Sol. W9124D-23-R-0007

Information Technology Support Services (ITSS),   
U.S. Army Recruiting Command, Fort Knox, KY (USAREC)

Due: October 27, 2022 09:00 a.m. ET

Submitted by:

HunaTek

**Contents**

Understanding of the Government’s Needs 1

Evaluation Criteria 1

Corporate Information 1

Corporate Experience (1.3) 2

Technical Approach 2

5.1. Functional Support 2

5.2. Requirements Engineering 3

5.3. Business Process Modeling 3

5.4. Software Engineering 3

5.5. Applications and Web Integration 3

5.6. Data Engineering 3

5.7. Database Management and Administration 3

5.8. Project Management 3

5.9. Project Control 3

5.10. Software Integration Engineering 3

5.11. Training Support Services for Recruiting and Retention College 4

5.12. Process Improvement 4

5.13. Information Technology Asset Coordinator 4

5.14. Telecommunications Control Officer 4

5.15. Test and Evaluation 4

5.16. Business Intelligence Experience 4

5.17 General System Support 4

5.18. Computer Graphics 4

5.19. Technical Writers 4

5.20. Incident Management 4

5.21. Information Management Services 4

5.22. Support the Administration of the IT Workforce Readiness 4

5.23. Administrative Support 4

5.24 Network Operations 4

5.25. Cyber Security 5

5.26. Monthly Report 5

Quality Control / Quality Assurance 5

Management Approach 5

Approach to Managing Personnel and Deliverables 5

Subcontractor Management 5

Recruiting and Retaining Cleared, Qualified Personnel 5

Staffing Plan (1.2) 5

Security 6

GFI/GFP 8

OCI 8

Transition 9

Submission: 1” margins, 11 pt Calibri font/9pt for tables. Technical capability (Page limit 20 pages)

# Understanding of the Government’s Needs

Objectives: To provide USAREC with ongoing ITSS for the USAREC for joint recruiting services through innovation, responsiveness, flexibility, and reliability while delivering a fully integrated environment supporting anytime, anywhere IT services.

## Evaluation Criteria

|  |  |
| --- | --- |
| Technical Capability - Responses shall be evaluated to assess feasibility of the proposed approach, plans, methods, and managerial ability to perform/manage the work, based on the Government’s assessment of the work. |  |
| Resource Information - Responses shall be evaluated to assess the feasibility of meeting the mission requirements with the proposed staffing plan based on the Government’s assessment of the work. |  |
| Experience - Responses will be evaluated to assess corporate experience with respect to projects similar in scope (tasks similar in complexity to those outlined in the PWS, Part 5) and size (annual value of $3.5 million or greater) to the work described herein. |  |

# Corporate Information

Separate from the non-price factor and price factor, Contractors must provide a cover letter addressing the following:

Company Name  
Company Address  
Point of Contact – authorized to obligate the contractor  
Phone Number  
E-Mail Address  
Unique Entity Identifier  
CAGE Code  
Tax Identification Number  
Confirm Yes or No, regarding participating under Supplier Self-Service Pilot (252.232-7998)

Any assumptions, exceptions, or deviations shall be addressed citing specific solicitation paragraph. Acknowledge of all amendments (if applicable) .

Proposal Acceptance Period shall be identified. Proposal acceptance period shall remain valid for a period of 90 calendar days after the closing date and time identified in the solicitation. Proposals offering less than 90 calendar days may be rejected as non-responsive.

## Corporate Experience (1.3)

(2 page limit)

# Technical Approach

(a) Describe the technical approach, plans, and methods for completion of the following tasks identified in PWS Part 5. The tasks are representative of some of the more complex tasks performed as part of overall mission requirements. Information provided should be in sufficient detail that it demonstrates Contractor’s technical understanding of the requirements:

(i) 5.2.1 Determine, analyze, and validate detailed requirements specifications.

(ii) 5.9.1 The contractor shall provide support to establish and maintain standardized project controls for Government assigned projects and ensure that project schedules are maintained and integrated into one master schedule.

