Contract Opportunity

Sources Sought Notice

PRODUCT SERVICE CODE *	D399
SUBJECT*	Radiation Therapy Treatment Plans (VA-20-00035772)

GENERAL INFORMATION

CONTRACTING OFFICE'S ZIP-CODE *	07724
SOLICITATION NUMBER *	36C10B20Q0474
RESPONSE DATE/TIME/ZONE	07-30-2020 12 PM EASTERN TIME, NEW YORK, USA
ARCHIVE	90 **DAYS AFTER THE RESPONSE DATE**
RECOVERY ACT FUNDS	N
SET-ASIDE	
NAICS CODE *	541519
CONTRACTING OFFICE ADDRESS	Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724
DESCRIPTION *	**See Attachment**
POINT OF CONTACT * (POC Information Automatically Filled from User Profile Unless Entered)	Contract Specialist: Tinamarie Giraud Tinamarie.Giraud@va.gov 732-440-9641

PLACE OF PERFORMANCE

ADDRESS	
POSTAL CODE	
COUNTRY	

ADDITIONAL INFORMATION

AGENCY'S URL	
URL DESCRIPTION	
AGENCY CONTACT'S EMAIL ADDRESS	
EMAIL DESCRIPTION	

*** = Required Field**

Request for Information

Radiation Oncology Peer Review Software Program

TAC Number: VA-20-00035772

1. Introduction

This RFI is for planning purposes only and shall not be considered an Invitation for Bid, Request for Task Execution Plan, Request for Quotation or a Request for Proposal. Additionally, there is no obligation on the part of the Government to acquire any products or services described in this RFI. Your response to this RFI will be treated only as information for the Government to consider. You will not be entitled to payment for direct or indirect costs that you incur in responding to this RFI. This request does not constitute a solicitation for proposals or the authority to enter into negotiations to award a contract. No funds have been authorized, appropriated or received for this effort. Interested parties are responsible for adequately marking proprietary, restricted or competition sensitive information contained in their response. The Government does not intend to pay for the information submitted in response to this RFI.

Be advised that set-aside decisions may be made based on the information provided in response to this RFI. Responses should be as complete and informative as possible.

2. Submittal Information:

All responsible sources may submit a response in accordance with the below information.

There is a page limitation for this RFI of 10 pages. **NO MARKETING MATERIALS ARE ALLOWED AS PART OF THIS RFI.** Generic capability statements will not be accepted or reviewed. Your response must address capabilities specific to the services required in the attached Product Description (PD) and must include the following:

a. Interested Vendors shall at a minimum, provide the following information in the initial paragraph of the submission:

Name of Company

Address

Point of Contact

Phone Number

Fax Number

Email address

Company Business Size and Status

For VOSB and SDVOSBs, proof of verification in VIP.

b. Provide a summary of your capability to meet the requirements contained within the draft PD for the following areas:

1. Detail your company's capabilities and experience supporting federal agencies in providing a Software as a Service (SaaS) product, and how your SaaS product can satisfy the requirements listed in the PD. Include examples of federal experience implementing your SaaS product (specific examples or references provided must include the agency, point of contact, dollar value, and contract number).

2. Detail your company's SaaS product cloud infrastructure and accessibility from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The system shall not require download of software to VA computers. The VA shall not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or individual application capabilities. The system shall be vendor or third-party hosted and require no servers within VA. Please validate that your proposed SaaS product is SaaS in accordance with the NIST 800-145 definition and describe its hosting environment.

3. Is customer data hosted in the U.S.? Do company employees or contractors outside the U.S. have access to customer data for any reason? If yes, please describe.

4. Please detail any interfacing or custom development that your SaaS product requires ahead of go-live necessary to support the requirements in the attached PD. Can your company's proposed SaaS product meet all PD requirements without developing an interface or performing any kind of custom development?

5. Please describe your company's willingness and ability to adopt and incorporate customer feedback in the product roadmap of your proposed SaaS product.

6. Please describe your pricing model to include the threshold for named user subscriptions vs. an enterprise/site subscription. Is your pricing model driven by total users, concurrent users, transaction-based, number of records, etc? Are any additional services needed outside of the subscription model (e.g., configuration to meet functional requirements, data storage, data migration, additional features)? If so, please provide the items and proposed price for these additional services.

7. Please provide separate Rough Orders of Magnitude (ROMs) for the SaaS product in accordance with PD Paragraph 1.0 and associated subparagraphs.

