

ATTACHMENT A

PERFORMANCE WORK STATEMENT FOR DEPARTMENT OF VETERANS AFFAIRS (VA), OFFICE OF ASSET ENTERPRISE MANAGEMENT (OAEM) STRATEGIC ADVISORY, LEASE PROGRAM COMPLIANCE, OVERSIGHT, AND TECHNICAL SUPPORT

A. GENERAL INFORMATION

1. **Title of Project:** Lease Program Compliance and Technical Support

2. **Scope of Work:** Contractors must demonstrate capabilities to accomplish tasks under this Indefinite Delivery Indefinite Quantity (IDIQ). Tasks under this IDIQ relate to management of an enterprise-wide lease portfolio, including: the GSA delegation process; milestone tracking of leases through the leasing lifecycle; data reviews and validation; and systems integration. The high-level requirements identified in this IDIQ may be refined adaptively in task orders over the course of this project in an effort to continuously meet specified user needs. User needs will be prioritized based on business value and technical dependencies.

Examples of the tasks that may be required under this IDIQ may include one or more of the following: maintaining and updating VA's SharePoint based tracking and reporting system for leases currently in the process of receiving internal approval, delegation from GSA, or execution of lease contract; review of submitted lease packages to ensure compliance with internal approval, GSA, and OMB A-11 requirements including documentation and communication of any identified deficiencies; detailed review of each lease scoring to ensure proper scoring is done and a lease qualifies as an operating lease under OMB A-11; specific documentation and training material related to the lease delegation process, best practices, and scoring of leases and application of OMB A-11 Appendix B; enhancements to the existing SharePoint based tracking tool to include improved data validation, reporting, quality control, and security; update of VA's lease scoring model (an Excel template already exists) and associated training material; data integrity reviews and updates; data integration with other systems; general lease process flow review and documentation; studies related to the lease portfolio and/or delegation process' and general program support including meetingminutes.

OAEM, VA's Office of Real Property (ORP), VHA, and other organizations will be responsible for package creation and interaction directly with GSA's GREX system. Information on project status will come from the same sources; however, the contractor is responsible for the tracking and update of information provided by these various offices and ensuring the quality of the data in ELMT. The tasks are to support VA in maintaining compliance with GSA's delegation policies. Tasks will not replace inherently governmental reviews of individual lease projects.

3. **Background:** The Department of Veterans Affairs, Office of Asset Enterprise Management (OAEM), is held accountable for meeting a number of requirements pertaining to its capital asset management. Capital Asset initiatives and the Strategic Capital Investment Planning (SCIP) process are coordinated to ensure capital investments are based on sound business practices and principles and, most importantly, meet Veterans' health care, benefits and burial needs. Laws, Presidential directives and regulations containing these requirements include:

- Executive Order (EO) 13327, “Federal Real Property Asset Management.”
- 38 U.S.C. §§ 8161-8169, “Enhanced-Use Lease of Real Property.”
- 38 U.S.C. § 8151-8153, “Sharing of Health Care Resources.”
- VA Directive 4085, “Capital Asset Management Policy”.
- VA Directive 7415, “Enhanced-Use Leasing Program Policies and Procedures.”
- VA Handbook 7415 and appendices, “Enhanced-Use Leasing Program Policies and Procedures.”
- Section 106 of the National Historic Preservation Act (16 U.S.C. § 470(f)).
- Comprehensive Environmental Response, Compensation, and Liability Act (“CERCLA”), 42 U.S.C. §§ 9601-9675.
- Resource Conservation and Recovery Act (“RCRA”), 42 U.S.C. §§ 6901-6908a.
- National Environmental Policy Act (“NEPA”), 42 U.S.C. §§ 4321-4347.
- OMB A-11, Part 7, Exhibit 300 and Capital Programming Guide.
- American Recovery & Reinvestment Act (P.L. 111-5) (February 17, 2009).
- Government Performance and Results Act (1993).
- Veterans Health Care Improvement Act of 2004 (Public Law 108-422) – Requiring VA provide a long-term and short-term real property disposal plan to the Congress.
- GAO Report 08-939, Federal Real Property – Progress Made in Reducing Unneeded Property, but VA needs Better Information to Make Further Reductions.
- Federal Acquisitions Streamlining Act (1994).
- Energy Policy Act of 2005 (EPA 2005).
- EO, 13423, Strengthening Federal Environmental, Energy and Transportation Management, 2007.
- EO, 13514, Federal Leadership Environmental, Energy and Economic Performance, 2009.
- Energy Independence and Security Act, 2007.

OAEM follows instructions and guidance issued by the Office of Management and Budget and other agency instructions, directives and guidance containing specific capital asset performance metrics.

