**Performance Work Statement (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**
**VETERANS HEALTH ADMINISTRATION**

# Endoscopy Information Systems (EIS)
# EndoSoft® Brand Name or Equal

**FORCE Requirement #: - VA-18-00024348**
**September 9, 2019**

## Prepared By:


**Department of Veterans Affairs**
**Office of Procurement and Logistics (10NA2)**

**and**

**Office of Acquisition Operations (OAO)**
**Strategic Acquisition Center (SAC)**
**10300 Spotsylvania Avenue, Suite 400**
**Fredericksburg, VA 22408**

**Concur:**

_____

Charles Herring
Project Manager
Clinical Program Team
Procurement & Logistics Office (10NA2)

_____

Jeff Young
Deputy Program Manager
Clinical Program Team
Procurement & Logistics Office (10NA2)

**Approved:**

_____

Tim Johnson
Supervisory Contracting Officer
Strategic Acquisition Center
Department of Veterans Affair

**Performance Work Statement for**
**Veterans Health Administration (VHA)**

**Non-Expendable Equipment (NX EQ)**

**Endoscopy Information System (EIS)**

**VA-18-00024348**

## 1. BACKGROUND

The Veterans Health Administration (VHA) Equipment Life Cycle Management (ELCM) Program has identified Information System: Data Management: Endoscopy here after referred to as Endoscopy Information Systems (EIS) as a candidate for VA-wide (otherwise referred to as “national”) contract award. EIS are designed to manage GI and Pulmonary endoscopy clinical (documentation and embedded images) and administrative data (e.g., finances, reimbursement, materials management) within in a healthcare facility. EIS consist of hardware, including servers for image acquisition and storage, computer workstations for data entry and viewing and peripheral devices (e.g., printers) that are connected to the VA network behind a medical device virtual local area network (VLAN), as well as software, including an EIS electronic medical record (EMR) application, operating systems, a database management system, interfaces and other application programs. EIS are dedicated systems intended to collect, store, analyze, retrieve, display, and print information related to GI and Pulmonary endoscopy procedures. EIS exchange information with endoscopic video systems usually following DICOM (Digital Imaging and Communications in Medicine), a standard in the field of medical informatics that ensures interoperability. EIS allows digital image transmission to any networked part of the hospital, direct access to stored images, simultaneous access to images for several different physicians (e.g., surgeons and emergency room personnel), and centralized consultation for comparisons.

## 2. APPLICABLE DOCUMENTS

The following documents are required in the performance of the tasks associated with this Performance Work Statement (PWS):

a. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”.
b. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”.
c. FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006.
d. 10 U.S.C. § 2224, "Defense Information Assurance Program".
e. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes.

f. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”.
g. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”.
h. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” June 4, 2010.
i. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008.
j. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards”.
k. OMB Circular A-130, “Management of Federal Information Resources”.
l. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”.
m. NIST SP 800 Rev 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008.
n. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998.
o. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004.
p. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012.
q. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012.
r. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010.
s. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012.
t. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
u. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010.
v. VA Handbook 6500.6, “Contract Security,” March 12, 2010.
w. VA Technical Reference Model (TRM) (reference at https://www.voa.va.gov/).
x. National Institute Standards and Technology (NIST) Special Publications.
y. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008.
z. VA Directive 6300, Records and Information Management, February 26, 2009.
aa. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010.
bb. OMB Memorandum, “Transition to IPv6”, September 28, 2010.
cc. VA Directive 6550, Pre-Procurement Assessment for Medical Device/Systems, February 20, 2015

The listing of reference materials in this section is not intended to require the Contractor to perform any other specific tasks or services that are not expressly described in and required to be performed by other sections in this PWS.

## 3. SCOPE OF WORK

The Contractor shall deliver to the Government a commercially available, off the shelf software (COTS), enterprise-wide (in accordance with specific tasks orders under this

contract) endoscopy information system (EIS) comprised of software and related hardware (System) that meets or exceeds the following salient characteristics:

SC1. Must support Gastroenterology (GI) and Pulmonary endoscopy specialties workflow including procedure documentation, information, data and endoscopy procedure reports.

SC2. Must provide image capture and management of images from various GI and pulmonary endoscopes and capsule camera vendors (vendor neutral, independent, agnostic).

SC3.Must provide reports.

SC4. Must provide interfaces including, at a minimum HL7, ADT, pathology requisitions, Electronic Medical Record (EMR)/Electronic Health Record (EHR) (Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS), VistA Imaging, and Cerner).

SC5. Must be customizable.

SC6. Must include data migration.

SC7. Must support coding (e.g., International Classification of Diseases (ICD), Current Procedural Terminology (CPT), etc.

The Contractor shall provide all personnel, software, hardware, software upgrades, maintenance and support, transportation, tools, material and supervision necessary to deliver the products and perform the services for the EIS in both the Test and Production environments within the Department of Veterans Affairs (VA) Medical Centers in accordance with each specific task order placed under this contract.

The upgrades, maintenance, and support shall include all scheduled preventive maintenance, technical support, unscheduled repairs/corrective maintenance, database administration support, and training services described in this PWS. The Contractor shall provide necessary support services so that the EIS operates in an efficient manner.

The EIS shall utilize the existing Government owned and operated network(s).

The Contractor shall identify minimum specifications for VA networks that allows software to operate.

The Contractor shall complete and update VA Form 6550 Pre-Procurement Assessment of Networked Medical Systems.

## 4. PERFORMANCE DETAILS

### 4.1 PERFORMANCE PERIOD

The period of performance (POP) shall be one (1) twelve (12) month base period, with four (4) consecutive option periods of (12) months each. Any VA Medical Center that adopts this contract after the beginning of the base year or any option shall only be entitled to the benefit of the period remaining in the base year or option period, as applicable.