(iii) 5.16.1 Applies industry-standard strategies and technologies used for the data analysis of business information.

(iv) 5.20.1 Contractor shall provide technical resolution for an average of 4,000-6,000 incident tickets per month (incident volume increases during periods such as system upgrades, network disruptions, and asset lifecycle replacement). Incidents are submitted by approximately 13,000 users located within the USAREC Headquarters building (Fort Knox), Army Marksmanship Unit (AMU) (Fort Benning), Special Operations Recruiting Battalion (SORB) (Fort Bragg), Recruiting and Retention Collage (RRC) (Fort Knox), and across USARECs 1800+ Brigades, Battalions, Companies and Stations worldwide. 80% of incidents should be resolved during the first contact and 100% within 72 hours. Contractor must be capable of serving as subject matter experts (SME) on common and advanced incident topics as described below and liaison with external agencies, vendors and key stakeholders to resolve incidents, problems, and events.

(v) 5.20.6 Problem and Event Management. Contractor shall identify risks, secondary impacts, and systemic problems that are reported from end users, service providers, other agencies, and commercial vendors. Problems should be promptly reported, assigned/escalated to the appropriate resource for resolution, and tracked through resolution.

(vi) 5.22.6.4 Provide configuration, customization, and administration of Army and commercial standard platforms. This may include customizing screens, editing fields, creating workflows, configuring reports, user account management, permissions, and roles, configuring security and privacy settings, and any other functions that would be required to ensure the platforms meet the government’s needs.

(vii) 5.24.1 Monitor network, system and application performance and work with government identified service providers to resolve issues such as outages, service degradation, upgrades, and maintenance. Networks include but are not limited to commercial and government hardwired and mobile networks providing internet, data, voice, fax, and other telecommunications services. Systems and applications include both GOTS and COTS products.

(b) Provide clearly defined management and organization structure and procedures that demonstrate Contractor's ability to manage a requirement of this size (annual value of $3.5 million or greater) and scope (tasks similar in complexity to those outlined in the PWS) as well as quality control matrix that demonstrate Contractor's ability to meet or exceed performance standards.

## 5.1. Functional Support

The contractor shall provide support services to the USAREC IT Projects, Programs, and Planning Division (P3MD). The contractor will support specific functional areas such as: requirements systems maintenance, sustainment, minor development, information management, business process modeling, enterprise architecture, data engineering, database management and administration, documentation, training, deploying software maintenance, integration engineering, process improvement, project management, and application software post-deployment support.

## 5.2. Requirements Engineering

The Government will provide needed modification requirements via government-issued actions such as scope documents, requirement documents, change requests, problem reports, and troubleshooting and/or other maintenance tasks related to the sustainment of production systems. The contractor shall:

## 5.3. Business Process Modeling

## 5.4. Software Engineering

Software development activities are limited to minor development incidental to systems maintenance and sustainment, which may include minor code construction, populating databases, integrating services, and other data files with data values; and other activities needed to implement the requirements and design. All activities must be presented to Government in the timeline set when acquiring the project. The Government, at its discretion and with approval of the Contracting Officer, may ask the contractor to follow an alternate development process or may waive some documentation requirements, particularly with minor change requests. The contractor shall:

## 5.5. Applications and Web Integration

## 5.6. Data Engineering

## 5.7. Database Management and Administration

## 5.8. Project Management

## 5.9. Project Control

## 5.10. Software Integration Engineering

The contractor shall provide Software Integration Engineering support to coordinate the technical architecture and the integration between major components thereof.

## 5.11. Training Support Services for Recruiting and Retention College

## 5.12. Process Improvement

The contractor shall provide process improvement using industry best-practices.

