PERFORMANCE WORK STATEMENT (PWS)
United States Department of Veteran's Affairs (VA)
Southeast Louisiana Veterans Health Care System (SLVHCS)
Human Resources Support (Recruitment)
Base Contract
November 2016 Revised January 27, 2017

1. BACKGROUND: The New Orleans VAMC had been a tertiary care medical center for 23 parishes in Louisiana as well as a referral center for much of the Gulf Coast from the Florida panhandle to the Louisiana/Texas border. In 2005, Hurricane Katrina devastated the Gulf Coast and destroyed the medical center. Since then, the Southeast Louisiana Veterans Health Care System (SLVHCS), renamed to reflect the organizational change, operates as a system of eight community based outpatient clinics (CBOC) with inpatient care coordinated through other VA and local community facilities.

In addition to recovering health care services post-Katrina, SLVHCS completed the design of a new state of the art medical center that will return the organization to its original mission of being a tertiary care referral medical center. Construction on the replacement facility is ongoing. It will serve as the recruitment and training center for the nearly 1100 new employees that will need to be hired in advance of the full medical center completion and activation in 2016.

2. PERFORMANCE REQUIREMENTS:

2.1 Task 1: Recruit and Refer Physicians for full time employment at SLVHCS.

Task Performance Standard

2.1.1. Recruit Physicians for full time employment at New Medical Center. Contractor will recruit and refer candidates interested in Full-time Employment at the New Medical Center to Human Resources.

2.1.2 The Contractor shall make referrals based on the request of the SLVHCS. The total quantity of 10 placements may be accomplished via Physicians based on the needs of the SLVHCS. Recruitment strategy may be changed at any time based on the changing needs of the SLVHCS.

2.1.3 The Government will provide functional statements for each recruitment strategy at the time of that request. These functional statements will include the base standards for eligibility and may also include preferences for additional skills and/or qualifications.

2.2 Contractors will be available by phone Monday through Friday excluding weekends and Federal Holidays from the hours of 8:00am to 430pm Central Standard Time. Refer to the list of Federal Holidays under the section titled "Period of Performance" below.

3. APPLICABLE REGULATIONS

3.1 VHA Handbook 5005 and 5007, Chapter 10, located on the OHRM Website

3.2 Office of Oversight & Effectiveness Website, USA Staffing Guide- located in USA Staffing

4. DELIVERABLES AND DELIVERY SCHEDULE

4.1 Contractor is expected to actively and aggressively search and recruit for Physicians to fill positions from the vacancy list provided.

4.2 Contractor is expected to refer a minimum 5 applicants that are hired to fill positions from the list of vacancies during the contract term. Contractor is expected to refer additional candidates as required until all 10 positions are successfully filled.

4.3 Contractor will send the name of the qualified interested candidate and the documents listed below to the COR. Contractor will send the name of the qualified interested candidate and all required documents. At a minimum the contractor shall send the below documents:

4.3.1 VA Form 10-2850 “APPLICATION FOR PHYSICIANS”

4.3.2 Optional Form OF-306 “DECLARATION OF FEDERAL EMPLOYMENT “

4.3.3 CV “CURRICULUM VITAE “

5 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION (GFE/GFI): The contractor will receive a listing of vacant positions. The listing will be prioritized by Hard to Fill and desired Entrance on Duty date. Contractor staff shall sign non-disclosure statements prior to using this information.

6. PLACE OF PERFORMANCE:

Work will be performed virtually away from the Medical Center. Contractor shall provide location and all equipment for performance.

7. PERIOD OF PERFORMANCE: The period of performance for this contract is one base year beginning March 1, 2017 until February 28, 2018. Work shall not take place on Federal holidays or weekends.

7.1 Federally recognized holidays include: New Year’s Day, Martin Luther King Jr. Birthday, President’s Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran’s Day, Thanksgiving, and Christmas.