### 4.2 HOURS OF OPERATION

The Contractor shall provide support 24 hours per day, seven days per week, 365 days per year. However, normal hours of work are defined as Monday through Friday from 7:00 a.m. to 6:00 p.m. Central Standard Time, excluding Federal holidays or as otherwise arranged with the Contracting Officer's Representative (COR).
The Contractor must always maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS.

#### 4.2.1 RECOGNIZED HOLIDAYS

New Year's Day
Martin Luther King Jr.'s Birthday
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

### 4.3 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at VHA facilities throughout the United States, U.S. Territories, Guam, and the Philippines. Delivery requirements and specific locations shall be specified under each individual order. Tasks under this PWS shall be performed at VA Medical Centers or may be performed remotely at Contractor facilities. Work may be performed at remote locations other than Contractor facilities with prior approval of the COR.

### 4.4 TRAVEL

The Government anticipates Contractor travel under this contract in accordance with each task order. The Contractor is responsible for travel for on-site installation, implementation, training, go-live support and maintenance. All travel shall be incorporated into the overall firm fixed price for the contract. No travel costs will be reimbursed by VA. The Government acknowledges the possible use of remote access

for installation and implementation purposes, within the constraints of all applicable VA Information Security Requirements.

### 4.5 OPTION TO EXTEND SERVICES

In accordance with FAR Clause 52.217-8, Option to Extend Services, the contract may be extended, at the Government's sole discretion, for a period of up to four (4) years, exercisable in increments of twelve (12) months. If the contract contains an unexercised option period, the Government may elect to exercise the option pursuant to FAR Clause 52.217-9, Option to Extend the Term of the Contract.

## 5. REQUIREMENTS

The Contractor shall perform the following:

### 5.1 PROJECT MANAGEMENT

The Contractor shall provide a Project Manager (PM) who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the Contractor when the PM is absent shall be designated in writing to the Contracting Officer (CO). The PM or alternate shall have full authority to act for the Contractor on all contract matters relating to daily operation of this contract. The PM shall be responsible for the project management of the EIS task orders. Specifically, the PM shall work with the Contractor team to coordinate, schedule and oversee the services provided to accomplish the technical, administrative, managerial aspects of this effort. The PM shall be responsible for required status reports, documentation and updates that need to be provided to the VA Medical Center Point of Contact (POC) and Contracting Officer's Representative (COR). The PM shall review and approve project documents. The PM shall coordinate project changes with the VA Medical Center POC, COR and CO.

#### 5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall prepare and deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, tools and quality controls to be used in execution of the PWS. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The schedule must identify detailed tasks and subtasks, including task duration, milestone dates, task dependencies, resource requirements and planned dates for initial deliverables. The CPMP shall clearly state how the Contractor will coordinate and execute the deliverables for each task order. The initial baseline project plan shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the approved project plan throughout the period of performance.

#### 5.1.2 MEETINGS

The Contractor shall conduct a kick-off meeting with the COR and other Government representatives within ten (10) calendar days after award of the national contract. The meeting will be conducted by conference call and coordinated by the COR after award and separately after each task order is placed. The Contractor shall present its project plan, schedule, staffing plan, contact information and identification of key risk points and mitigation plans. Working collaboratively with the Government, the Contractor shall finalize all planning and submit final plans to the COR following the meeting.

The Contractor shall attend recurring meetings or conference calls scheduled by the COR to address areas of concern and exchange information to ensure consistent high levels of professional services. The Contractor shall be responsible for all costs associated with attending meetings and/or conference calls.

### 5.1.3 PROJECT ACTIVITY REPORTS

The Contractor shall provide monthly project activity reports and other information as required by the VA Medical Center POC or COR. The Contractor shall utilize project metrics to track, manage, and analyze task progress and communicate findings to the COR to ensure appropriate focus on critical attention areas.

## 5.2 INSTALLATION, CONFIGURATION, CUSTOMIZATION AND IMPLEMENTATION

The Contractor shall provide all services and supplies required to install, configure, customize and implement the EIS at each location defined in each task order, including all local network configuration and programming required to achieve integration of the EIS across the VA Medical Center, Veteran Integrated Service Network (VISN) and VHA, in accordance with the specific task order. Installation and implementation shall not be considered complete until the Government has verified that the EIS is fully functional and available for use without further configuration and/or programming, by trained VA staff, at locations defined in each task order.

The Contractor shall provide a form/report to the COR on all EIS products being shipped to VA Medical Centers under this contract. Prior to delivery and installation, the contractor is required to contact the facility points of contact (POC) to schedule the installation during a time that will result in the least amount of disruption of services. The Contractor shall track all orders which provides line item information including part #, serial #, model #, tracking # and who signed for the order at each VA Medical Center. Upon delivery of all components, the contractor will supply a detailed packing list with model numbers and serial numbers so that the components can be entered into the local inventory by the VA facility warehouse without unboxing the shipment. The Contractor shall obtain packing slips and proof of deliveries for each VA Medical Center and provide them to the COR as requested. The Contractor will verify receipt of all necessary components. The Contractor shall assist EIS VA Medical Centers in receipt of new equipment to initiate a request for local Biomedical Engineering to have the new equipment inspected in accordance with VA Medical Centers policy and procedures. The Contractor will unpack and rack network servers in VA supplied racks in a data

center and verify operation of the servers. The contractor will unpack and setup workstations and verify hardware operation. The contractor will install software on the servers and configure HL7, CPRS and Cerner connectivity with VA's biomedical engineering and Information Technology departments. The Contactor will be required to supply all tools and instruments needed to complete the installation. No VA tools or instruments will be provided.