VA has as its unique mission the delivery of comprehensive assistance and benefits to the nation’s Veterans and their families. Through its Veterans Health Administration, the VA is one of the largest direct providers of health care in the world. The Department is also a major land holding agency, with an extensive and diverse portfolio of properties including over 32,000 acres of land and over 5,400 buildings at approximately 300 locations nationwide. To manage its property, VA uses all of the traditional authorities available to federal agencies. In many instances these authorities do not adequately address the needs of specific mission or developmental issues. Because of these limitations, exacerbated by on-going budgetary constraints, privatization and income-generation programs have become increasingly important to the Department.

The SCIP process includes development of Long-Range Action plans and later budget year business cases to meet existing performance gaps (space, facility condition, access, etc.) and enhance healthcare and delivery of services and benefits to the Nation’s Veterans. As part of VA’s continual improvement of its capital asset initiatives and planning management, the Office of Management (OM) and the Office of Acquisition, Logistics, and Construction (OALC) developed the Capital Program Requirements Management Process

(CPRMP) to address changes to Major Construction and Authorization Level Lease projects that have been approved through the Strategic Capital Investment Planning process. The process was

approved on August 30, 2013.

4. Performance Period: The period of performance is for thirty-six (36) months / 1095 calendar days from date of award. Work at the government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

5. Type of Contract: Indefinite Delivery Indefinite Quantity (IDIQ).

6. Place of Performance: The primary place of performance will be at the contractor's facilities; however, some task orders may require work to be performed at a Government facility.

B. CONTRACT AWARD MEETING

The contractor shall not commence performance on the tasks in this PWS until the CO has conducted a kick-off meeting or has advised the contractor that a kick-off meeting is waived.

C. GENERAL REQUIREMENTS

The following general requirements apply to this contract:

1. The contractor shall identify its proposed technical approach in writing. The contractor's IDIQ and task order quotes shall include its proposed labor categories, rates and number of hours by task, together with associated delivery dates and sub-milestone dates (if any), and proposed key personnel résumés. Résumés are not required for clerical personnel.
2. All written deliverables shall be phrased in layperson language. Statistical and other technical terminology shall not be used without providing a glossary of terms.
3. Unless otherwise specified in an individual task order, the following schedule requirements apply: Where a written milestone deliverable is required in draft form, the VA will complete its review of the draft deliverable within 12 calendar days from date of receipt, subsequent drafts will be provided as necessary until no additional edits are requested by VA. The contractor shall then have 12 calendar days to deliver the final deliverable from date of receipt of the Government's comments.
4. The contractor shall provide, via email, minutes of all Government-contractor meetings to the COR and CO. The contractor shall provide these minutes within one calendar day after completion of the meeting unless otherwise specified in an individual task order.
5. Except for proprietary information in company quotes identified and marked in accordance with FAR 52.215-1(e), the contractor shall not deliver to VA any proprietary products or information of any type in completing the requirements of each task order PWS. The contractor's internal development tools (that is, those development tools not developed for VA work and not required by VA to install, use, or revise the deliverables) are exempted from this requirement. If the contractor believes an exception to this requirement is necessary for the effective or efficient execution of a task order, the contractor shall request a specific exception, in writing, to the CO, and shall not use the proprietary tools or information in VHA work until approval is received from the CO.
6. The contractor shall ensure contract employees maintain an open and professional communication with the staff at the VA facilities. For transparency purposes, email to the CO shall not be blind carbon copied (BCC) to other Government personnel.
7. Complaints or violation validated by the COR or VA staff will be reported in writing to the CO, Office of the Inspector General (OIG), or Head of the Contracting Activity (HCA) for action. If

the contractor fails to correct validated complaints raised by the COR and or CO, it will be considered a failure in performance.

8. The CO may require the contractor to meet with the CO, contract administrator, and other Government personnel at least quarterly, and as often as deemed necessary. The contractor may request a meeting with the CO when deemed necessary.

D. TASKS – LEASE PROGRAM COMPLIANCE AND TECHNICAL SUPPORT

Description of Tasks: Task orders awarded under this IDIQ may require the completion of one or more of the following tasks:

a. Task One: PMP and Briefing.

The contractor shall provide a Project Management Plan (PMP) and briefing for the project team, which presents the contractor's plan for completing the task order. The contractor's plan shall be responsive to the task order PWS and describe, in further detail, the approach to be used for each aspect of the task order as defined in the technical proposal. The contractor shall keep the PMP up to date throughout the period of performance.

b. Task Two: Maintaining and updating of the tracking and reporting system for lease status.