8. PERFORMANCE REQUIREMENTS SUMMARY:

Task	What will be inspected	Who will inspect it	What is Acceptable?	When it will be inspected	Where it will be inspected	How it will be inspected
1	Recruit Physicians for full time employment New Medical Center	Human Resources Officer, Chief of Staff and Service Chief	Minimum of 3 Candidates hired per Qtr	When candidate is referred	At SLVHCS via phone or in person	Candidate Interview

9. SECURITY

VA ACQUISITION REGULATION SOLICITATION PROVISION AND CONTRACT CLAUSE

The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE

1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A contractor/subcontrator shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to

ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

3. VA INFORMATION CUSTODIAL LANGUAGE

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d)(1).

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the

contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia,

alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, Certification and Accreditation and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to

document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or contractor/subcontractor-owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, Electronic Media Sanitization upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

6. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the

designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of $ 37.50 affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

(1) Notification;

(2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

(3) Data breach analysis;

(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

8. CONTRACTOR RULES OF BEHAVIOR

Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall sign on an annual basis an acknowledgement that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior which is included

in the training outlined in paragraph (Training). If the contractor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the vendor's designated representative. By signing the Rules of Behavior on behalf of the vendor, the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing VA's information and information systems. A copy of the signed rules of behavior must be submitted before work begins (within 5 business days of contract award).

9. TRAINING

All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix D relating to access to VA information and information systems;

b. Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior training and annually complete required security training;

c. Successfully complete VHA Privacy Policy Training if Contractor will have access to PHI;

d. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

e. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

f. The Contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

g. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

h. VA training site is located at www.tms.va.gov

There is only one course the contractor needs to complete and print the certificate at the end. A copy of the completed certificate must be submitted before work begins (within 5 business days of contract award).

++

Instructions to get to the Courses in TMS www.tms.va.gov

Log onto the site and create a new user account; if you already don't have one. Search for your course entitled VA Privacy and Information Security Awareness and Rules of Behavior. Complete course, print certificate (s), and sign/print contractor rules of behavior.

VA Learning University (VALU)

Help Desk: 1-866-496-0463

valmshelp@va.gov

++
++++++++++++++++++++++++++++++++++

Examples

VA Privacy and Information Security Awareness and Rules of Behavior

10. CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

a. The following security requirement must be addressed regarding Contractor supplied equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COTR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

b. All contractor employees who require access to the Department of Veterans Affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the VA Security and Investigations Center (07C). The level of background security investigation will be in accordance with VA Directive 0710 dated September 10, 2004 and is available at: http://www.va.gov/pubs/asp/edsdirec.asp (VA Handbook 0710, Appendix A, Tables 1 - 3). Appropriate Background Investigation (BI) forms will be provided upon contract (or task order) award, and are to be completed and returned to the VA Security and Investigations Center (07C) within 30 days for processing. Contractors will be notified by 07C when the BI has been completed and adjudicated. These requirements are applicable to all subcontractor personnel requiring the same access. If the security clearance investigation is not completed prior to the start date of the contract, the employee may work on the contract while the security clearance is being processed, but the contractor will be responsible for the actions of those individuals they provide to perform work for the VA. In the event that damage arises from work performed by contractor personnel, under the auspices of the contract, the contractor will be responsible for resources necessary to remedy the incident.

c. The investigative history for contractor personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use a vendor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

11. CONFIDENTIALITY AND NONDISCLOSURE

1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

2. CONFIDENTIALITY AND NONDISCLOSURE

It is agreed that:

1. The preliminary and final deliverables and all associated working papers, application source code, and other material deemed relevant by the VA which has been generated by the contractor in the performance of this task order are the exclusive property of the U.S. Government and shall be submitted to the CO at the conclusion of the task order.

a. The CO will be the sole authorized official to release verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this task order. No information shall be released by the contractor. Any request for information relating to this task order presented to the contractor shall be submitted to the CO for response.

b. Press releases, marketing material or any other printed or electronic documentation related to this project, shall not be publicized without the written approval of the CO.