### 5.3 LEGACY DATA MIGRATION SERVICES

The Contractor will migrate four years of prior exams from each of the legacy systems to the proposed EIS at each corresponding VA Medical Centers in accordance with the specific task order within a 6-month period from the start of clinical usage (Go-Live date). A minimum of the most recent two years of exams must be migrated prior to go-live. Aging and "archive and remember "rules should also apply to migrated studies from the legacy EIS. The Contractor will validate migrated studies to confirm archival, then flag the respective studies as being archived, and remember where they are archived for automatic retrieval. Migration work times are not restricted and shall be accomplished without affecting clinical operations. The use of onsite contract personnel for migration must be coordinated with VA Medical Center POC to ensure personnel availability. The Contractor shall agree to provide final migration reports to the VA Medical Center and COR upon completion of each migration that clearly demonstrates validation of successful migration and details how many exams existed for the migration period in each legacy system, which images were migrated, and which images were not migrated, including technical explanations why they could not be migrated. The report should also disclose a list of all exams that could not be validated as being archived.

### 5.4 TRAINING AND GO-LIVE SUPPORT

#### 5.4.1 ON-SITE CLINICAL USER TRAINING

The Contractor shall provide on-site user training to end-users of the EIS that covers how to use the software safely and effectively. The Contractor shall offer onsite new user training that provides Endoscopists, Nurses, other clinical users and administrative personnel the knowledge to fully utilize the system. The Contractor must agree that training documentation will be provided back to the COR at time of acceptance testing detailing training date, trained topics, and users trained.

#### 5.4.2 ON-SITE SYSTEM ADMINISTRATOR TRAINING

The Contractor shall provide on-site system administrator training to system administrators of the EIS that covers how to manage the EIS. The Contractor shall offer System Administrator training for at least two VA System Administrators for each installed system in accordance with the specific task order. System administrator training must cover all application tools and functions, all unique Operating System commands and functions, and all third-party applications for the EIS and troubleshooting techniques specific to the EIS.  All training materials shall be provided

on CD or DVD to the VA Medical Center for future use and inclusion in local training initiatives. All training courses will be addressed in the context of the course learning objectives and an outline will be provided detailing expectations and course structure.

### 5.4.3 ON-SITE BIOMEDICAL/TECHNICAL TRAINING SERVICES

The Contractor shall provide technical training to hospital staff responsible for servicing/maintaining the EIS. Training shall include maintenance, software administrative, software options for continued updates of the medical servers and software and troubleshooting techniques.

### 5.4.4 ON-SITE GO LIVE SUPPORT

The Contractor shall provide on-site go-live support that includes a planning checklist to aid VA staff in planning for EIS implementation, the go-live event and to identify any issues that need to be addressed beforehand. The Contractor shall use this checklist to validate that everything on the list has been performed. The Contractor shall coordinate a rehearsal of the go-live day using a test environment to perform each of the application's functions. The Contractor shall plan and coordinate the go-live date with the VA Medical Center POC, review evidence of readiness from training, testing of the network, hardware, software and interfaces. The Contractor shall review achievement of goals with VA staff and reaffirm readiness for go-live. One day prior to go-live the Contractor shall speak with key clinical and technical personnel to verify readiness including user access, network speed, interfaces, printers and review the escalation procedures to follow in the event of a problem. The Contractor shall provide clinical on-site go-live support staff to accompany initial users in the field for the first three days of use at each VA Medical center in accordance with the specific task order. The Contractor shall attend a mid-day "huddle" to evaluate progress and to address any concerns and an end-of-shift debriefing for VA staff to identify and address any issues. The Contractor shall ensure support staff will be available to make critical system changes during the go-live event.

## 5.5 ON-GOING MAINTENANCE AND SUPPORT

The Contractor shall maintain and support all hardware and software associated with the specific task order including all software updates, software version changes, patches, enhancements, corrections and new releases for the EIS within the VA Medical Center. The service under this task includes all labor, tools, test equipment, diagnostic software, supplies, parts, shipping, and Contractor staff supervision necessary to perform remote and/or on-site services. The Contractor shall provide express delivery of replacement parts when needed to maintain full performance of the system. There shall be no additional cost to the Government for shipping replacement parts.

The Contractor shall provide remote system support including remote diagnostics via VPN/remote access (note: The Contractor shall utilize the VA national Site-to-

Site VPN, or the Contractor shall work with the Office of Cyber and Information Security and VA Medical Centers in accordance with each task order that their Information Security Officer [ISO] to establish a client-based VPN).

The updates, maintenance, and support shall include all proactive monitoring, remote and on site scheduled preventive maintenance, unscheduled repairs/corrective maintenance, technical support and database administration support. The Contractor shall provide necessary support services so that the EIS operates in accordance with the manufacturer's specifications. The Contractor shall coordinate maintenance and support with the COR and VA Medical Center Points of Contact (POCs) as designated on each order.

The Contractor shall be required to coordinate with VA Medical Centers to provide maintenance options for all hardware and software beyond the standard first year warranty for all EIS equipment. The Contractor shall monitor OEM maintenance and coordinate with OEM's to insure maintenance work is performed as required. The Contractor shall track all maintenance plans to insure they are kept current on an annual basis. The Contractor shall track all Return to Manufacturer Action's (RMA's) to insure they arrive at the manufacturers' and replacement parts are delivered to the VA. Software upgrades need to be approved by the COR who will coordinate with VA Medical Centers.

