

**Department of Veterans Affairs
Southeast Louisiana Veterans Health Care System
Install Parking Bumpers Buildings 4 and 5 Parking Garages
2400 Canal St. New Orleans, LA**

**Firm Fixed Price Contract
Statement of Work
June 30, 2016**

1) GENERAL INFORMATION

- 1.1. Title of Project: Install Parking Bumpers in Buildings 4 and 5, Patient Parking Garage (N. Galvez St.) and Employee Parking Garage (N. Rocheblave St.).
- 1.2. Scope of Work: The contractor shall provide all resources necessary to accomplish the deliverables described in this statement of work (SOW), except as may otherwise be specified. This includes but is not limited to: Installing 1164 parking bumpers at Building 4 and 1167 parking bumpers at Building 5. Chemical mounting adhesive will be provided by the government and shall be used for securing the bumpers to the parking slab (use Superior Industries, Inc., #303 Bumper Mount, parking bumper mounting adhesive or approved equal). No drilling into the slab will be allowed. The parking bumpers will be painted and ready to install by the contractor. The contractor shall be responsible for any touch up painting required as a result of damage to the painted parking bumpers as a result of the installation.
- 1.3. Background: The parking garages in question are the main means of parking at the new VA facility located at the 2400 Canal Street campus. Building 4 provides for patient parking and Building 5 provides employee parking. Because the parking decks are constructed of precast concrete members, drilling into the parking decks will not be allowed. The goal of this project is to provide parking bumpers to all parking spaces in the new garages.
- 1.4 Performance Period: The contractor shall complete all work noted within this statement of work, issued drawings and specification seventy-five (75) calendar days from issuance of notice to proceed, unless otherwise directed by the Contracting Officer (CO). Work shall begin no more than fourteen (14) calendar days after issuance of notice to proceed. If the Contractor proposes an earlier completion date, and the Government accepts the Contractor's proposal, the Contractor's proposed completion date shall prevail. Work at the Government site is permissible, and expected, on Federal holidays or weekends, but subject to approval by Contracting Officer's Representative and/or the CO.
 - 1.1.1. Recognized Federal Holidays:
 - New Year's Day, January 1*
 - Martin Luther King Jr. Day, Third Monday in January
 - Washington's Birthday (President's Day), Third Monday in February

Memorial Day, Fourth Monday in May
Independence Day, July 4*
Labor Day, First Monday in September
Columbus Day, October 12*
Veterans Day, November 11*
Thanksgiving, Fourth Thursday in November
Christmas, December 25*

1.1.2. *Note: Federal Holidays that fall on a Saturday will be observed the Friday prior.
Holidays that fall on a Sunday will be observed the Monday following.

1.1.3. The anticipated work schedule will be restricted to weekends beginning 6:30 pm
Friday evening through 6:00 am Monday mornings.

1.4. Type of Contract: Firm Fixed Price Contract

2. CONTRACT AWARD MEETING

2.1. The contractor shall not commence performance on the tasks in this SOW until the Contracting Officer (CO) has conducted a kick off meeting, or has advised the contractor that a kick off meeting is waived.

2. DEFINITIONS:

- 2.1. Contracting Officer: The services to be performed under this contract are subject to the general supervision, direction, control and approval of the Contracting Officer.
- 2.2. VA Project Engineer/Contracting Officer's Representative (COR): The Contracting Officer's authorized representative at the construction site. The COR is responsible for protecting the Government's interest in the execution of the construction contract work. His duties include surveillance of all construction work to assure compliance with the contract documents, interpretation of the contract documents, approval of changed work, approval of all submittals, samples, shop drawings, etc.
- 2.3. Firm-Fixed Price (FFP) Contract: This term, as used herein, refers to the Contract(s) to perform all provisions and implementation of the project.
- 2.4. Contractor: This term, as used herein, refers to the Contractor under this contract or the FFP team.
- 2.5. National Electric Code (NEC)
- 2.6. National Fire Protection Association (NFPA)
- 2.7. American Society of Safety Engineers (ASSE)
- 2.8. Occupational Safety and Health Administration (OSHA)
- 2.9. American Society for Testing and Materials (ASTM)
- 2.10. Veterans Affairs (VA)
- 2.11. The Joint Commission (TJC)
- 2.12. Experience Modification Rating (EMR)

3. GENERAL REQUIREMENTS

- 3.1. For every task, the contractor shall identify in writing all necessary subtasks (if any), and associated costs by task.
- 3.2. All written deliverables shall be phrased in layperson language. Statistical and other

technical terminology shall not be used without providing a glossary of terms.

