROGRAM MANAGEMENT

The contractor will be expected to provide program management throughout the USSOUTHCOM AOR, including multiple OCONUS locations. The government expects the contractor to provide proactive and integrated program management that fosters an information environment that is seamless and integrates with all levels of the command. The contractor's program management strategy is expected to ensure that enterprise IT core capabilities are maintained, that all aspects of the IT service portfolio and lifecycle are cyber-informed, and that robust configuration management is integrated at every phase of project execution. USSOUTHCOM expects program management responsibilities to include oversight of all activities performed by contractor personnel, including subcontractors, to

satisfy the requirements identified in this RFI, including management, scheduling, administration, oversight of all locations, reporting, and staffing requirements. This task includes many subtasks such as accounting for servicing contract reporting, coordinating a project kick-off meeting, preparing monthly and weekly status reports, coordinating assorted meetings, preparing and updating a Project Management Plan (PMP) that includes an Integrated Master Schedule (IMS), providing on-site project management, preparing trip reports, providing quality management, ensuring quality control and quality assurance, providing change management, providing transition-in and transition-out processes for various locations, and providing schedule management on a global scale.

TASK 2 – SERVICE STRATEGY

The contractor is expected to develop, implement, and continually manage cyber-informed IT service strategies. The contractor is also expected to enable portfolio management by continually informing the entirety of the USSOUTHCOM planning, programming, budgeting & execution process (PPB&E). The service strategies are anticipated to ensure robust configuration management that is predictable and authoritative at every phase of the IT service life cycle, balances the existing operating environment with future requirements, drives proactive decision making, and enables the contractor to respond to unpredictable world events. The contractor providing services is expected to ensure all strategies align with relevant USSOUTHCOM decision frameworks, promote collaboration, and result in effective communication with Government decision makers. Finally, it is expected that strategy execution will drive measurable efficiencies, increase effectiveness, and provide measurable returns on investment.

TASK 3 – SERVICE DESIGN

These services are anticipated to ensure designs align and match current and future DoD and USSOUTHCOM requirements. The contractor's approach is expected to account for the receipt of new requirements, the continuous evaluation of existing requirements and service catalogs, revisions to requirements and service catalog, the deployment and divestment of service design offerings, and the integration of relevant data into a USSOUTHCOM data bus. The contractor providing services is expected to identify mission relevant terrain in cyberspace and where relevant include mission defense plans. Additionally, the contractor is expected to develop Service Design Packages (SDP) that enable continual evaluation of the existing requirements and service-catalogs and integrate cyber-informed strategies into the operating environment. The designs are expected to include robust configuration management that accounts for people, processes, and technology. Furthermore , all designs are expected to be resilient, operationally informed, and when appropriate account for continuity of operations. As a result of these efforts, the contractor providing services is expected to create seamless interoperability throughout the USSOUTHCOM environment and across all echelons of the USSOUTHCOM command, and, when applicable, with interagency and foreign partners.

TASK 4 – SERVICE TRANSITION

The contractor is expected to manage services as they move from concept to production within DAO USSOUTHCOM. The contractor is expected to oversee and execute the implementation or decommissioning of services or service components and make modifications to services because of required corrective actions or to improve an existing service. All service transition activities are expected to be mission effective, fiscally efficient, resilient, proactive, and cyber informed. The contractor providing services is expected to test all relevant aspects of operations against key performance parameters and interoperability standards. All transition activities need to be interoperable with all echelons of the command and mission partners seamlessly integrating into the operating environment. The contractor is expected to manage the accountability and retirement of deprecated infrastructure and services in a timely and efficient manner. Furthermore, the contractor is expected to ensure appropriate configuration management repositories and processes are updated and fully integrated into each step of any service transition and that critical functions are not disrupted. Overall, the successful execution of this task is expected to maintain the integrity and effective control of services reducing the risk of unintended consequences during change execution.