### 5.5.1 TELEPHONE, ON-LINE SUPPORT AND TECHNICAL CONSULTATION

The Contractor shall provide VA with toll free corporate office telephone numbers, mobile telephone numbers and email addresses for the Contractor's key staff for both normal hours and after hours. The Contractor shall provide telephone and online remote support 24 hours per day, 7 days per week, and 365 days per year for both maintenance and technical support.

### 5.5.2 SCHEDULED MAINTENANCE

The Contractor shall perform any required scheduled (preventive) maintenance in accordance with manufacturer's recommendations of all EIS identified in each task order. The Contractor shall initiate corrective maintenance whenever equipment defects are discovered because of the Contractor performing scheduled/preventive maintenance services or its proactive monitoring of the systems.
The Contractor shall provide scheduled maintenance and software updates during normal working hours or at a mutually agreed upon time by the COR and VA Medical Center POC on each order and the Contractor.

### 5.5.3 SOFTWARE, SOFTWARE LICENSES, SOFTWARE MAINTENANCE AND SUPPORT

The Contractor is required to provide software, software license, software maintenance services and technical support for the EIS. Distribution of maintenance copies shall be accomplished by using an appropriate magnetic, electronic or printed media. As further

defined below, software maintenance includes enhancements, periodic updates, corrections to the software, and technical support. The EIS software and commercial operating system licenses provided to the Government must be perpetual, nonexclusive license to use the software. The software shall be used in a networked environment. Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d). All limitations of software usage are expressly stated in the SF 1449 and the Performance Work Statement.

Medical device encryption modules shall have FIPS 140-2 certification in accordance with VA security requirements for medical devices/systems connected to VA information networks. The Contractor shall provide the certificate number.

The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents of the EIS, throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, updates, upgrades, and any physical components 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 Contractor shall ensure that security fixes does not negatively impact the systems.

Updates to the operating system or system application that remedy bugs or defects in system function should be provided free of charge for the life of the product. If the updates are embedded with system upgrades that add additional functionality and the vendor is unable to provide the update as a distinct deliverable separate from the upgrade, the VA will not be liable for the cost.

### 5.5.3.1 SYSTEM ENHANCEMENT SERVICES

The Contractor shall perform software enhancement services as part of scheduled maintenance. Updates and new versions generally refer to software releases or update containing patches, bug fixes and modifications, enhancements or improvements to existing applications
and such items are included in the scheduled maintenance services without additional charge. The Contractor will maintain a formal process for receiving, recording and assessing software feature requests from VA and for deciding what features to include in its future commercial software development program and new releases. Any request by the VA for enhancement will be approved on a uniform basis by the VA EIS Group before submission to the Contractor. Upon approval, the Contractor shall coordinate

and distribute enhancement and maintenance updates and releases by using an appropriate electronic media, printed media or its website in accordance with VA requirements for electronic, printed or web based media. The Contractor shall continue monitoring the system after any changes to ensure that the system continues to function in accordance with manufacturer's specifications.

Contractor shall maintain and provide an initial and updated list of any/all known compatibility issues to include issues with antivirus software.

### 5.5.3.2 SOFTWARE UPDATES

The Contractor shall provide ongoing operating system and database updates throughout the life of the contract at no additional charge. Software updates can be 1) initiated by the Contractor to improve functionality of the EIS, 2) in response to changes in VA/VISN enterprise needs, 3) to maintain the EIS as compliant with VA data standards, and/or regulatory requirements, 4) to maintain compatibility with other systems, 5) to maintain VA standards regarding security updates and patching. It is estimated that updates will occur no more frequently than quarterly per year. Regardless of the reason for the update, the Contractor shall plan and schedule updates through coordination with the VA Medical Center POC and COR as designated on each task order. The Contractor shall provide an initial planned release schedule including major as well as enhancement releases, and provide updates to the planned release schedule immediately when any change is made to the schedule (same day). The Contractor shall provide complete descriptions of all system updates and upgrades including dates within the calendar year prior to initial system installation. Updates or corrections related to patient safety, regulatory requirements or interface to VistA will be classified as a patient safety issue with urgent priority. The Contractor shall provide an action plan within 30 days and shall implement an update (fix) within 180 days from the time of notification. All software and supporting release notes, user and technical literature shall be updated and provided to the VA Medical Center POC and COR as software updates are implemented.

Software, including commercial Operating Systems, must not be self-canceling, which is interpreted to mean the function of the software will not be stopped due to elapsing time or other conditions not identified with original equipment purchase. If the licensed software or hardware requires a password (or license key) to be operational, it shall be delivered with the software media and hardware and have no expiration date. The Government requires delivery of computer software and hardware that does not contain any code that will, upon the occurrence or the nonoccurrence of any event, disable the software. Such code includes but is not limited to a computer virus, restrictive key, node lock, time-out or other function, whether implemented by electronic, mechanical, or other means, which limits or hinders the use or access to any computer software based on residency on a specific hardware configuration, frequency of duration of use, or other limiting criteria. If any such code is present, the Contractor agrees to indemnify the Government for all damages suffered because of a disabling caused by such code, and the Contractor agrees to remove such code upon the Government's request at no

extra cost to the Government. Inability of the Contractor to remove the disabling software code will be considered an inexcusable delay and a material breach of contract, and the Government may exercise its right to terminate for cause. In addition, the Government is permitted to remove the code as it deems appropriate and charge the Contractor for consideration for the time and effort in removing the code.

The Contractor is responsible to ensure any third-party provided software is included in this restriction.

The Contractor shall report and distribute software updates or releases by using an appropriate electronic or printed media to the VA Medical Center POC and COR. Alternatively, the Contractor may offer access to maintenance copies through its company website.