- 3.3. The Government shall complete their review of deliverables within five (5) business days from date of receipt. The Contractor shall have ten (10) business days to deliver the final deliverable from date of receipt of the government's comments.
- 3.4. The Contractor shall provide daily logs reporting on the following items: risk review, planned work for the day, tasks accomplished. Logs shall be created for each day work occurs.
- 3.5. The Contractor shall meet with CO and the Contracting Officer's Representative (COR) on a weekly basis to report on topics such as: schedule review, risk review, tasks accomplished in the past week, explanation of tasks not accomplished as expected; tasks to be accomplished in the upcoming week.
- 3.6. Invoicing paperwork, reports and certifications shall be submitted and received by government prior to payment of each line item.
- 3.7. The contractor shall have an Experience Modification Rating (EMR) less than 1.0 at the time of bid. The contractor must provide proof of this rating to the Contracting Officer prior to bid opening.
- 3.8. Work to be completed:

3.8.1.1 Building 4 shall have the following bumpers installed at the parking spaces:

	Std. Pkg. Spaces	HC Std. Pkg. Spaces	HC Van Pkg. Spaces
Level 1	79		16
Level 2	157	15	---
Level 3	157	15	---
Level 4	157	15	---
Level 5	157	15	---
Level 6	157	15	---
Roof	88	4	---

3.8.1.1.1. The contractor shall provide all labor, equipment and tools necessary to accomplish this task.

3.8.1.2 Building 5 shall have the following spaces:

	Std. Pkg. Spaces	HC Std. Pkg. Spaces	HC Van Pkg. Spaces
Level 1	---	---	---
Level 2	183	1	6
Level 3	177	5	---
Level 4	177	5	---
Level 5	177	5	---
Level 6	177	5	---
Roof	115	5	---
Fleet Pkg.	75	2	2
Transitional Living	44	2	1

3.8.1.2.1. The contractor shall provide all labor, equipment and tools

necessary to accomplish this task

3.8.2. All work shall be completed 6:30 pm Friday evening through 6:00 am Monday mornings or on a Federal Holiday.

3.8.3. Access to the space shall be granted by the VA.

4. SPECIFIC MANDATORY TASKS AND ASSOCIATED DELIVERABLES

4.1. The Contractor shall submit the following preconstruction documentation for approval prior to issuance of notice to proceed (NTP):

4.1.1. Initial Register

4.1.1.1. Log shall contain a listing of all deliverables noted herein as well as noted within the specifications.

4.1.1.2. The Contractor shall submit one (1) hard copy and one (1) electronic copy

4.1.1.2.1. The Contractor shall be responsible for furnishing updated copies of the Submittal log as changes are made within five (5) days of any changes.

4.1.2. Site Specific Safety Plan

4.1.2.1. This plan shall include at a minimum

4.1.2.1.1. List of key personnel and points of contact from the Contractor

4.1.2.1.2. Reporting

4.1.2.1.3. Construction Barriers

4.1.2.1.4. Housekeeping

4.1.2.1.5. Maintenance

4.1.2.1.6. Hazards that may be present during construction, either as part of the construction or in the vicinity of the construction

4.1.2.1.7. Smoking

4.1.2.1.7.1. There is no smoking allowed on site. Contractors will be instructed by COR on designated smoking facilities and alternate sites

4.1.2.1.8. Fire Protection 4.1.2.1.8.1.
Fire Safety Plan

4.1.2.1.8.1.1. It shall include at a minimum:

4.1.2.1.8.1.1.1. Specifics pertaining directly to the Construction Site

4.1.2.1.8.1.1.2. The Contractor shall provide a general risk prevention checklist

4.1.2.1.8.1.1.3. Flammable and Combustible Material checklist

4.1.2.1.8.1.1.4. Proof of employee safety orientation

4.1.2.1.8.1.2. The Contractor shall provide one electronic and one hard copy to the CO and COR for review and approval.

4.1.2.1.9. Emergency Management Plan

4.1.2.1.9.1. Emergency Evacuation

4.1.2.1.9.2. Emergency Room/ Hospital Identified 4.1.2.1.9.2.1.

Note, while the facility where work shall occur is a healthcare facility, it is not an emergency care facility. Emergency services cannot be provided at this location and must be sought at another facility. If medical staff are on site, they may be able to provide humanitarian aid by way of stabilization.