## 5.13. Information Technology Asset Coordinator

## 5.14. Telecommunications Control Officer

## 5.15. Test and Evaluation

## 5.16. Business Intelligence Experience

## 5.17 General System Support

## 5.18. Computer Graphics

## 5.19. Technical Writers

## 5.20. Incident Management

## 5.21. Information Management Services

## 5.22. Support the Administration of the IT Workforce Readiness

## 5.23. Administrative Support

## 5.24 Network Operations

## 5.25. Cyber Security

## 5.26. Monthly Report

# Quality Control / Quality Assurance

1.6.1. Quality Control (QC): The contractor shall develop and maintain an effective quality control program to ensure services are performed by this PWS. The contractor shall develop and implement procedures toidentify, prevent, and ensure the non-recurrence of defective services. The contractor’s quality control program is how the contractor assures that work complies with the requirement of the contract. The contractor quality control plan shall be delivered to the contracting office no later than 15 days following contract award. After acceptance of the quality control plan, the contractor shall receive the contracting officer’s acceptance in writing of any proposed change to the QC system.

1.6.2. Quality Assurance: The government shall evaluate the contractor’s performance under this contract by the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed by the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

# Management Approach

1.6.9. Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post-award conference convened by the contracting activity or contract administration office by Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings, the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

## Approach to Managing Personnel and Deliverables

## Subcontractor Management

## Recruiting and Retaining Cleared, Qualified Personnel

## Staffing Plan (1.2)

(5 page limit)

1.6.11. Key Personnel: The following personnel is considered key personnel by the Government: The contractor shall provide an on-site Program Manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the contracting officer. The Program Manager or alternate shall have full authority to act for the contractor on all contract matters relating to the daily operation of this contract. The Program Manager or alternate shall be available between 0730-1730, Monday thru Friday except on Federal holidays or when the Government facility is closed for administrative reasons.

1.6.12. Identification of Contractor Employees: All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

1.6.13. Contractor Travel: The contractor shall be required to travel to CONUS and OCONUS during the performance of this contract to attend events such as meetings, conferences, and training, and to provide technical support as required. OCONUS USAREC locations include Puerto Rico, Virgin Islands, Germany, Italy, Guam, American Samoa, Korea, and Japan. The contractor may be required to travel to off-site training locations and to ship training aids to these locations in support of this PWS. The contractor shall be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. All travel requires Government approval/authorization and notification to the COR.

## Security

1.6.7. Security Requirements: IAW AR 25-2 and HSPD-12, Installation Security Office will submit all background investigations on prospective contractors requiring CAC and/or network access. Provost Marshal’s Office wilconduct NCIC- III background checks on all other contractor personnel. For contractor personnel, the minimum requirement for access to unclassified federal information systems is as follows: IT-I access, a Single Scope Background Investigation (SSBI/SF 86); IT-II access, a NACLC (SF 86); and IT-III access, a NACI (SF 85P). Before CAC issuance, the NAC (FBI 10-point FBI fingerprint check) must be completed without adverse comment, and the NACI or equivalent must be initiated. CACs will not be issued before the fingerprint check results have been completed and the investigation has been submitted. Fingerprints and the appropriate investigation will be submitted by the Government.

1.6.7.1 Status of Forces Agreement (SOFA). Contractor shall comply with the provisions of current SOFAs of host nations identified in the PWS.

1.6.7.2. PHYSICAL Security: The contractor shall be responsible for safeguarding all government equipment, information, and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.6.7.3. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon the direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due to the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government, and the total cost deducted from the monthly payment due to the Contractor.

1.6.7.4. The Contractor shall prohibit the use of Government-issued keys/key cards by any persons other than the Contractor’s employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit the entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.6.7.5. Anti-Terrorism and Information Assurance Training.

1.6.7.6. AT Level I Training: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete AT Level I awareness training within 30 calendar days after the contract start date or the effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or the contracting officer, if a COR is not assigned, within 30 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: https://jkodirect.jten.mil/.

1.6.7.7. AT Awareness Training for Contractor Personnel Traveling Overseas: US-based contractor employees and associated sub-contractor employees to make available and receive government-provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

1.6.7.8. Access and General Protection/Security Policy and Procedures: Contractor and all associated sub-contractor’s employees shall comply with applicable installation, facility, and area commander installation/facility access, and local security policies and procedures. The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA, and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

1.6.7.9. iWATCH Training: The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 60 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

1.6.7.10. Contractor Employees Who Require Access to Government Information Systems: All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) https://atc.us.army.mil/iastar/index.php at the commencement of services and must complete the DOD Information Assurance Awareness before access to the information systems and then annually thereafter.

