STATEMENT OF OBJECTIVES (SOO)

Conference Room Management System (CRMS)
Southeast Louisiana Veterans Health Care System (SLVHCS)

June 21, 2016

1.0 PURPOSE

1.1 The purpose of this Statement of Objectives (SOO) is to present the performance objectives and establish the design framework for the procurement of a Conference Room Management System (CRMS) to be implemented at the Southeast Louisiana Veterans Health Care System (SLVHCS), in New Orleans, LA. It is the intent of SLVHCS to provide maximum flexibility to each Offeror to propose an innovative design and execution approach and solutions using proven processes, methods, standards, and technologies. The purpose of the solution is to provide an automated, flexible, and scalable architecture to view, schedule, and request support for events in over 100 conference rooms, for approximately 3,000 employees and 300 adminstrators. This solution will enhance SLVHCS' ability to meet and collaborate, effectively communicate requests for event support/notifications, and manage/administer automated workflow processes and controls.

1.2 Offerors shall use this SOO, as the basis for preparing their quote.

2.0 INTRODUCTION

2.1 The goal of the CRMS is to create efficiencies and improvements to the methods by which staff collaborate to utilize, support, and promote events and associated resources. The solution will centralize communications through a Client-side Microsoft Outlook (2010) and web based interface for conference room event viewing, reservation/booking, and support request management system that will be installed once approved or waiver obtained in One-VA Technical Reference Model (TRM) . The software will be installed, administrated and monitored by VA OI&T staff. Key attributes of the software solution include:

2.1.1 Users can search/find the conference room that meets their search criteria (location, size, equipment, etc.) via existing Microsoft Outlook 2010 client software

2.1.2 Administrative controls to provide various levels of authority in booking, deleting, and grant permissions for select users and rooms

2.1.3 See peoples' schedule and availability simultaneously, with a Microsoft Outlook 2010 integration solution
2.1.4 View conference room building/room numbers, number of seats, audio-visual and telephonic equipment available, prior to booking
2.1.5 Prevent double-booking of conference rooms
2.1.6 VA will locally administer user rights-based groups to view, book, bump/delete, and in select cases authorize conference room events
2.1.7 Embed workflow processes and controls to easy restrict executive or special rooms or require authorization
2.1.8 Enable users to reserve/request equipment, catering, transportation, room set-up/tear-down, security/access, and other ancillary event support services and/or equipment
2.1.9 Track (date-time stamp) event bookings and deletions
2.1.10 The software system does not need to integrate with HVAC, lighting, facilities, or signage systems
2.1.11 The software system will not be used to display/house electronic patient health record information, but it may include the name and phone number of the person(s) responsible for booking/hosting events, which could be considered personally identifiable information
2.1.12 A system that is user-friendly, intuitive and easy to navigate

2.2 The intent of this procurement is to allow SLVHCS' workforce to schedule conference rooms and events, to request/notify others of a variety of pre/post-event product and service support needs, plus allow SLVHCS staff internal administrative controls for various levels of user rights administrator groups.

2.3 The technology-enhanced system will include the necessary tools for administrators to deliver efficient, comprehensive and continuous messages to staff to provide immediate improvement to the efficient use of government resources and contribute to significantly improved workflow efficiencies and employee experiences.

3.0 BACKGROUND

3.1 Designed as a monument to our country's military veterans, SLVHCS' VA Medical Center, currently under construction, is located on a 30-acre campus in New Orleans, LA. The New Orleans VAMC campus footprint includes multiple building structures which are being activated incrementally. Upon completion, the medical campus will have over 100 conference rooms, computer labs, auditoriums, and event calendars that will need to be included in the system solution.

4.0 PERFORMANCE OBJECTIVES

4.1 As a direct result of the implementing the CRMS, SLVHCS expects to achieve the following:

4.1.1 Optimized workflow process by allowing real-time event scheduling changes to be communicated to staff through a Microsoft Outlook integrated product.

4.1.2 System Availability and up-time and availability are paramount, with the goal of 100% uptime 24x7x365. Back-up or contingency measures for system availability should be well documented in proposals, including technical point of contact for integration and post-integration support.

4.1.3 Hierarchical authentication/authorization controls, with SLVHCS administering User rights, based on the role (employee event viewer, scheduler, and administrators).