4.1.2.1.9.3. Inclement weather

4.1.2.2. The Contractor shall deliver one (1) hard copy and one (1) electronic copy to VA for review.

4.1.2.3. Due date for initial review by VA staff: 10 calendar days after award

notice issuance

4.1.3. Employee OSHA Certifications

4.1.3.1. The Superintendent/onsite manager (OSHA “Competent Person”) – 30-Hour or higher

4.1.3.2. All other construction staff – 10- Hour or higher certification

4.1.3.3. Submissions of OSHA Certifications can be made via electronic submission.

4.1.3.4. All OSHA certifications must be received by the Government prior to commencement of work.

4.1.4. Schedule of Values

4.1.4.1. Shall be submitted electronically (one copy).

4.1.4.2. Subject to approval by VA COR prior to acceptance.

4.1.5. Construction Schedule

4.1.5.1. One (1) hard copy and one (1) electronic copy in MS projects format

4.1.6. Demolition/Installation Phasing Plan

4.1.6.1. This should include:

4.1.6.1.1. Street closure locations and equipment set ups

4.1.6.2. Shall be submitted to CO and COR within 10 calendar days of award.

4.1.6.3. Phasing plan is subject to approval of CO and COR prior to implementation. The contractor shall, at no cost to the Government, perform the necessary revisions to the phasing plan as needed.

4.1.7. Roof of EMR rating less than 1.00. Ratings above 1.00 are grounds for contract termination.

4.2. The Contractor shall submit the following construction documentation for approval prior to implementation:

4.2.1. Hot Work Permit

4.2.1.1. All hot work must be requested by the contractor for approval prior to the commencements of any potential hot work.

4.2.1.2. Hot work includes, but is not limited to: any tasks that may produce a spark, involve grinding, burning, welding

4.2.1.3. A fire watch log must accompany all executed hot work permits

4.2.1.3.1. Note: a fire watch log is mandatory for any work that may negatively impact the fire suppression or warning systems.

4.2.1.3.2. Entries must be made in instances of no more than once every 60 minutes.

4.3. The Contractor shall submit the following construction documentation for approval during Construction:

4.3.1. OSHA 300 Logs

4.3.1.1. Submitted electronically to CO and COR

4.3.1.2. Submissions shall be made monthly. See SAFETY REQUIREMENTS specification for more details.

4.3.2. Pay Applications

4.3.2.1. Submitted electronically to CO and COR prior to submission for payment

4.3.2.2. Pay applications must be approved by CO or COR prior to payment submissions.

4.3.2.3. Pay applications shall be subject to rejection or delay if contractor fails to submit all documents required within the affected time frames.