1.6.7.11. Global Address Listing (GAL): All contract employees who require access to Government Information Systems shall update their profile and Global Address Listing (GAL) information: https://www.dmdc.osd.mil/milconnect within 10 working days of being granted IT access.

1.6.7.12. OPSEC Training: Per AR 530-1, Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

1.6.7.14. Threat Awareness and Reporting Program (TARP). DA contract employees possessing a security clearance shall receive annual TARP training instructed by a CI agent or other trainer as specified in AR381-12,2-4b. Training shall be accomplished annually during the organization's scheduled TARP training session. In those instances where live training is not possible, such as in deployed theaters of operation, CI units may, in coordination with appropriate commanders, develop alternative means to conduct threat awareness training and meet the requirements of this AR 381-12.

1.6.7.15. Information assurance (IA)/information technology (IT) training: All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working in IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M, and AR 25-2 within 30 days of starting employment.

1.6.7.16. Annual Cyber Awareness Training: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete the Annual Cyber Awareness Training located at the US Army IA Training Center website listed below (previous training expires 25/Nov/13): Link: https://ia.signal.army.mil/DoDIAA/default.asp.

1.6.7.17. Acceptable Use Policy: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete a new Acceptable Use Policy (Annual Requirement) at the same website: Link: https://ia.signal.army.mil/DoDIAA/default.asp. (Click “Login”, Log in with CAC, confirm the information on-page, and click on “View and Sign AUP”.

1.6.8. Special Qualifications: All contractor employees shall adhere to the requirements of DoDD 8570.01- M and AR 25-2 training and qualification requirements for each position classification. Contractors shall obtain any certifications inherent with job/position functions. We will ensure that individuals check their training profile on the ATCTS site.

5.27.1. By DOD Regulation 8570.01-M paragraphs C1.4.4.12, C7.3.4.4, C1.4.4.5, C2.1.5, C1.4.4.12, C3.2.4.8.1 and C4.2.3.1, contractor employees with privileged access to any information system, contractors performing described Information Assurance (IA) functions must satisfy both preparatory and sustaining DOD IA training and certification requirements. Any personnel hired to perform functions in a position deemed as requiring elevated access privileges must be able to attain the security background check needed for the functions required. There are other determining factors regarding whether a user is placed in one of these training groups. Ensure staff have Approved Baseline Certifications. 5.27.2. The following certifications have been approved as IA baseline certifications for the IA Workforce for IAT Level II. Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level. IAT Level II: CCNA Security; CySA+ \*\*; GICSP; GSEC Security+ CE; CND; SSCP

## GFI/GFP

1.6.15. Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, including the source codes of any software, produced under this contract shall be Government-owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

3. GOVERNMENT-FURNISHED ITEMS AND SERVICES:

3.1. Services: None.

3.2. Facilities: The Government will provide the necessary workspace for the contractor staff to provide the support outlined in the PWS to include desk space, telephones, computers, and other items necessary to maintain an office environment.

3.3. Utilities: The Government will provide all utilities required to perform under this contract. The contractor (to include sub-contractors) shall instruct employees in utility conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

3.4. Equipment: The Government will provide the necessary computing and telecommunications equipment to perform services under this PWS.

3.5. Materials: None

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: The Contractor shall furnish all necessary supplies, equipment, and services required to perform work under this contract that is not listed under Section 3 of this PWS.

## OCI

1.6.16. Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications, or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor’s mitigation plan will be determined to be accepted solely at the discretion of the Contracting Officer and in the event, the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequently contracted requirements which may be affected by the OCI.

# Transition

1.6.17. PHASE IN /PHASE OUT PERIOD: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the 30-day phase-in / phase-out periods. During the phase-in period, the Contractor shall become familiar with performance requirements to commence full performance of services on the contract start date.