The Contractor shall provide all software updates and new versions including any replacement version or name revisions of the existing perpetual unlimited, non-exclusive software licenses. All new software versions shall be covered in this effort including all subsequent versions designed to replace a version installed under any resultant task orders issued against this national contract. As part of scheduled and/or unscheduled maintenance the Contractor shall furnish, install and maintain all software version changes and/or updates to the system. The Contractor shall monitor and maintain the system with the most current software releases including maintaining up-to-date current security patches at no additional charge to the Government. The Contractor shall complete installations of new updates within 180 days of the date the new release is made available.

The Contractor shall provide a complete description of the licensing models(s) employed at the time of original system installation and not change the licensing model without written approval form the CO.

The Contractor shall complete a VA Form 6550 Pre-Procurement Assessment of Networked Medical Systems initially and must update the 6550 anytime a software update will change any factor associated with the current 6550.

### 5.5.3.3 SOFTWARE UPDATES TRAINING

The Contractor shall provide release notes, manual updates and clinical and technical informational training sessions associated with updates that affect the use of the system, at no additional cost. In addition to such documentation, the Contractor shall make available qualified personnel remotely for consulting with the VA EIS users about a new release containing changes to the software usability.

## 5.6 UNSCHEDULED MAINTENANCE

The Contractor shall provide an unlimited number of unscheduled maintenance and technical support incidents during the performance period. Support includes both remote and, when a problem cannot be resolved remotely, on-site support. The Contractor shall perform all unscheduled corrective maintenance during the

performance period of each order. The Contractor shall troubleshoot, repair and/or resolve, on request by the VA Medical Center POC or COR, all EIS equipment and software identified in each task order. All software repaired by the Contractor shall be restored to manufacturer's specifications. For technical problems, functional incidents or for questions during business hours, the Contractor shall provide the following communication options: call the Contractor Help Desk, create a field service request online or email the incident or question. For each request, the Contractor shall communicate the following via email or telephone to VA Medical Center POC or make available on line, in response to each event communicated by VA to the Contractor:

a. Incident reference number
b. Brief Description of the problem
c. What version or software is being affected
d. What equipment or component is being affected
e. If this issue affects patient safety
f. Workaround (if any) and expected release date of patch, upgrade or update.
g. Status and estimated completion date/time

The Contractor shall notify the VA Medical Center POC and COR within two (2) business hours when any system failures occur that impair the ability of the Contractor to provide full functionality of the EIS. The Contractor shall communicate known material software and hardware issues to the COR weekly via email or by telephone. The Contractor shall respond to a request for unscheduled corrective maintenance for a software or hardware issues, malfunctions or failures, by a fully qualified representative, in accordance with response time requirements defined in Table 1 of Section 5.13.

**5.7 INTERFACE SUPPORT**

As part of the scheduled and unscheduled maintenance, the Contractor shall ensure that all EIS side interfaces, including but not limited to VistA Imaging/CPRS, Cerner, Medical Devices, analytics, etc., and data transfer links are operational and maintained consistently throughout the period of performance in accordance with the processes established as part of the implementation. The Contractor shall coordinate with other Vendors and/or Contractors when necessary to accomplish this task. The Contractor is not responsible to make any payments to any device vendor and is not obligated to incur any licensing or other obligations or liabilities to a device vendor aside from customary mutual confidentiality commitments. In addition, the Contractor obligation to maintain or develop interfaces assumes and is conditioned on the device manufacturer's compliance with an industry recognized technical means of providing device interface capability to ensure the reliability and accuracy of the available data. Any devices requiring non-standard means of interfacing will need to be evaluated for technical feasibility and separate cost on a case-by-case basis and are not included in the initial scope of this contract.

### 5.7.1 VISTA/CPRS, VISTA IMAGING, CERNERINTERFACE SUPPORT

The integration of EIS with VistA, CPRS and Cerner shall be maintained by the Contractor to ensure that the EIS side of the interface provides for transfer of clinical and administrative data and images between the EIS and the VistA and Cerner systems at each VA Medical Center under the specific task order. The Contractor must perform ongoing testing as updates are released to verify that the EIS retains full interface functionality.

### 5.7.2 ANALYTICS INTERFACE SUPPORT

The Contractor shall maintain data integrations with EIS analytics database(s). The Contractor shall ensure that data is inclusive of all administrative and clinical data contained within the EIS. The Contractor shall ensure that the EIS provide the data extracts to the analytics database(s) in the proper format. The Contractor shall coordinate with analytics Contractor(s), VA data warehouse staff, VA Medical Center POC and the COR to validate the data being transmitted by the EIS.

## 5.8 THIRD PARTY SOFTWARE SUPPORT

The Contractor shall provide an initial list of all third-party software components included in the EIS and update this list whenever any third-party components are added, deleted or modified. The Contractor will work with third-party vendors that VISNs or VA Medical Centers contract with to interface any 3D software with the 3rd party software at no additional charge. (For example: current Picture Archive and Communication Systems (PACS) that are on contract with a VISN or VA Medical Center).

## 5.9 SYSTEM TESTING

The Contractor will perform quality assurance testing before and after installing a software updates including connectivity tests with medical devices, VA networks, servers, work stations, VistA/CPRS, data marts and data extractions for VA and/or commercial analytics systems. Contractor shall certify that all system component updates, upgrades, bug fixes and other recommended system modifications are rigorously tested and proven to be stable prior to installation and implementation. The Contractor shall not install and/or implement any custom, alpha or beta developmental software versions, modules, plug-ins, etc. beyond the version(s) specified within the original proposal without written CO approval prior to installation of the same. Upon completion of any EIS repairs, updates, upgrades and installations, the Contractor shall test the system to ensure it is fully functional in accordance with the manufacturer specifications. Testing shall be coordinated and scheduled with the VA Medical Center POC and COR as mutually agreed and designated on each task order. The Contractor shall coordinate with other Vendors and/or Contractors when necessary to accomplish this task.