4.3.3. Construction Waste Tonnage Report

4.3.3.1. Submitted electronically to CO and COR

4.3.3.2. Submissions shall be made monthly.

4.3.3.3. Report shall include, at a minimum the following

- 4.3.3.3.1. Total tonnage collected for the reporting period
- 4.3.3.3.2. Total tonnage collected for the project to date
- 4.3.3.3.3. Disposal method
- 4.3.3.3.4. Contractor personnel certifying the report submitted
- 4.4. The Contractor shall submit the following construction documentation for approval post Construction:
 - 4.4.1. As Builts
 - 4.4.1.1. The contractor shall submit one (1) electronic and one (1) hard copy.
 - 4.4.1.2. As Builts shall be submitted to the VA no later than fourteen (14) calendar days after substantial completion for the project.
 - 4.4.1.3. Hard copies of As Builts sheet size shall be 30"x42", shall be "to scale" and legible when printed at that size
 - 4.4.1.4. Electronic copies of As Builts shall be completed via CAD (AutoCAD 2010 or later) file.
 - 4.4.2. Warranty Information
 - 4.4.2.1. Warranty information shall be received from the contractor no later than seven (7) calendar days after total acceptance of work.
 - 4.4.2.2. Warranty period shall be either one (1) year from date of acceptance or shall adhere to manufacturer's warranty, whichever is greater.
 - 4.4.2.3. Warranty shall cover all materials used and installed during the project and shall also cover all workmanship.
 - 4.4.2.4. All warranty information shall be signed by the Contractor and submitted (one hard copy and one electronic copy) to the COR.
 - 4.4.2.5. All warranty information shall be submitted via one (1) hard copy and one (1) electronic copy. The hard copy submission shall be bounded, 8 ½" by 11" submission.
- 4.5. The contractor shall perform all work as cited in the General Requirements pertaining to the complete removal of the signage noted and repair of surrounding areas associated with the removal of the noted signage.

5. EVALUATED OPTIONAL TASKS AND ASSOCIATED DELIVERABLES

5.1. N/A

6. SCHEDULE FOR DELIVERABLES

- 6.1. The contractor shall complete the Delivery Date column in Attachment A for each deliverable specified. All deliverables, unless otherwise noted within the SOW, construction documents or specifications, shall adhere to the schedule described in Attachment A.
- 6.2. Unless otherwise specified, the number of draft copies and the number of final copies shall be the same.
- 6.3. If for any reason any deliverable cannot be delivered within the scheduled time frame, the contractor is required to explain why 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.

7. CHANGES TO STATEMENT OF WORK

- 7.1. Any changes to this SOW shall be authorized and approved only through written correspondence from the CO. A copy of each change will be kept in a project folder along with all other products of the project. Costs incurred by the contractor through the actions of parties other than the CO shall be borne by the contractor.

8. REPORTING REQUIREMENTS

- 8.1. During the service, the contractor shall report any changes in delivery requirements/problems to the COR.
- 8.2. Upon final delivery of services, for each service, the contractor will notify the COR.

9. TRAVEL

- 9.1. The contractor is responsible for providing transportation/travel for all materials, supplies, personnel and all items needed to complete this work. Parking will not be provided on site.

10. GOVERNMENT RESPONSIBILITIES

- 10.1. The government shall provide, at the contractor's request, access to all relevant areas associated with the completion of this project. Requests for access shall be made to the government in writing no fewer than two (2) business days in advance.
- 10.2. Removing Employees for Misconduct or Security Reasons. The Government may, at its sole discretion, direct the contractor to remove any contractor employee from U.S. VA/VHA facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under any Contract awarded. The Contracting Officer will provide the contractor with a written explanation to support any request to remove an employee.

11. CONTRACTOR EXPERIENCE REQUIREMENTS

- 11.1. All qualified, experience, and license personnel for the service will be provided for by the contractor. The contractor will be responsible for presenting all documentation noting their experience concerning traffic marking, exterior building painting, and use of the materials specified in this scope of work and associated specifications.
- 11.2. Qualifications of Key Personnel
 - 11.2.1. The Contractor shall provide, at minimum, a listing of the following key personnel who will work on this project:
 - 11.2.1.1. Project Manager/Team Lead
 - 11.2.1.2. Superintendent
 - 11.2.1.3. The Contractor shall identify, by name, the key management and technical personnel who will work under this project at the time the work is being negotiated. If a key person becomes unavailable to complete the request, the proposed substitutions of key personnel shall be made only as approved directed by the Contracting Officer and the COR. The Government will not dictate specific experience and education requirements of the employees initially proposed to perform the work stated herein. The Contractor shall submit a resume of qualifications to the COR for key personnel and all other

direct employees proposed for the project. All Contractor employees will be approved by the COR prior to bringing on duty. If, at any time from date of award to the end of the contract, non-key Contractor personnel are no longer available, the VA reserves the right to review qualifications of proposed replacement personnel and to reject individuals who do not meet the qualifications set forth. Team personnel proposed by the Contractor should possess some of the following knowledge and/or skills.