TASK 5 – SERVICE OPERATION

The contractor is expected to ensure seamless, compliant, and secure operations of existing, new, and updated IT services. Service operation efforts are expected to be fully integrated into existing configuration management and data-centric processes to ensure mission effectiveness and fiscal efficiency. Furthermore, service operations are expected to be cyber-informed, aligned with Continuity of Operations (COOP) strategies (when applicable), and enable effective DoDIN and defensive cyber operations. The contractor performing this task is expected to make use of all available sensors in the operating environment to drive proactive reporting and decisions. Additionally, the contractor is expected to integrate government evaluation and feedback through user experience and customer advocacy. Overall, these efforts are expected to enable command and control for DoDIN operations activities and enable DoDIN operations at the timing and tempo of mission commanders that are executed across DAO USSOUTHCOM from the SOUTHCOM Joint DoDIN Operations Center (JDOC).

TASK 6 – CONTINUAL SERVICE IMPROVEMENT (CSI)

The contractor is expected to employ methods and principles consistent with industry best practices, while conforming to DOD regulations and policies, for quality management and service measurement practices. The contractor is expected to ensure services provided within DoD remain aligned with mission objectives and the ever changing needs of USSOUTHCOM. These efforts are expected to be in concert with improving and maintaining quality and performance of services. The contractor is expected to be responsible for optimizing cyber-informed IT services, while remaining aligned with evolving mission requirements, and DoD strategies. The contractor is expected to ensure mission effectiveness and fiscal efficiency throughout all task areas and provide the government actionable and achievable opportunities to make informed decisions to improve services. The contractor is expected to actively balance operational needs while introducing innovation in relevant areas

of the task order that directly result in improved effectiveness, greater efficiencies, and a return on investment. The contractor is expected to ensure quality control and configuration management activities are accurate, consistent, cyber-informed, and integrated throughout the entire enterprise of IT services. The contractor is expected to use all available sensors in the operating environment to drive proactive reporting and decision making.

TASK 7 – SUPPLEMENTAL IT ENABLING SERVICES

The contractor is expected to provide all other additional services to enable and execute operations across DAO USSOUTHCOM. These services include the following: training, transport services, land mobile radio, satellite communications, logistics services, warehouse services, personnel security, management and oversight of U.S. State Department pouch system, special event service, country / location specific services anywhere in the USSOUTHCOM AOR, and provide other related enabling services. To clarify physical security services are to ensure the security of physical IT assets, security logs, and compliance with USSOUTHCOM policies and procedures.

VI. Current Environment

See attachment 1: DAO SOUTHCOM JDOC

VII. Business Systems

The Government expects the following business systems will be required:

a. An adequate cost accounting system, as determined by the cognizant Federal agency (e.g., Defense Contract Audit Agency (DCAA) or Defense Contract Management Agency (DCMA)) as defined in Federal Acquisition Regulation (FAR) 42.003 and the process for assignment of contract audit services as defined in FAR 42.1b.

b. An audited and approved purchasing system, as determined by the cognizant Federal agency (e.g., DCAA or DCMA) as defined in FAR 42.003 and the process for assignment of contract audit services as defined in FAR 42.1.

c. An adequate Property Management System as determined by DCMA.

VIII. Security

a. Information Assurance

The contractor may have access to sensitive (including privileged and confidential) data, information, and materials of the Government. These printed and electronic documents are for internal use only and remain the sole property of the Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED). Unauthorized disclosure of PA covered materials is a criminal offense.

Cybersecurity personnel will have, or obtain, SIPRNet and National Security Agency Network (NSANet) accounts and access to cybersecurity databases for eMASS, Xacta, and Ports, Protocols, Services, Management (PPSM) to facilitate data entry.