## 5.10 TOPOGRAPHICAL DIAGRAM AND THEORY OF OPERATION

The Contractor shall provide a graphic depiction of the initial planned system network and dataflow design, the final installed system design and update the graphic whenever the design changes through the life of the contract in accordance with each task order. The Contractor shall provide a writte Theory of Operation that addresses the following:

i. Image acquisition and storage from Pulmonary and GI endoscopes and capsules.

ii. Communication with VistA and Cerner.

iii. Storing data and images

v. Archiving data and images

vi. Ad hoc disaster recover de-archiving of data and images

vii. In-mass disaster recovery de-archiving of data and images

viii. Ability for one facility to read for another facility

viiii. Ability to run reports at a facility, at a VISN, at a Region and at the National Program Office

## 5.11 REPORT TEMPLATE SHARING

All EIS report templates produced using data aggregation, analytics, stored procedures, extractions, reporting services, business intelligence tools, or any other method, for information gathering and expressing (in any format) including but not limited to statistical analysis, compliance measures, performance measures, audits, quality improvement, usage trends, etc., that are made available by the Contractor for any VA Medical Center or a VISN, must be made available to all other VA Medical Centers and VISNs having a task order under the national contract at no additional cost to VA.

## 5.12 MANDATORY CHECK IN/OUT AND REMOVABLE MEDIA SCANNING

For any services performed on-site the Contractor shall, upon arrival at the VA Medical Center, report to the VA Medical Center POC to check in before proceeding to the any department and before performing any services. Prior to leaving the medical center, the Contractor shall check out with the POC. This check in and check out is mandatory. Upon checking in with the VA Medical Center POC and before performing any services, the Contractor shall ensure that any removable media is scanned by the Biomedical Engineering Section prior to connecting to any VA network, device or system. The Contractor shall provide any removable media to Biomedical Engineering staff. Biomedical Engineering staff will perform a malware/virus scan of the Contractor's removable media. If "nothing found" is displayed, the Contractor may proceed and use the removable media. If "nothing found" is not displayed and/or the number of detections is greater than zero, the removable media shall be presumed infected with malware and shall not be allowed to be used. The media shall be returned to the

Contractor for virus removal. The Government will not perform any virus or malware removal on the Contractor's removable media. Biomedical Engineering will report any detection to the VA ISO. Failure by the Contractor to check in, check out, provide removable media for scanning, or use of any infected media is a breach of security and shall be acted upon in accordance with the terms and conditions of this agreement and any subsequent orders. (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 preapproved and described in the purchase order or contract.

All medical device hard drives or other media containing VA sensitive data must follow VA's currently published media sanitization policy - VA Handbook 6500.1 Electronic Media Sanitization.

**5.13 RESPONSE TIME**

The Contractor shall provide the maintenance and technical support within a specified time published in the response time requirements below in Table 1. Table 1 list response times by priority types as defined by VA. The Contractor shall meet the response time requirements associated with each priority. If the problem cannot be resolved over the phone or remotely, then an authorized representative of the company will commence work within the designated time identified, and will proceed progressively and diligently to rectify the problem without undue delay and without any additional cost to the government. The Contractor shall be responsible to coordinate the method of response with the VA Medical Center POC and COR as designated on each task order. The following priorities will be determined for each issue by the VA Medical Center POC and COR.

**Urgent priority** is defined as any issue that affects patient safety, regulatory compliance, and/or EIS side interfaces which affect life and/or property. Urgent priority applies when malfunction or failure can result in patient injury or death or significant damage to equipment. This includes any issue that adversely impacts patient care. Examples include partial or complete system outages, interruptions making a critical functionality inaccessible, interruptions causing a severe impact on application availability, or data corruption resulting in missing or incorrect patient information, duplicate records, loss of data, etc. Urgent priority requires immediate action by the Contractor.

**High priority** is defined as having a potential to affect patient care such as degradation in performance or functionality, work flow interruptions or delays, etc. High priority warrants special attention and takes precedence over normal and low priorities. Examples include interruption to critical functionality, access denied to data and systems, sustained degraded or unusable capabilities, not life threatening but having a potential for impact on services availability if not resolved. High priority also requires

immediate action by the Contractor to minimize risk of becoming an urgent priority event.

**Normal priority** is defined as a defect or fault event but the system is operable with no impact to patient care. Normal priority requires same day initial action but resolution may take more time. Examples include impairment of non-critical functions or procedures, capabilities that have become unusable or hard to use but with no direct impact on patient care services or system availability. Normal priorities will typically have a workaround available. Normal priorities take precedence over low priorities.

**Low priority** is defined as preventive maintenance or issues that do not require immediate action or attention.

**Table 1 – Response Time**

| Priority | Call Back Response Time | Remote Log-In Response Time | Restore to Full Performance |
|---|---|---|---|
| **Urgent** | **1 hour** | **1 hour** | **4 hours** |
| **High** | **2 hours** | **2 hours** | **8 hours** |
| **Normal** | **2 hours** | **8 hours** | **16 hours** |
| **Low** | **2 hours** | **10 hours** | **40 hours** |

If full performance cannot be restored within the above anticipated timelines, an on-site response may be required as agreed upon by VA and the Contractor. A failure to meet the anticipated timelines will not be a default so long as the Contractor uses the requisite level of effort required for the applicable problem priority. Full performance means that all defective software, hardware, and / or parts have been repaired or replaced with equivalent to or better than the original manufacturer's parts that replacement meets original performance specifications. Except in the case of Urgent priority problems, such Response Times shall apply only during normal business hours (i.e. Monday through Friday from 7:00 a.m. to 6:00 p.m. Central Standard Time, excluding Federal holidays) and in the case of service requests received outside of the normal hours, the start times shall be measured from the beginning of normal business hours for next business day. In the case of Urgent or High priority problems, the Contractor will use its commercially reasonable best efforts and proceed diligently and on a substantially continuous basis to resolve the problem so that the system is restored to an operational condition and available for its intended use as soon as technically feasible. In the case of normal or low priority problems, the Contractor will proceed during normal business hours in a reasonable manner to resolve the problem within a reasonable time. The Contractor may reduce the severity level of a problem by implementing reasonable work-arounds to mitigate or eliminate the problem subject to the COR's reasonable approval of such work-around.