The contractor shall maintain and update the lease tracking system by which status of all leases in the procurement pipeline can be actively tracked and reported on. The contractor is responsible for on-going tracking and reporting of all leases currently in the procurement pipeline, beginning with initial approval/request through acceptance of the space. This reporting will be done on a bi-weekly basis and updates to status may be provided as they occur; however, ad-hoc requests for updates and reports may be made, which may include detailed reporting and tracking of each individual lease. In addition, the contractor will be required to perform bulk updates to the tracking system on a regular basis, including such items as loading newly approved leases from VA's budget submission or operating plan, updating delegation status/dates based on reports from GSA, and updating procurement milestone dates based on reports from eCMS. The updates are "mass- quantity" updates that will be required in addition to the individual project status updates the contractor will be performing.

c. Task Three: Review of lease package submissions for GREX uploading, including detailed analysis of scoring for each lease.

The contractor shall review all lease packages submitted for the following:

- 1) Completeness of package – is the package complete and includes all necessary documents required by both OMB and GSA.
- 2) Internal approvals – does the package have all necessary internal approvals required.
- 3) Scoring – is the scoring completed correctly, in compliance with OMB A-11, and score as an operating lease.
- 4) Quality – are the documents included in the package consistent,

represent a clear understanding of the requirement, and are supported by necessary data.

For each submission, contractor shall document in scorecard type format the items noted above, including specific comments related to any issues or concerns noted during the review. The estimated and maximum number of reviews, including both original and re-submissions will be established in each task order. Each review should be completed within 2 calendar days of receipt. In rare instances, some review requests may be expedited to the same day.

d. Task Four: Lease process training and documentation support.

The contractor shall provide training content on the lease review, delegation process, and other requested training that relates to the leasing lifecycle. Training will be end user focused and include best practices, templates, guidance, examples, videos, web-based instruction, and other supporting documents related to the leasing process. Contractor will support training to be provided by OAEM. The contractor will participate in the training and provide assistance on detailed aspects of the process, when requested.

e. Task Five: Lease Tracking System enhancements.

Contractor shall make enhancements to the existing SharePoint based tracking systems. Enhancements include fully leveraging SharePoint to provide improved data management, reporting, security, data validation, workflow, alerts, and other features available in SharePoint. Contractor shall develop, test, and implement changes upon approval by VA. Existing tracker functionally and data cannot be lost and must be maintained with any enhancements.

f. Task Six: General program support and status reporting.

Contractor shall convene status meetings bi-monthly, including meeting minutes. Status reports should be created outlining the status of each deliverable in the task order, including number of packages reviewed, number and type of issues found, and general summary of the leases in process.

g. Task Seven: Updates to VA's Lease Scoring Template.

Contractor shall update VA's Excel based lease scoring template to incorporate revised data sets and updates to methodology as needed. There are currently three primary data sets that will need to be included in the model as they are released: 1) GSA Location Factors, 2) OMB Discount Rates, and 3) RS Means data. Any requirements for new or additional data sets will be provided by VA. Each of these data sets should be incorporated once available and new versions of the template produced (the total number of required updates will be indicated in the task order).

With each update, any necessary documentation or training material should also be updated to reflect the latest information. This task does NOT include completing scoring for specific leases, only updates to the model/template itself.

h. Task Eight: Data integrity reviews and updates.

Contractor shall review the accuracy and consistency of stored data, to include: analyzing or reconciling any gaps in or absences of data; monitoring or tracking alterations in data records; performing error checking and validation routines; preventing accidental or deliberate, but unauthorized, insertion, modification or destruction of data; and updating data with values derived from other VA resources, values provided by the VA end user, or values otherwise provided by VA.

i. Task Nine: Data integration with other systems.

Contractor shall provide analysis and integration of data between VA systems and databases such as the Capital Asset Inventory (CAI), SCIP Automation Tool (SAT), Electronic Contract Management System (eCMS), or other VA systems and databases that may be specified in individual task orders; develop and prepare system integration survivability and countermeasure plans; perform functional analyses, systems studies and risk assessments of system integration survivability and countermeasure plans; and recommend the most feasible architectures, design approaches, system upgrades, and deficiency correction for system integration survivability and countermeasure plans. Based on these analyses and studies, the contractor may be required to prepare reports, white papers, and briefings – specific requirements will be indicated in individual task orders.

j. Task Ten: General lease process flow review and documentation.

Contractor shall provide general lease process flow review and documentation for one or more phases of the leasing lifecycle, which may include: requirements development, market research, cost benefit analysis, prospectus preparation, scoring analysis, delegation request assistance, and post-award compliance. Specific requirements will be indicated in individual task orders.

k. Task Eleven: Studies related to the lease portfolio and/or delegation process.