8. For the SaaS portion of this effort, VA intends on providing limited payment, in accordance with the attached PD, until the SaaS product has achieved a FedRAMP Authorization and a VA Authority to Operate (ATO). Once approved by the VA Authorizing Official, VA intends on setting up a subscription payment for the duration of the base period and option periods, if exercised. Do you concur or propose different payment terms?

9. The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. Is your company's SaaS product FedRAMP Authorized? If not, are you willing and ready to comply with the schedule for FedRAMP authorization deliverables in the attached PD? If not, what alternate deliverable schedule would you propose?

10. Following guidance from the Federal CIO, VA will utilize existing JAB ATO or agency ATO issued by another agency as a starting point for FedRAMP requirements. If neither of those exist, VA will sponsor FedRAMP ATO. VA will be using the FedRAMP baselines as a starting point, since they are specifically tailored for cloud services. Does your company's SaaS product have an ATO from any federal agency?

11. Detail your company's support Service Level Agreements (SLAs) for all tiers of service.

12. What was your uptime rate during the past 12 months?

13. Describe your standard release and patch cycle.

14. Do you have a preferred contract vehicle (e.g. NASA SEWP, GSA, FBO, etc.)?

Responses are due no later than Thursday July 30, 2020 at 12PM EST via email to the Contracting Officer and Contract Specialist listed below. Mark your response as "Proprietary Information" if the information is considered business sensitive.

All questions can be directed to both of the Points of Contacts listed below:
Contracting Officer: Peter Lewandowski, Peter.Lewandowski@va.gov, 732-440-9640
Contract Specialist: Tinamarie Giraud, Tinamarie.Giraud@va.gov, 732-440-9641

DRAFT

PRODUCT DESCRIPTION (PD)

DEPARTMENT OF VETERANS AFFAIRS

Veterans Health Administration

National Radiation Oncology Program

Radiation Oncology Peer Review Software Program

Date**: June 8, 2020**

VA-20-00035772

PD Version Number: 5.0

1.0 Product requirements

High quality patient care is important in any medical discipline but is of particular concern in radiation oncology given the potential for serious harm in the event of a treatment-related error. Radiation treatment planning is a very complicated process with many safety aspects involved and with the increased application of more sophisticated technologies in radiation therapy, concerns have arisen about whether radiation is being used appropriately. Quality-assurance procedures must evolve with complex radiotherapy planning and delivery systems in order to ensure that consistently effective and safe therapy is delivered. The Veterans Health Administration (VHA) concurred with the Office of Inspector General (OIG) Health Inspection report, dated March 10, 2011, that there was a need for a robust physician peer review process related to all VHA radiotherapy programs. The Radiation Oncology Peer Review will give VA centers providing inhouse radiation oncology care the capability to seek prospective physician peer reviews online. The capability will enable VA radiation oncologists to consider treatment refinements and alternatives prior to radiation delivery for the safety of Veterans.

The C&A requirements do not apply and a Security Accreditation Package is not required.

1.1 SOFTWARE APPLICATION REQUIREMENTS

VA has a requirement for software that shall be provided as part of a Software as a Service (SAAS) subscription which shall include a one-year license with 2 option years for unlimited users, upgrades, technical support and training.

The peer review SAAS shall be accessible to all 40 VA Radiation Oncology clinics via the internet using Internet Explorer or Chrome browsers and shall enable VHA radiation oncologists to seek treatment plan peer reviews on demand from any expert anywhere with Internet web access. The peer review software shall have no dependencies on or interfaces with other VA software systems. The software architecture shall allow prospective peer reviews of radiotherapy treatment plans by VA contracted nationally recognized experts in radiation oncology outside the VA. The Contractor Peer Review SaaS product shall be a hosted on the Contractor cloud environment.

1.1.1 The Software as a Service (SAAS) subscription that shall meet the following criteria:

A. Users shall be able to securely upload & download imaging datasets from modalities such as computerized tomography (CT), magnetic resonance (MR), secondary capture (SC), computer radiograph (CR), portal, and digitally-constructed radiograph (DRR) as well as

radiation therapy data objects (DICOM Intranet (Digital Imaging and Communication in Medicine (DICOM) Radio Therapy (RT) plans, RT Structure set, RT Dose, RT Images) over the VA's intranet.