4.1.4 Per the May 5th, 2015 memorandum from the VA Chief Information Security Officer (CISO) FIPS 140-2 Validate Full Disk Encryption (FOE) for Data at Rest in Database Management Systems (DBMS) and in accordance with Federal requirements and VA policy, database management must use Federal Information Processing Standards (FIPS) 140-2 compliant encryption to protect the confidentiality and integrity of VA information at rest at the application level. If FIPS 140-2 encryption at the application level is not technically possible, FIPS 140-2 compliant full disk encryption (FOE) must be implemented on the hard drive where the DBMS resides. Appropriate access enforcement and physical security control must also be implemented. All instances of deployment using this technology should be reviewed to ensure compliance with VA Handbook 6500 and National Institute of Standards and Technology (NIST) standards. *It is the responsibility of the system owner to work with the local CIO (or designee) and Information Security Officer (ISO) to ensure that a compliant DBMS technology is selected and that if needed, mitigating controls are in place and documented in a System Security Plan (SSP).*

4.1.5 Anticipated period of performance for support services is October 1, 2016 to September 30, 2017 with three one-year options through March 6, 2020. Support services begin when final software installation.

4.2 Achieve Optimal Results through Best Practices

The CRMS is expected to be a central feature in the communications and workflow processes for staff members and, like the medical technology used by staff personnel while providing patient care, the CRMS shall be delivered free of any defects and the installation should be compliant with the industry's "best practices".

4.3 Comply with Applicable Laws and Regulations

It is important that all systems, equipment, peripherals, and components meet the standards delineated by applicable laws and regulations, such as Section 508 Amendment to the Rehabilitation Act of 1973 and others. In recognition and support of the "Electronic and Information Accessibility Standards" defined by Section 508 of the Rehabilitation Act, the offeror should include published accessibility self-assessments of proposed products using Voluntary Product Accessibility Templates (VPAT) and/or Government Product Accessibility Templates(GPAT) when available. See Section 10 (References) for a complete list.

4.4 Support the VA's Green Management Program

The Green Management Program leads VA's efforts to reduce the agency's ecological footprint, complying with federal mandates and supporting the President's commitment to ensure that the Federal Government leads by example. The designed and implemented system is expected to incorporate technology that possesses as many of these features as possible.

5.0 SCOPE OF WORK

5.1 General

5.1.1 SLVHCS CRMS task order will encompass the complete range of activities and services required to successfully achieve the objectives presented in the SOO. Under this task order, the contractor, as an independent entity and not an agent or employee of the Government, shall furnish to the Government all necessary labor, services, and materials (except as specified by the Government) required to design, develop and provide maintenance support for the SLVHCS CRMS.

5.1.2 The operating system must be equivalent to Windows 7 or newer.

5.1.3 System Users should have readily available access to conference room resources (room seating capacity, AV system(s), computers, podiums and telephonic equipment available, restrictions and special permissions for reservations/use), plus job-aids/resources to help standardize system usage by all User types.

5.1.4 The software must be compliant or possess the ability to be compliant with the Office of Information Technology One VA Technical Reference Model (TRM).

6.0 DELIVERABLES

Deliverables will be established in the Quality Assurance Surveillance Plan, Offerors quote, and subsequent firm fixed-priced task order. Contractor shall deliver all software to the Southeast Louisiana Veterans Health Care System (SLVHCS), 2400 Canal St, New Orleans, LA 70119 by September 30, 2016. Deliver materials to job in manufacturer's original sealed containers with brand name marked thereon. Package the software products to prevent damage or deterioration during shipment, handling, storage, and installation. Maintain protective covering in place and in good repair until removal is necessary. Deliver specified items only when the site is ready for installation work to proceed. Store software products in dry condition inside the enclosed facilities. Any government requested delayed delivery up to 90 days after initial award delivery date, shall be at no additional cost to the Government.

A pre-delivery meeting will be conducted 60 days prior to initial award delivery date for verification of delivery. Delivery will be coordinated through the COR.

The Contractor shall provide, at no charge, two (2) complete and unabridged printed copies and one (1) electronic version (CD) of operator manuals, service manuals, and troubleshooting guides. Additionally, the Contractor shall provide free of charge any upgrades to these documents. These manuals and documentation shall contain the diagnostic codes, commands, and passwords utilized in CRMS system administration of software.

The vendor shall provide a one-year warranty, on all software and labor, with the option of extending the warranty for a period of three years. The warranty shall include all travel and shipping costs associated with any warranty repair. The warranty should begin once the software is installed.

The vendor shall provide answers to the IT integration questionnaire with their proposal. See attachment A.

7.0 PROJECT MANAGEMENT AND GOVERNANCE

7.1 Installation Support & Hours

Hours will be from 8:00 am – 4:00 pm – Monday through Friday except holidays unless negotiated and approved in advance by the contracting officer (CO). The contractor shall ensure that software is operational before turning over the project to maintenance

phase. The government will install the software. Contractor shall provide support such as guidance, technical advice, or reference information, as needed.