Contractor shall perform data and functional studies regarding the lease portfolio and the delegation process. Lease portfolio studies may include analyzing lease details to provide a comprehensive view of leasing obligations – including costs, terms, and expiration dates. Delegation process studies may involve identifying and documenting best practices, performing a risk analysis, and recommending process enhancements. Based on these studies, the contractor may be required to prepare reports, white papers, and briefings – specific requirements will be indicated in individual task orders.

Performance Standards and Methods as specified in each task. Past performance will be documented in accordance to IL 001AL-10-03, dated February 22, 2010.

Surveillance Area	Performance Standards	Method of Assessing Performance
Management of price and schedule	<p>Timely delivery to the COR within the contract/order schedule.</p> <p>Status Meetings are scheduled on time, with appropriate Vendor staff attending and issues addressed satisfactorily to VA.</p>	<p>Review of Monthly Status Reports and Status Meetings</p> <p>100% inspection</p>
Technical quality of deliverables	<p>Deliverables are high quality, address required performance work statement areas and contain three (3) or fewer defects identified in the Final deliverable submittal.</p>	<p>Review of Final deliverables and Status Meetings</p> <p>100% inspection</p>
Quality of Project Management and Relationship Management	<p>Timely Responses to open acquisition issues 98% of the time.</p> <p>Corrections and Re-submittal to VA within five calendar days of rejected deliverables.</p> <p>Low Turnover of Key Personnel.</p> <p>Contractor develops and maintains a staffing plan that adequately supports the requirements of the task orders 98% of the time.</p> <p>Open communication between VA and Vendor.</p> <p>Contractor provides a single point of</p>	<p>Review of Final deliverables, Status Reports and Status Meetings</p> <p>Review and approval of Key Personnel changes</p> <p>VA customer satisfaction</p>

	<p>contact responsible for task order performance.</p> <p>Ability to meet the within scope changing demands of the program as it evolves.</p>	
--	---	--

E. SCHEDULE FOR DELIVERABLES

1. Each individual task order will contain a schedule of deliverables with associated dates and time.
2. If for any reason the scheduled time for a deliverable cannot be met, the contractor is required to explain why (include the original deliverable due date) in writing to the CO, including a firm commitment of when the work shall be completed. This notice to the CO shall cite the reasons for the delay, and the impact on the overall project. The CO will then review the facts and issue a response in accordance with applicable regulations.
3. Any hard copy documents the Contractor provides to OAEM must be printed double-sided on recycled paper with at least 30 percent post-consumer fiber.

F. CHANGES TO PERFORMANCE WORK STATEMENT

Any changes to this PWS and all Task Orders shall be authorized and approved only by the CO in writing. Costs incurred by the contractor through the actions of parties other than the CO shall be borne by the contractor.

G. TRAVEL

As required by each task order, the contractor may be required to travel to Washington, D.C., or to other VA locations. Travel and per diem shall be reimbursed in accordance with Federal Travel Regulations. Each contractor invoice must include copies of all receipts that support the travel costs claimed in the invoice. No General and Administrative (G&A) fees or costs, and no other fees or costs shall be added to travel expenses. Local travel within a 50-mile radius from the Contractor's facility is considered the cost of doing business and will not be reimbursed. This includes travel, subsistence, and associated labor charges for travel time. Local travel within a 50-mile radius from the Contractor's employee's residence is considered the cost of doing business and will not be reimbursed. This includes travel, subsistence, and associated labor charges for travel time. Travel performed for personal convenience and daily travel to and from work at the contractor's facility will not be reimbursed. Travel, subsistence, and associated labor charges for travel time for travel beyond a 50-mile radius of the Contractor's facility are authorized on a case-by-case basis and must be pre-approved by the CO at least 30 calendar days in advance for the requested travel.

H. GOVERNMENT FURNISHED PROPERTY AND INFORMATION

The Government will provide access to the Space Analysis model, Space Calculator tool, and all

required data files required for use in these two tools. In addition, the Government will also provide current and projected inpatient and outpatient workload and utilization data and assumptions for both the hospital and surrounding area which will be validated by the contractor.

I. CONTRACTOR EXPERIENCE REQUIREMENTS—KEY PERSONNEL

1. These skilled experienced professional and/or technical personnel are essential for successful contractor accomplishment of the work to be performed under this contract and subsequent task orders and options. The contractor shall include in the technical proposal for each task order the résumés on all proposed professional and/or technical personnel who will perform the tasks in the task order. Résumés are not required on clerical personnel. The personnel whose résumés are submitted are defined as key personnel. The contractor agrees that the key personnel listed below shall not be removed, diverted, or replaced from work without approval of the CO and COR (résumés do not need to be provided if it is already in the contract file).