## 5.15 REPORTS/DOCUMENTATION

### 5.15.1 SERVICE REPORTS

The Contractor shall provide a Service Report to the pertinent VA Medical Center Point of Contact (POC) designated by the COR at the completion of an on-site service call prior to departing the VA Medical Center or after the conclusion of remote service. In case of remote service, the Service Report may be made available via an Electronic Service Log for tracking of services. The Service Report shall document the services rendered and, when applicable, shall include equipment description, model, equipment entry (barcode) number, serial number, date and time of service, description of services, the latest version of software patch or upgrade, results of services, name of individual who performed the services, and travel, labor and parts information.

### 5.15.2 MANUALS, RELEASE NOTES, AND SERVICE BULLETINS

The Contractor shall provide an electronic copy of the user manuals, system administrator manuals, operating/maintenance and/or technical manuals, release notes, service bulletins, etc. necessary for the operation and support of the software and hardware to the COR and each VA Medical Center as designated on each order.

### 5.16 DISASTER RECOVERY AND FAILOVER PLAN

The Contractor shall provide a disaster recovery plan in the event of the occurrence of general hardware or software failure, a major system outage resulting from such disasters or other causes not covered by the Contractor's basic support responsibilities. Such plan shall provide detailed information concerning the process, resources, implementation schedule and costs for restoration of the system to full capability as soon possible. Approval of the plan for implementation shall be made by modification signed by the COR under the applicable order. This critical fail-over solution consists of both hardware and software. This feature permits another EIS system server(s) to be installed at a physically separate location from the other main production servers (This can be a secondary data center, a VA Medical Center, or another location available via the Wide Area Network (WAN) from the main server location. This "Disaster Operational Continuity" server is updated by the main production servers on a per-transaction basis. Should a catastrophic failure occur involving an entire EIS at a site or data center (fire, flood, or other unplanned major outage) this fully redundant Disaster Operational Continuity server continues full operations of all EIS activities with all the patient data intact. The server is immediately available for use by any clinical users via remote access via the WAN. Once the main production server at the sites or data centers comes back on line, the Disaster Operational Continuity server can be used to restore the data to the affected production systems. The Disaster Operational Continuity server, like the site servers, is intended to run without any operator intervention.

### 5.17 PRODUCT MODIFICATION, REMOVAL, OR RECALL

If any product supported under this agreement and subsequent orders requires modification, is removed or recalled by the Contractor or manufacturer, or if any

required modification, removal or recall is suggested or mandated by a regulatory or official agency, the Contractor shall notify the COR within forty-eight (48) hours via email notification that includes the following information:

a. Complete item description and identification

b. Reasons for modifications, removal or recall

c. Necessary steps for return for credit, replacement or corrective action. The Contractor shall provide the above information to all VA Facilities that purchased the product. The COR shall be provided a copy of the notification and a list of all VA facilities notified. The Contractor shall perform all steps required for return for credit, replacement or corrective action for all affected Facilities.

**5.18 METHOD AND DISTRIBUTION OF DELIVERABLES**

The Contractor shall deliver documentation in electronic format, unless otherwise mutually agreed on each order. Acceptable electronic media include: Microsoft (MS) Word 2016 or current version, MS Excel 2016 or current version, MS PowerPoint 2016 or current version, MS Project 2010 or current version, MS Visio 2010 or current version, and Adobe Postscript Data Format (PDF) current version.

**5.19 VA/RESOURCE PROVISIONS**

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR, as designated on each order, as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

**5.21 SPECIAL SHIPPING INSTRUCTIONS**

Prior to shipping any parts or supplies, the Contractor shall notify VA Medical Center POCs, by phone and by email, of all incoming deliveries including line-by-line details for review of requirements. The Contractor shall make any changes to the delivery schedule at the request of Site POC. Contractors shall coordinate deliveries with Site POCs before shipment of hardware or other material to ensure sites have adequate storage space. All shipments, either single or multiple container deliveries, will bear the VA Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA PO number shall indicate total number of containers for the complete shipment (i.e. “Package 1 of 2”), clearly readable on manifests and external shipping labels. Packing Slips/Labels and Lists shall also include the following:

PO #: _____

Total number of Containers: Package ___ of ___. (i.e., Package 1 of 3)

## 5.22 DATA RIGHTS

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

## 5.23 QUALITY CONTROL

The Contractor shall develop, implement and maintain an effective Quality Control Program (QCP). The QCP is how the Contractor assures that the work complies with the requirement of the task order. The QCP shall be delivered within 30 days after the contract is awarded. The QCP procedures ensure services are performed in accordance with this PWS and results in correction of potential and actual problems without dependence upon Government direction. The Contractor shall implement the QCP procedures to identify, prevent, correct and ensure non-recurrence of defective services. The Contractor shall maintain records of all Contractor quality control inspections and corrective actions throughout the scope of the contract performance.