The contractor shall place an individual or group in place on-site to work closely with the site COR and/or Project Manager to coordinate and or help with scheduling the installation of associated software components.

The contractor must inform the COR, or Contracting Officer when any personnel is removed from contract within 2 workdays of receiving notice unsatisfactory performance of contract employee. 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.

Final Approved Schedule: 10 Days after Award. Network Design Plan: 30 Days after Award. Physical Installation: 75 Days after Award, but the installation cannot occur until the Network Plan is approved by the COR. Implementation: 75 Days after Training.

7.4 Training

The contractor shall provide an agreed upon number of user training classes to an unlimited staff during normal working hours and one other shift to be determined. The training will cover the proper use of the software and should be provided by a certified trainer for the equipment being installed. Copies of the operator and maintenance/service manuals shall be provided upon completion of project. The contractor shall provide a training program and job aids for each SLVHCS employee user group (CRMS administrators, medical media, OI&T, Emergency Management, and Police Services). All training for the software shall be included with the purchase. Contractor shall offer training and documentation/resources needed for all Users. If interim patches/upgrades are made to the system, training material shall be added and updated to ensure that training resources are kept current.

7.5 Maintenance & Warranty

Maintenance services shall be performed on an on-call basis. At a minimum, during normal working hours, Monday through Friday, 8:00 a.m. – 4:00 p.m. CST (excluding holidays observed by the Government), the Contractor shall respond to verbal or written requests for service calls. The Contractor shall respond to the written or verbal service all within two (2) business days and the repair services shall be completed within five (5) business days after the initial written or oral notification. Warranty to begin after software has been placed in use by the Vendor. Vendor to provide optional cost for 3

year extended warranty. Warranty timeline is subject to change due to actual activation date.

7.6 Post Installation Inspection

Post Installation Inspection will consist of verifying proper software installation to make sure that software is properly works s integrated with VA's IT systems. Inspection of units will be conducted by COR, Public Affairs Office, Emergency Management Service, Facilities Management Service; and Medical Media or any Integrated Project Team(IPT) representatives prior to release to SLVHCS. The Contractor shall conduct a joint inspection with the COR once all software has been delivered and installed by VA OI&T. The COR shall inspect all phases of delivery and provide a punch list of any and all missing or damaged products. Contractor shall provide dates of completion of punch list items and replacement parts and/or short ship items from the manufacturer(s). The COR shall ensure the software is installed properly is completed satisfactorily prior to acceptance. Disputes shall be resolved by the Contracting Officer.

7.7 Other Requirements

Returns and Credit Allowances: Must be in writing by SLVHCS and must be done within 60 days of receipt of merchandise unless concealed damage, defective or covered under warranty.

OI&T to install software that is approved or waiver obtained in One-VA Technical Reference Model (TRM) under the direct supervision of VA's OIT staff.

Contractor is responsible for notifying COR for escorting duties prior to arriving at the facility for post installation inspection. Contractor personnel shall check in with VA Police upon arrival and departure each day. All contractor personnel must provide one form of valid picture identification at the time of check-in to receive a visitor's badge. Badges must be worn above the waist and visible at all times while on the jobsite. All contractor personnel will be accompanied by a cleared member of the contractor (PIV cardholder) or SLVHCS representative at all times while on the jobsite. All contractor personnel must turn-in their badges at the end of each day.

8.0 Information Security

In accordance with Handbook 6500.6 Contract Security (March 12, 2010) include this contract security language into the Statement of Work (SOW) immediately following the security clause section: ***"A&A requirements do not apply--Security Accreditation Package is not required".***

8.1 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.

8.2 Confidentiality and Nondisclosure

8.2.1 It is agreed that:

8.2.2 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.

8.2.3 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.

8.2.4 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

Southeast Louisiana Veterans Healthcare System (SLVHCS)
Manufacturer Disclosure Statement Questionnaire

Information provided on this form is intended to assist professionals knowledgeable with SLVHCS' IT, security, and risk assessment processes and systems, for the management of IT and security issues and proposal selection. This questionnaire should be submitted as part of your complete proposal package.

Use the last page to expand on your answers to any of the questions below, as needed.

This software will *not* be used to manage any Electronic Protected health Information (ePHI).