2. Any personnel the contractor offers as substitutes shall have the ability and qualifications equal to or better than the key personnel that are being replaced. Requests to substitute personnel shall be approved by the COR and the CO. All requests for approval of substitutions in personnel shall be submitted to the COR and the CO at least 30 calendar days prior to making any change in key personnel. The request shall be written and provide a detailed explanation of the circumstances necessitating the proposed substitution. The contractor shall submit a complete résumé for the proposed substitute, any changes to the rate specified in the order (as applicable) and any other information requested by the CO needed to approve or disapprove the proposed substitution. The CO will evaluate such requests and promptly notify the contractor of approval or disapproval thereof in writing.

Note:

- a. Standards of Conduct. The Contractor shall ensure that personnel assigned to this contract comply with the Standards of Ethical Conduct specified by the Office of Government Ethics at 5 CFR 2635.
- b. Personnel assigned by the Contractor to perform work on this IDIQ shall be acceptable to VA in terms of personal and professional conduct and technical knowledge. The Contracting Officer may notify the Contractor and request that a person be immediately removed from assignment on this contract should any contractor personnel be determined to be unacceptable in terms of technical competency or personal conduct during duty hours. The contractor shall immediately remove and replace the unacceptable on-site personnel at no additional costs to the Government. Replacement personnel qualifications shall be equal to or greater than those of the personnel being replaced. Employment and staffing difficulties shall not be justification for failure to meet established schedules.
- c. Contractor personnel shall be able to communicate effectively in English, both written and oral.

- d. The contractor shall notify the CO whenever an employee of the United States Government is utilized by the contractor in the performance of the contract. The notification shall include sufficient information for the Contracting Officer to review the matter in accordance with FAR Part 3 and Subpart 9.5.
- e. The contractor shall verify employee eligibility through the E-Verify system.

J. SECURITY REQUIREMENTS

1. The contractor shall follow the following (or other established procedure) contractor personnel security guidance:
 - a. The contractor and their personnel shall be subject to the same Federal laws, regulations, standards, and VA policies as VA personnel, regarding information and information system security. These include, but are not limited to Federal Information Security Management Act (FISMA), Appendix III of OMB Circular A-130, and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST's Web site at: <http://checklists.nist.gov>
 - b. To ensure that appropriate security controls are in place, Contractors must follow the procedures set forth in "VA Information and Information System Security/Privacy Requirements for IT Contracts" located at the following Web site: <http://www.iprm.oit.va.gov>.
 - c. These provisions shall apply to all contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on the VA's behalf.
 - d. Clauses (a) and (b) shall apply to current contracts and acquisition vehicles including, but not limited to, job orders, task orders, letter contracts, purchase orders, and modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. § 6301 et seq.
2. The required contractor employee Position Sensitivity level is Limited Risk and the level of Background Investigation is NACI for contractor employees who require access.
3. The designated Government employee will provide the contractor a Background Investigation Request Worksheet within two calendar days of task order award listing the place of performance, type of investigation requested, the VA sponsor and requesting the applicant's name, date of birth, social security number, company name and point of contact, and other required data.
 - a. The contractor shall complete the Background Investigation Request worksheet and

return it within 5 calendar days of receipt.

- b. The CIS will send an email notification to the contractor identifying the website link that includes detailed instructions regarding completion of the background clearance application process and what level of background was requested. Upon receipt of required investigative documents, SIC will review the investigative documents for completion and initiate the background investigation by forwarding the investigative documents to OPM to conduct the background investigation.
 - c. The COR will notify the contractor when the investigation has been favorably or unfavorably completed and adjudicated by the Government. The contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.
4. The contractor shall not commence performance prior to the initiation of the process that requests the appropriate investigative action be taken. During the time required to conduct the appropriate investigation, the contractor shall be responsible for the actions of its respective employees until official notification of a favorable determination is received from the Office of Security and Law Enforcement.
 5. Cost of Background Investigations will be borne by the organization requesting the investigation. For contractors and its personnel performing the contract, the VA office or organization that is requesting the procurement will coordinate with the designated contracting officer to ensure VA initiates the necessary investigations and/or screenings for contractor personnel. For those contractors and its personnel, the contractor will bear the cost of such investigations.
 6. Failure to comply with the contractor personnel security requirements may result in termination of the contract for default also please reference to VA Directive 0710 for further guidance

IT CONTRACT SECURITY

1. VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY

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/subcontractor 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 FAR 52.227-14(d)(1), Rights in Data – General.

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 on-site 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 calendar 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 38 U.S.C. § 5705, confidentiality of medical quality assurance records and/or 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 COR.

4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

b. The contractor/subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

d. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

e. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800- 37, Guide for Applying the Risk Management Framework to Federal Information Systems, VA Handbook 6500, Information Security Program and VA Handbook 6500.5, Incorporating Security and Privacy in System Development Lifecycle.

f. The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. § 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

g. The contractor/subcontractor agrees to:

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the contractor/ subcontractor is to perform;

(1) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

(2) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

h. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on

individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.