### 5.23.1 QUALITY ASSURANCE

The Government shall evaluate the Contractor's performance under each task order under the contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

## 6. PERFORMANCE REQUIREMENTS SUMMARY

The Contractor service requirements are summarized into performance objectives that relate directly to project essential items. The performance requirements summary briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to project success.

| Performance Requirements Summary | | | |
|---|---|---|---|
| **Performance Objective** | **Performance Standard** | **Acceptable Performance Level** | **Method/Measure** |
| 1. Project Management | Manages the project, provides Contractor project management plan, project schedule, coordinates meetings and monthly project activity report. | 100% of items are provided on time and issues are addressed for each VA Medical Center task order. | Quality Assurance Surveillance conducted by COR monthly. |
| 2. Installation, configuration, customization and implementation | Provides services and supplies required to install the EIS | 100% of services and supplies are provided on time for each VA Medical Center task order. | Quality Assurance Surveillance conducted by COR monthly. |
| 3. Legacy Data Migration Services | Migrates prior exams to the EIS within a 6-month period from the start of clinical use. | 100% of past 2 years migrated before Go-Live and 100% of remaining 2 years migrated within 6 months after the Go-Live date. | Quality Assurance Surveillance conducted by COR monthly. |
| 4. Training and Go-Live Support | Trains clinicians, system administrators and biomedical staff. | 100% of trained provided prior to Go-Live date. | Quality Assurance Surveillance conducted by COR monthly. |

| | | | |
|---|---|---|---|
| 5. On-Going Maintenance and Support | Performs remote and/or on-site services in accordance with the PWS. | 100% of all unscheduled requests are addressed; 99% schedule maintenance is achieved on time. | Quality Assurance Surveillance conducted by COR monthly. |
| 6. Response Time | Ensures response times are met in accordance with PWS Table 1 – Response Time. | 98% of response times are met. | Quality Assurance Surveillance conducted by COR monthly. |
| 7. System Uptime | Ensures the EIS at each VA Medical Center is operable and available for use. | 99% availability (uptime). | Quality Assurance Surveillance conducted by COR monthly. |
| 8. Reports and Documentation (Effective Communication) | Project status reports, product delivery reports are accurate and received on time. | 99% of reports are provided on schedule. | Quality Assurance Surveillance conducted by COR monthly. |



## 7. IDENTIFICATION OF PARTICIPANTS IN ACQUISITION PLAN PREPARATION

| Name | Title | Organization |
|---|---|---|
| Jason Dominitz | MD, National Director | VHA National Gastroenterology PMO |

| | | |
|---|---|---|
| Robert Zing | RN, Nurse Manager | VHA National Gastroenterology PMO |
| James Wilson | Administrative Officer | VHA National Gastroenterology PMO |
| Jason Newman | Dep PM, Biomedical Engineer | ELCM PEO |
| | | |
| Michael McDonald | Biomedical Engineer | VISN 20 Biomedical Engineer |
| Charles Herring | Project Manager | ELCM PEO, Clinical Equipment Team |
| Jeff Young | Dep PM, NX EQPEO | ELCM PEO, Clinical Equipment Team |
| Nadia Northrup | Contract Specialist | SAC |
| Sharon Redman | Contracting Officer | SAC |

## 8. SECURITY

### 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. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

c. 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.

d. 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.

## 8.3. VA INFORMATION CUSTODIAL LANGUAGE

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

b. 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 ontractor/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.

c. 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.

d. 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.

e. 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.

f. 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.

## 8.4. 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 COTR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

b. 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.

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. 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 30 days.

g. 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.

f. VA prohibits the installation and use of personally-owned or contractor/subcontractor owned equipment or software on VA’s network. If non-VA owned equipment must be

used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.
g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

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 preapproved 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.

**8.5. SECURITY INCIDENT INVESTIGATION**

a. The term "security incident" means an event that has, or could have, resulted in

unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

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

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

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

**8.6. 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. However, it is the policy of VA to forgo collection of liquidated damages in the event the contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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, plain text;
(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 $_____ 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.

**8.7. 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 VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

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

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.

**9. Position Risk Designation Level**

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

| **Position Sensitivity** | **Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A) |
|---|---|
| **Low/ Tier 1** | **Tier 1/ National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions. |

| | |
|---|---|
| **Position Sensitivity** | **Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A) |
| **Moderate/ Tier 2** | **Tier 2/ Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree. |
| **High/ Tier 4** | **Tier 4/ Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree. |

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

| Task Number | Tier1/ Low/ NACI | Tier 2/ Moderate/ MBI | Tier 4/ High /BI |
|---|---|---|---|
| All Tasks | ☒ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |

**9. 1 Contractor Personnel Security Requirements**

Contractor Responsibilities:

The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
The contractor shall bear the expense of obtaining background investigations.
Within three (3) business days after award, the contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement, etc. The contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within one (1) day of any changes in employee status, training certification completion status,

Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
The contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
The contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:

1. For a Tier 1/Low Risk designation:
    1. OF-306
    2. DVA Memorandum - Electronic Fingerprints
2. For a Tier 2/Moderate or Tier 4/High Risk designation:
    1. OF-306
    2. VA Form 0710
    3. DVA Memorandum - Electronic Fingerprints

The contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

The contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the contractor employee should notify the COR within three (3) business days that documents were signed via e-QIP).
The contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor shall be responsible for all resources necessary to remedy the incident.
A contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the contractor will be responsible for the actions of the contractor personnel they provide to perform work for VA. The investigative history for contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

The contractor, when notified of an unfavorably adjudicated background investigation on a contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
Failure to comply with the contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by contractor and Subcontractor employees and/or termination of the contract for default.
Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.