b. Security Clearances

In order to report to USSOUTHCOM-designated spaces for the first day of employment, contractor personnel must possess, at a minimum, a current Secret clearance determination reflected in the Defense Information System for Security (DISS). Under this TO, some contractor personnel may be required to have up to a current Top Secret (TS) clearance with an Sensitive Compartmented Information (SCI) eligibility determination. All contractor personnel with access to a Government-accredited Sensitive Compartmented Information Facility (SCIF) shall hold the appropriate clearances for the work to be performed, up to a TS/SCI. The majority of work is anticipated to occur at USSOUTHCOM Government facilities. There is flexibility for contractors to perform services at non Government locations with prior USSOUTHCOM approval. Contractors may be permitted access to classified information/material up to and including TOP SECRET and TOP SECRET/Special Access Program (SAP) in performance of their duties. For access to SAP contractors must have a need to know and provide a reoccurring material contribution to the success of the program/operation. Access to Alternative Compensatory Control Measures (ACCM) will be required (ON-SITE ONLY). Additional training on the handling and safeguarding of ACCM material is necessary. The Government will consider a security clearance requirement waiver on a case-by-case basis based on the complexity of the skill set and a security clearance is initiated for the individual whose security clearance is being waived. As a result, contractor personnel are required to:

a. Have a fully adjudicated Secret clearance with the initial investigation, periodic review, or enrollment into the Continuous Evaluation (CE) process within the last five years; and the ability to obtain a TS clearance.
b. Possess a current Secret security determination.

c. Facility Clearance

The contractor shall have a TS FCL. The contractor shall require access to Communications Security (COMSEC) information, SCI intelligence information, North Atlantic Treaty Organization (NATO) information, foreign government information, and controlled unclassified information (CUI) information.

d. Cyber-Supply Chain Risk Assessment

In the event of contract award, the Government may perform a cyber-supply chain risk assessment of the awarded contractor at any time during the period of performance. The Government may review any information provided by the contractor to the Government as part of this contract action, along with any other information available to the Government from any other source, to assess the cyber-supply chain risk associated with the contractor. The Government may monitor the following cyber-supply chain risk information, including, but not limited to:

1. Functionality and features of awarded products and services, including access to data and information system privileges.
2. The ability of a source to produce and deliver products and services as expected.
3. Foreign control of, or influence over, a source, product, or service (e.g.,

foreign ownership, personal and professional ties between a source and any foreign entity, legal regime of any foreign country in which a source is headquartered or conducts operations).

4. Security, authenticity, and integrity of products and services and their supply and compilation chains.
5. The contractor's capacity to mitigate identified risks.
6. Any other considerations that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of products, services, or sources.

In the event supply chain risks are identified during contract administration and corrective action becomes necessary, mutually agreeable corrective actions will be sought based upon specific identified risks IAW Federal Acquisition Regulation (FAR) 52.204-25 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.225-7975 and 252.239-7018. Failure to resolve any identified risk may result in Government action, including not extending the period of performance, not exercising remaining option periods, and contract termination.

IX. Government Estimate

The Government currently estimates the total amount of this requirement to be within the following range $650 million to $900 million. The period of performance for this contract may range between one-year base period and four, one-year options or one-year base period and six, one year options (two award term periods).

X. Questionnaires

Complete the following questionnaire as outlined below:

a. Responses should be submitted electronically by email only to Contracting Officer, Stephanie Crews, at *stephanie.crews@gsa.gov* and Contract Specialist, Shanneika Howell, at *shanneika.howell@gsa.gov* . Use the attached questionnaire to provide the requested information (no substitutions, additions, or deletions).
b. All responses must maintain one-inch margins, 12-point Times New Roman font, and be single spaced.
c. Table 1: Corporate Overview shall be no longer than 2 pages in length.
d. Table 2: Prior and Current Corporate Experience shall be limited to three submissions, each no longer than (2) pages in length for each example of Corporate Experience). All Corporate Experience must be performed by the respondent as a Prime contractor.
e. Corporate Capabilities and Approaches shall be no longer than 10 pages and is further limited below.
f. All information submitted shall be UNCLASSIFIED.
g. Please respond no later than *11:00 AM* Eastern Time on *10 September 2024*.
h. Send questions to *stephanie.crews@gsa.gov* and *shanneika.howell@gsa.gov*.