(1) “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

(2) “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

(3) “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

i. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

j. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than 3 calendar days.

k. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 calendar days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within 5 calendar days. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 calendar days of discovery or disclosure. Exceptions to this paragraph (e.g., for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

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 COR 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 memoranda 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 COR. 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 calendar days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

- (1) Vendor must accept the system without the drive;
- (2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- (3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

(4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

(a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

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 COR 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. The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non- Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term ‘data breach’ means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

- (1) Nature of the event (loss, theft, unauthorized access);
- (2) Description of the event, including:
 - (a) date of occurrence;
 - (b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- (3) Number of individuals affected or potentially affected;
- (4) Names of individuals or groups affected or potentially affected;
- (5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plaintext;
- (6) Amount of time the data has been out of VA control;
- (7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

- (8) Known misuses of data containing sensitive personal information, if any;
 - (9) Assessment of the potential harm to the affected individuals;
 - (10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
 - (11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
- d. 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 per 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. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 calendar-days' notice, at the request of the Government, the contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

9. TRAINING

a. 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:

- (1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix E

relating to access to VA information and information systems;

(2) Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training;

(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access to be defined by the COR

b. The contractor shall provide to the contracting officer and/or the COR 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.

c. 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.

K. 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 have been generated by the contractor in the performance of this IDIQ and any ensuing task orders are the exclusive property of the U.S. Government and shall be submitted to the COR with a copy to the CO at the conclusion of the task order.
2. 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 IDIQ and any ensuing task orders. No information shall be released by the contractor. Any request for information relating to this IDIQ and any ensuing task orders presented to the contractor shall be submitted to the CO for response.
3. Press releases, marketing material or any other printed or electronic documentation related to this IDIQ and any ensuing task orders, shall not be publicized without the written approval of the CO.

L. ORGANIZATIONAL CONFLICT OF INTEREST

The contractor shall disclose any actual or potential organizational conflicts of interest at the time of submitting the quotes for the basic IDIQ and any ensuing task orders. The contractor may be precluded from bidding on or working on future contracts in accordance FAR subpart

9.5.

Evaluations of Offers

Award shall be made to the offeror whose quote offers the best value to the government, considering technical capability, past performance, and price. The government will evaluate information based on the procedures authorized in FAR Part 13.106-2 – Evaluation of Quotations of Offers using the following evaluation criteria:

- 1) **Technical Evaluation** – The evaluation process will consider whether the proposal demonstrates a clear understanding of the technical features involved in meeting the requirements of the solicitation.
- 2) **Price** – The contractor’s quote shall include their proposed labor categories, and rates by task. The Government will evaluate offers by adding all line item prices - the Total of All CLINS will be that sum.
- 3) **Past Performance** – The Vendor’s quote must include a summary description of at least three but no more than five prior contracts/orders per team member/sub-contractor for projects completed within the last five years with organizations with similar mission and functional domains, and of comparable size, complexity and scope. These references must also include:
 - Contract/Order Number, brief description of the project, type of contract, amount of the contract
 - Contracting Officer’s Name and Phone Number, Government agency
 - Contracting Officer’s Representative Name and Phone Number

The contractor must indicate whether they were the prime contractor, sub-contractor or other teaming arrangement. Prime shall indicate which aspect they are directly responsible for of this requirement.

The Offeror is required to provide references for the above projects. In the event the company itself does not have relevant past performance, references may be submitted on contracts performed by the Key Personnel of the company. The VA reserves the right to contact all the references that the Offeror lists.

Evaluation Approach

- A. All quotes shall be subject to evaluation by Government personnel. The Government intends to award without discussions based upon the initial evaluation of quotes. However, it may be determined necessary to conduct discussions if award cannot be made on the initial quotes submitted.
- B. All Offerors are advised that, in the interest of efficiency, the Government reserves the right to conduct the evaluation in the most effective manner. The Government also reserves the right to evaluate all Offerors’ technical quotes should it desire to conduct discussions, or otherwise determine it to be in the Government’s best interest.
- C. The quote will be evaluated strictly in accordance with its written content. Quotes which merely restate the requirement or state that the requirement will be met, without providing supporting rationale, are not sufficient. Offerors who fail to meet

the minimum requirements of the solicitation will be rated Unacceptable and thus, ineligible for award.

- D. Unbalanced Pricing - The Government may evaluate whether the Offeror has submitted unbalanced pricing. An unbalanced price is one where the price of one or more contract line items is significantly overstated or understated and which will result in the Government paying an unreasonably high price for contract performance or otherwise present an unacceptable level of risk to the Government. If the Contracting Officer determines that the risk is unacceptable, then the bid or offer can be rejected.