- 11.2.1.4. The Contractor must notify VHA in advance and VHA will approve or reject proposed contractor key personnel for the performance of this contract.
- 11.2.1.5. The Contractor shall submit a resume of qualifications to the COR and CO for key personnel and all other direct employees proposed for the project. All Contractor employees will be approved by the COR and CO prior to bringing on duty. If, at any time from date of award to the end of the contract, Contractor personnel are no longer available, the VHA will approve the qualifications of proposed replacement personnel and will reject individuals who do not meet the qualifications set forth herein. The Contractor must inform the COR and CO when personnel are removed from the contract for any reason. The Contractor shall remove any employee from the performance of this contract within five (5) workdays of receiving notice from the Contracting Officer that the employee's performance is unsatisfactory. All Contractor employees are subject to immediate removal from performance of this contract when they are involved in a violation of the law, VA security, confidentiality requirements and/or other disciplinary reasons.
- 11.2.1.6. The VHA shall not be liable for further payment of any Contractor employee that VHA requires the Contractor to remove from the performance of this contract. VHA's payment liability, for unsuitable Contractor employees, ends five working days after Contractor's receipt of "removal request" for unsatisfactory performance and immediately for any violation of law, VA security, confidentiality requirements and/or other disciplinary action.
- 11.2.1.7. Experience
 - 11.2.1.7.1. The Contractor must demonstrate past experience involving exterior structural painting, traffic marking installation, crosswalk installations, use of thermoplastic and traffic paints within the past five (5) years similar in scope and size. This can be demonstrated through:
 - 11.2.1.7.1.1. Past performance questionnaires
 - 11.2.1.7.1.2. Past Project listing indicating
 - 11.2.1.7.1.2.1. Points of Contact
 - 11.2.1.7.1.2.2. Contract title
 - 11.2.1.7.1.2.3. Contract length
 - 11.2.1.7.1.2.4. Contract start and completion date
 - 11.2.1.7.1.2.5. Project Estimated Costs
 - 11.2.1.7.2. The Contractor may also submit other projects as they relate to the Department of Veterans Affairs or other Federal Agencies of similar size, scope or nature.

12. CONTRACTOR PERSONEL SECURITY REQUIREMENTS

- 12.1. All contractor personnel will be required to sign in/sign out with VA Police Services prior to entering/existing the premises. A visitor's badge will be issued by VA Police; this badge must be worn at all times while on the premises.
- 12.2. Contractor personnel shall, at no point, be unescorted on VA property. The contractor shall be responsible for coordinating necessary escort needs with the government no fewer than two (2) business days in advance. The contractor may have designated personal act as escorts on the contractor's behalf by undergoing a background check and receiving VA badging and access. Arrangements can be made with the COR. Access and badging is subject to approval.

13. PROTECTION OF PERSON AND PROPERTY

- 13.1. The contractor expressly undertakes', both directly and through its subcontractor(s), to take every precaution at all times for the protection of persons and property, including Medical Center employees and property and its own.
- 13.2. The contractor shall be responsible for initiating, maintaining and supervising all safety precautions and programs in connection with the work.
- 13.3. The contractor shall continuously maintain adequate protection of all work from damage and shall protect the Medical Center property from injury of loss arising in connection with this contract. The contractor shall make good any such damage, injury or loss, except as may be by agents or employees of the Medical Center.
- 13.4. In an emergency affecting the safety or life of individuals, or of the work, or of adjoining property, the contractor, without special instruction or authorization from the Medical Center, is hereby permitted to act, at the contractor's discretion, to prevent such threatened loss or injury. Also, should the contractor, in order to prevent threatened loss or injury, be instructed or authorized to act by the Medical Center, he shall so act, without appeal. Any additional compensation or extension of time claimed by the contractor on account of any emergency work shall be determined by mutual agreement.

14. INFORMATION SECURITY

- 14.1. GENERAL
 - 14.1.1. 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.
- 14.2. VA INFORMATION CUSTODIAL LANGUAGE
 - 14.2.1. 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).

- 14.2.2. 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.
- 14.2.3. 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.
- 14.2.4. 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.
- 14.2.5. 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.
- 14.2.6. 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.
- 14.2.7. 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.