Table 1: Corporate Overview

Question	Answer
Name of Company	
Name of Business Unit Responding to the RFI (if applicable)	
DUNS Number	
CAGE Code	
Corporate Address	
Total Number of Full Time Employees	
Website URL	
Small Business under NAICS 541512 (Yes/No)	□ YES □ NO
Type of Small Business, if applicable (e.g., Woman-Owned, Service Disabled Veteran Owned, 8(a), HUBZone)	
Do you have a cost accounting system deemed adequate by a cognizant audit agency? (e.g., DCAA)	□ YES □ NO
Do you have an Approved Purchasing System?	□ YES □ NO
One Point of Contact (POC) (Enter name, phone number, and email address)	Name: Phone #: Email:
Please identify which, if any, of the below formal accreditations or certifications are held by your firm (do not include any self-certifications):	
Tailor the following question to help support your commerciality determination and ensure the IPT is considering commerciality during the market research phase. How does your company integrate commercially available offerings for a customized solution to meet the needs of complex mission requirements, specifically in support of national defense?	
ISO 9001 QMS	□ YES □ NO
ISO 20001 ITSMS	□ YES □ NO
ISO/IEC 27001 ISMS	□ YES □ NO
Other, please specify.	□ YES □ NO

Table 2: Prior and Current Corporate Experience

Per the overview provided above, please respond to the following inquiries **(Note: If your company is divided into separate business units, responses shall be based upon the Corporate Experience of the business unit responding to the RFI)**:

Please complete the below template for prior Corporate Experiences performed in the last five years in which the contractor (serving as prime contractor) provided or currently provides services similar in size, complexity, and scope to the stated requirements and technical environment as listed in Sections III and IV. Note: use individual task order values for the template below, not the overall Indefinite Delivery Indefinite Quantity (IDIQ) or Blanket Purchase Agreement (BPA) ceiling value the task order may have been awarded from.

Question	**Answer**
Contract Vehicle/Contract#	
Contract/Project Name	
Value at Award	
Value at Completion/Current Value	
Contract Type: check the type that represents the largest ($) for this contract	□ Time-and-Materials (T&M)/Labor-Hour (LH) □ Firm-Fixed-Price (FFP) □ Cost-Plus-Incentive-Fee (CPIF) □ Cost-Plus-Award-Fee (CPAF)
Client Department or Agency	
Project Description	
Client POC, Name, E-mail, Phone	
Percentage of Services Sub-contracted	
Number of Users	
Average Monthly Service Contact Volume	
Amount of Tools / Other Direct Costs (ODCs) Procured for Life of Task Order	

Corporate Capabilities and Approaches

a. Describe your corporate capabilities as they relate to the holistic and integrated Task Areas listed above. Please include which contract types these experiences were with, making specific note of Cost-Plus-Award-Fee task orders (limited to 2 pages).
b. Describe your company/business unit's experience, if any, with providing innovative solutions in terms of technology, process, or automation to drive operational service delivery efficiencies (cost and performance) without disrupting current operations, leveraging investment through savings in automation, and integrated delivery (limited to 2 pages).
c. Describe your company/business unit's capability, experience, and methodology for properly staffing a major IT infrastructure, CPAF contract, with the same size, scope, and complexity as referenced in Section II above. Additionally, please provide the methodology used to provide cleared personnel (see above requirements) for all individuals so as not to burden cleared Government and contractor resources with escort duty. (limited to 2 pages)
d. Describe your company's ability to staff up and meet the needs of the requirement within a 60-day timeframe. Your response should take into consideration the size (Greater than 300 employees), scope, and various required operational locations of the contract (CONUS and OCONUS). Additionally, the response shall demonstrate the offerors ability to provide the percent of the labor for this effort required by FAR clause 52.219-14 over the anticipated life of the contract. (limited to 2 pages)
e. Describe your company's technical ability and experience providing full-service enterprise IT support services, as described above, across a similar geographic area, for similar efforts of similar size, scope, and complexity, in both unclassified and classified environments. (limited to 2 pages)