The full text of FAR provisions or clauses may be accessed electronically at <http://acquisition.gov/comp/far/index.html>.

The following solicitation provisions apply to this acquisition:

1. 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (OCT 2015)
2. 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (JUL 2013)
3. 52.216-1 TYPE OF CONTRACT (APR 1984)
4. 52.233-2 SERVICE OF PROTEST (SEP 2006)
5. VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (JAN 2008)
6. VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (JAN 1998)
7. 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)
8. 52.212-2 EVALUATION—COMMERCIAL ITEMS (OCT 2014)
9. 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL ITEMS (JAN 2017)

Offerors must complete annual representations and certifications on-line at <http://orca.bpn.gov> in accordance with FAR 52.212-3, "Offerors Representations and Certifications—Commercial Items." If paragraph (j) of the provision is applicable, a written submission is required.

The following contract clauses apply to this acquisition:

1. FAR 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)
2. VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)
3. VAAR 852.203-71 DISPLAY OF DEPARTMENT OF VETERAN AFFAIRS HOTLINE POSTER (DEC 1992)
4. VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)
5. VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)
6. VAAR 852.219-10 VA NOTICE OF TOTAL SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS SET-ASIDE (JUL 2016) (DEVIATION)

7. 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2017) VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)
8. 52.204-16 --COMMERCIAL AND GOVERNMENT ENTITY CODE REPORTING (JUL 2016)
9. 52.204-18 COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (JUL 2016)
10. 52.212-4 -- CONTRACT TERMS AND CONDITIONS -- COMMERCIAL ITEMS (JAN 2017)
11. 52.204-21 – BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)
12. 52.222-56 – CERTIFICATION REGARDING TRAFFICKING IN PERSONS COMPLIANCE PLAN (MAR 2015)
13. 52.217-8 – OPTION TO EXTEND SERVICES (NOV 1999)
14. 52.217-9 – OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

Addendum to FAR 52.212-1 INSTRUCTIONS TO OFFERORS--COMMERCIAL ITEMS
Submission of Quotes:

Quotes shall be received on or before 3:00 PM ET – March 9, 2018. All quotes shall be sent to the Contract Specialist Jason Phillip at jason.phillip@va.gov **Note:** Quotes received after the due date and time **shall not** be considered.

- (1) Quotes shall be based on the documents issued in the solicitation.
 - (a) Technical Questions: Questions of a technical nature must be provided in writing and shall be submitted by the prospective offerors only via e-mail to: jason.phillip@va.gov. The subject line must read: **Lease Compliance – Technical Questions**. Oral questions of a technical nature are not acceptable due to the possibility of misunderstanding or misinterpretation. **THE CUT-OFF DATE AND TIME FOR RECEIPT OF QUESTIONS IS February 16, 2018 at 3:00 PM ET.**
 - (b) Amendments: Amendments to this solicitation will be posted on FBO. FBO copies of the amendments will NOT be individually mailed or sent via email. No other notification of amendments will be provided. Potential Offerors are advised that they are responsible for obtaining and acknowledging any amendments to the solicitation. Failure to acknowledge an amendment may result in your proposal being considered non-responsive or unacceptable.
 - (c) System for Award Management (SAM): Federal Acquisition Regulations require that federal contractors register in the SAM database at <http://www.sam.gov> and enter all mandatory information into the system. Award cannot be made until the contractor has registered. Offerors are encouraged to ensure that they are registered in SAM prior to submitting their quotation.
 - (d) Restrictive or Proprietary Data: Contractors that include in their quotes data that they do not want disclosed to the public for any purpose, or used by the Government except for evaluation purposes shall:
 1. Mark the title page with the following legend:
This quote includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed-in whole or in part-for any

purpose other than to evaluate this quote. If, however, an Order is awarded to this Vendor as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets *[insert numbers or other identification of sheets]*; and

2. Mark each sheet of data it wishes to restrict with the following legend:
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this quote.

(e) Use of Advisors: Contractors are advised that VA contractor personnel may assist the Government during the Government's evaluation of Quotes. These persons shall be authorized access to only those portions of the quote and discussions that are necessary to enable them to provide specific technical advice on specialized matters or on particular problems. These individuals will be required to protect the confidentiality of any specifically identified trade secrets and/or privileged or confidential commercial or financial information obtained because of their participation in this evaluation. They shall be expressly prohibited from scoring, ranking or recommending the selection of a Vendor.

(f) Quote Preparation Costs: The Contracting Officer is the only individual legally authorized to commit the Government to the expenditure of public funds in connection with this procurement. The solicitation does not commit the Government to pay any costs for the preparation and submission of an offer in response to this solicitation.