- 14.2.8. 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.
- 14.2.9. 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.
- 14.2.10. 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.
- 14.2.11. 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.
- 14.2.12. 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.
- 14.3. **INFORMATION SYSTEM DESIGN AND DEVELOPMENT**
- 14.3.1. 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 COTR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.
- 14.3.2. The contractor/subcontractor shall certify to the COTR 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.
- 14.3.3. 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.

- 14.3.4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
- 14.3.5. 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.
- 14.3.6. 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.
- 14.3.7. The contractor/subcontractor agrees to:
 - 14.3.7.1. 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:
 - 14.3.7.1.1. The Systems of Records (SOR); and
 - 14.3.7.1.2. The design, development, or operation work that the contractor/subcontractor is to perform;
 - 14.3.7.2. 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
 - 14.3.7.3. 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.
- 14.3.8. 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.
 - 14.3.8.1. “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.
 - 14.3.8.2. “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.

14.3.8.3. "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.

14.3.9. 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.

14.3.10. 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 30 days.

14.3.11. 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 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within ____ days.

14.3.12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 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.

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

14.4.1. 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.

14.4.2. 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.

- 14.4.3. 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.
- 14.4.4. 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, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.
- 14.4.5. 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.
- 14.4.6. 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.

14.4.7. 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.

14.4.8. 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:

14.4.8.1. Vendor must accept the system without the drive;

14.4.8.2. 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

14.4.8.3. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

14.4.8.4. 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;

14.4.8.4.1. 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

14.4.8.4.2. 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 preapproved and described in the purchase order or contract.

14.4.8.4.3. 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.

14.5. SECURITY INCIDENT INVESTIGATION

14.5.1. 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.

14.5.2. 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.

14.5.3. 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.

14.5.4. 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.

14.6. LIQUIDATED DAMAGES FOR DATA BREACH

14.6.1. 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.

14.6.2. 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.

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

14.6.3.1. Nature of the event (loss, theft, unauthorized access);

14.6.3.2. Description of the event, including:

14.6.3.2.1. Date of occurrence;

- 14.6.3.2.2. Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 14.6.3.3. Number of individuals affected or potentially affected;
- 14.6.3.4. Names of individuals or groups affected or potentially affected;
- 14.6.3.5. 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, plain text;
- 14.6.3.6. Amount of time the data has been out of VA control;
- 14.6.3.7. The likelihood that the sensitive personal information will or has been compromised (Made accessible to and usable by unauthorized persons);
- 14.6.3.8. Known misuses of data containing sensitive personal information, if any;
- 14.6.3.9. Assessment of the potential harm to the affected individuals;
- 14.6.3.10. Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
- 14.6.3.11. 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.
- 14.6.4. 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 \$2000 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
 - 14.6.4.1. Notification;
 - 14.6.4.2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
 - 14.6.4.3. Data breach analysis;
 - 14.6.4.4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
 - 14.6.4.5. One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
 - 14.6.4.6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.
- 14.7. SECURITY CONTROLS COMPLIANCE TESTING
 - 14.7.1. 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 working-day's 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.
- 14.8. CONFIDENTIALITY AND NONDISCLOSURE
 - 14.8.1. It is agreed that:

- 14.8.1.1. 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 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.
- 14.8.1.2. 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 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.
- 14.8.1.3. 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.

Attachment A to the Statement of Work

DELIVERABLE	DELIVERABLE DATE
Proof of EMR below 1.00	Within 5 Calendar days of award intent
Key Personnel Listing	Within 5 Calendar Days After Award
Site Specific Safety Plan	Within 10 Calendar Days After Award
Submittal Register	Within 10 Calendar Days After Award
Phasing Plan	Within 10 Calendar Days After Award
Copies of OSHA Certification	Within 10 Calendar Days After Award
Construction Schedule	Within 15 Calendar Days After Award
Schedule of Values	Within 15 Calendar Days After Award
Completion Of All Work	Within 75 Calendar Days After Notice To Proceed
OSHA 300 Logs	Monthly, By The 30 th Of Each Month
Monthly Pay Application	Monthly, By The 30 th Of Each Month
Construction Waste Tonnage Report	Monthly, By The 30 th Of Each Month
As Builts	Within 14 Calendar Days After Substantial Completion
Project Warranty Information	Within 10 Calendar Days After Completion Of Construction