Manufacturer:_____
_____

Software Name:_____ Software Version:_____Release Date:_____

Manufacturer or Representative Contact Information	Name:	Title:	Department:
	Company Name:	Telephone #:	E-Mail:

OPERATING SAFEGUARDS

1. Does the software being installed require Active X components to run? Yes___
   a. Are the Active X components digitally signed and recognized as trusted? No___
   b. What are the expiration dates of your signatures? N/A___

   Comment: Yes___
   _____ No___
   N/A___
2. Does the software require special Drivers not included already provided by the operating system? Yes___
   a. Are the drivers digitally signed? No___
   b. Does it require additional hardware attached to the computer? N/A___
   c. If applicable, how does the hardware connect? (USB, Serial, Wireless, etc.) Yes___

   Comment: No___
   _____ N/A___
   Yes___
   No___
   N/A___
   Yes___
   No___

N/A___
Yes___
No___
N/A___

3. Is the software required to be installed locally on any machine for it to interface the application or server?
   Answer:_____
   _____
4. Does your application require a particular version of Microsoft Internet Explorer or can it work on any version?
   Answer:_____
   _____
5. Does your application require a particular version of Microsoft Outlook, or can it work on any version?
   Answer:_____
   _____
6. Does your application require a particular version of Flash or can it work on any version?
   Answer:_____
   _____
7. Has your software passed the Application Compatibility List? Yes___ No___ N/A___
8. Can your application run in 32 or 64 bit environments?
   Answer:_____
   _____
9. Has your application been tested and performs well on Windows 7 operating systems? Yes___ No___ N/A___
   Comment:
   _____
10. Has your application been tested on MACINTOSH operating systems? Yes___ No___ N/A___
11. Can your server be virtualized in environments such as VMWare? Yes___ No___ N/A___
    a. If applicable, what specialized components within the server preclude it from being virtualized?
       Answer:
       _____
12. Does the server environment require a particular operating system to run? Yes___ No___ N/A___
    a. What server platform and operating system does this require?
       Answer:
       _____
    b. Can the Server have critical patches applied as needed or do the patches need approval by the vendor prior to them being applied without affecting the stability of the application? Yes___ No___
       Comment:
       _____

13. Does the server require access to any databases? N/A___
    a. Is there a particular Database Operating System?
    Comment: Yes___
    _____ No___
    b. What type of interface does it require (ODBC, HL7 Bi-directional support)? N/A___
    Comment: Yes___
    _____ No___
    N/A___

    N/A___
14. If applicable, what are the storage space requirements?
15. Answer:_____
    _____
16. Does the device have an integral data backup capability (i.e., backup onto media such as tape, disk)? Yes___ No___
    N/A___
    a. If applicable, what are the necessary files needed to be backed up?
    Answer:_____
    _____

ADMINISTRATIVE SAFEGUARDS

17. Does manufacturer offer operator and technical support training or documentation on device security features?
    Answer:_____
    _____
18. What underlying operating system(s), including version number, are used by the device?
    Answer:_____
    _____

PHYSICAL SAFEGUARDS

19. Does the system have an integral data backup capability (i.e. backup onto removable media such as tape/disk?)
    Answer:_____
    _____
20. Can the system boot from uncontrolled or removable media (i.e. a source other than an internal driver or memory component)?
    Answer:_____
    _____

TECHNICAL SAFEGUARDS

21. Can software be serviced remotely (i.e. maintenance activities performed by service person via network or remote connection)?

    Answer:_____

    _____

    a. Can the device restrict remote access to specific devices or network locations (e.g. specific IP addresses)? Yes___ No___ N/A___
    b. Can the device log provide an audit trail of remote-service activity? Yes___ No___ N/A___
    c. Can security patches or other software be installed remotely? Yes___ No___ N/A___

    Comment:

    _____

22. Level of owner/operator service access to device operating system: Can the device owner/operator:

    a. Apply device manufacturer-validated security patches? Yes___ No___ N/A___
    b. Install or update antivirus software? Yes___ No___ N/A___
    c. Update virus definitions on manufacturer-installed antivirus software? Yes___ No___ N/A___
    d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)? Yes___ No___ N/A___

    Comment:

    _____

23. Does the software support user/operator specific ID and password?

    Answer:_____

    _____

24. Are access sessions terminated after a predetermined length of inactivity (e.g. auto logoff)?

    Answer:_____

    _____

25. Events recorded in software audit log (e.g. user, date/time, action taken): Can the audit log record:

    a. Log in and logout by users/operators? Yes___ No___ N/A___
    b. Creation, modification, or deletion of data? Yes___ No___ N/A___

    Comment:

    _____

26. Does the device incorporate an emergency access (“break-glass”) feature that logs each instance of use?
    Answer:_____
    _____

RECOMMENDED SECURITY PRACTICES

Please enter any comments applicable to recommended security practices here.

EXPLANATORY NOTES

Please enter any comments, notes, or details for any of the above questions. Use/attach another page if needed.