(2) Quote Format

(a) General: The submission shall be clearly indexed and logically assembled. Each volume shall be clearly identified and shall begin at the top of a page. All pages of each volume shall be appropriately numbered and identified by the complete company name, date and solicitation number in the header and/or footer. All files will be submitted as either a Microsoft Excel file or an Acrobat (PDF) file or compatible as indicated in Table One (1) (below). Page size shall be no greater than 8 1/2" x 11". The top, bottom, left and right margins shall be a minimum of one inch each. Font size shall be no smaller than 12-point. Arial font is required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than 8-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line. Page numbers, company logos, and headers and footers may be within the page margins ONLY, and are not bound by the 12-point font requirement. Footnotes to text shall not be used. The use of hyperlinks or embedded attachments within the proposal is prohibited. The written quote including title page, detailed table of contents, preface, for Volume I Technical shall not exceed a total of 50 pages in size 12 Arial font. Volume II Price Quote shall not exceed a total of 20 pages in size 12 Arial font. Use graphic presentations where such use will contribute to the compactness and clarity of the quote. The solicitation with completed Pricing Schedule, the Draft Project Plan, and any Contractor Teaming Arrangement documentation will not be counted to include samples in the page limit.

(b) File Packaging: All the proposal files may be compressed (zipped) into one file entitled “proposal.zip” using WinZip version 6.2 or later version. The proposal files may also be submitted individually using the naming convention identified in Table One (1) (below).

(c) Content Requirements: All information shall be confined to the appropriate volume. The titles and file type requirements for each volume are shown in the Table below:

Table 1

Volume Number	Evaluation Factor	File Name	Page Limitations
Volume I	Technical	Tech.pdf	50
Volume II	Price	Price.xls	20
Volume III	Solicitation, Amendments, Offer, Award Documents and complete FAR 52.209-5 and 52.209-7	Certs.pdf	NONE

Volume I - Technical Requirements -- Offerors shall propose a detailed approach that addresses the following which will be considered in the Technical Evaluation:

- The Offeror shall provide a summary that details their technical strategy for completing the Lease Program Compliance IDIQ contract in accordance with the PWS.
- The Offeror shall provide a summary that outlines their approach for completing the Lease Program Compliance in accordance with the PWS; this should include all labor rates required.

Volume II – Price Requirement -- The Pricing Volume shall consist of the following which will be considered in the PRICE evaluation:

- The prices shall be Firm Fixed Price. The CLIN pricing shall be in accordance with the labor categories, rates, and proposed discount.
- The quote submitted shall be entered on the priced Pricing Schedule below. Any costs associated with Reports/Deliverables/Travel shall be included in the CLIN price and not separately priced.

PRICING SCHEDULE				
CLIN	DESCRIPTION	QUANTITY	UNIT	PRICE
0001	Task 1: PMP and Briefing	1	JB	
0002	Task 2: Maintaining and updating of the tracking and reporting system for lease status.	1	JB	

0003	Task 3: Review of lease package submissions for GREX uploading, including detailed analysis of scoring for each lease.	1	JB	
0004	Task 4: Lease process training and documentation support.	1	JB	
0005	Task 5: Lease Tracking System enhancements.	1	JB	
0006	Task 6: General program support and status reporting.	1	JB	
0007	Task 7: Updates to VA's Lease Scoring Template.	1	JB	
0008	Task 8: Data integrity reviews and updates.	1	JB	
0009	Task 9: Data integration with other systems.	1	JB	
0010	Task 10: General lease process flow review and documentation.	1	JB	
0011	Task 11: Studies related to the lease portfolio and/or delegation process.	1	JB	

- PERIOD FOR ACCEPTANCE OF QUOTES. The Contractor agrees to hold the prices in its quote firm for ninety (90) calendar days from the date specified for receipt of quotes.

Volume III – Solicitation, Offer and Award Documents and Certifications/Representations: Solicitation, Amendments, Offer, Award Documents and complete FAR 52.209-5 and 52.209-7.

This is an open-market combined synopsis/solicitation for services as defined herein. The government intends to award a contract as a result of this combined synopsis/solicitation that will include the terms and conditions set forth herein. To facilitate the award process, all quotes must include a statement regarding the terms and conditions herein as follows:

"The terms and conditions in the solicitation are acceptable to be included in the award document without modification, deletion, or addition."

OR

"The terms and conditions in the solicitation are acceptable to be included in the award document with the exception, deletion, or addition of the following:"

Offeror shall list exception(s) and rationale for the exception(s).

Point of Contact

Any questions or concerns regarding this solicitation should be forwarded in writing via e-mail to the Contract Specialist, Jason Phillip at jason.phillip@va.gov.