B. Provide tools to anonymize the above mentioned datasets before the users upload them to the Contractor hosted Radiotherapy - Picture Archiving and Communication System (RT PACS) database. This tool shall have the ability to scrub all the PHI/PII data elements from the DICOM files based on the Health Insurance Portability and Accountability Act (HIPAA) privacy rules safe harbor methods. Section 164.514 of the HIPAA Privacy Rule provides the standard for de-identification of PHI/PII data elements. These anonymization tools shall be deployed on the VA computers where anonymization of the datasets shall be performed. Once the anonymization is complete the users shalls be able to upload the anonymized datasets to the Contractor hosted cloud based RT PACS database.

C. Provide all data communication between the users web portal and the Contractor hosted cloud based RT PACS database shall be secure and follow the industry standard (FEDRAMP) security protocols. The system shall be automated such that the data is automatically registered and entered into the RT PACS database.

D. Patient confidentiality shall be maintained throughout the peer review process and anonymous case datasets and peer reviewers observations data cannot be accessed by an unauthorized user within or external to the system.

E. Peer review cases submitted by the VA clinical providers need to be made available immediately (within 1 hour) for rapid review by the VA contracted nationally recognized experts in radiation oncology outside the VA.

F. Provide tools to download all clinical data in the Contractor cloud RT-PACS server to a local archive in the VA.

G. Data objects shall be editable with the support of data authoring and versioning (DAV) control.

H. Accessible to multiple simultaneous VA users at any given time. We estimate approximately 40 software user accounts to be accessed simultaneously. It is estimated that there will be up to 10,000 cases per year.

I. Security shall be implemented by performing lossless compression and encryption on all data before transmission. Data shall also be stored both compressed and encrypted in the database as a further measure of security.

J. The data exchange protocol employed throughout shall be secure hypertext transfer protocol (HTTPS) for all transfers. This enables transfer from most firewall-protected networks which typically allow HTTP and secure hypertext transfer protocol HTTPS data transfers.

K. Provide a software and tools online User Manual detailing all user capabilities and functions with troubleshooting section on the use of software and transmission of planning data files to National Expert and transmission of planning data files to the program office representative. Contractor shall ensure that the most recent version of the Online User Manual is assessable to VA and reflects capabilities of the most recent version of software.

Deliverable:

A. Online User Manual

1.1.2 SOFTWARE COMPONENTS

The Peer Review software application shall satisfy the following software components requirement as illustrated in the figure from Appendix A “Peer Review Infrastucture of VA Radiation Oncology”. All the below mentioned software components are illustrated in the figure from Appendix A.

A. Web-based secure object archiving system (Web based RT-PACS): The software shall support all DICOM Message Service Elements (DIMSE) listed in the table below and can read, write and analyze DICOM (including all radiotherapy information object definitions [IODs]) and flat files (Part 10 Format). The software application shall be able to accept data over secure HTTPS web services protocol

DIMSE Services:

Name	Group	Type
C-STORE	DIMSE-C	operation
C-GET	DIMSE-C	operation

Name	Group	Type
C-MOVE	DIMSE-C	operation
C-FIND	DIMSE-C	operation
C-ECHO	DIMSE-C	operation

B. DICOM RT data viewer: The software shall have the infrastructure of comprehensive tools required for preparation, submission, auto-archiving, Web-based review, and retrieval of diagnostic images, treatment-planning images, and radiation therapy objects. The software shall have the features of auto anonymizing datasets before they are submitted for peer review. The software shall have tools for calculating Dose Value Histograms (DVHs) and compositing doses from different trials of the patient. In addition to DICOM RT data the software shall have the ability to handle PDF attachments with the clinical cases for review.

C. Data analytics: The Contractor shall provide data analytic tools and dashboards to quantitatively evaluate the quality of treatment plans. The data analytics tool shall have interactive dashboards to view aggregated data from peer review results and treatment plans over time.

D. Data anonymizer: Template based anonymization tools shall be provided by the Contractor to remove any PHI/PII from the DICOM/DICOM-RT datasets before they are uploaded to the Contractor hosted cloud RT-PACS. The template-based anonymization shall have custom anonymization schemes to be applied automatically to the incoming treatment plan data. Upon anonymization the DICOM and clinical data shall be encrypted using Federal Information Processing Standards-140/2 (FIPS-140/2) supported encryption protocols. The anonymization tools will be deployed on the users VA computers where anonymzation and encryption of the abovementioned DICOM datasets will be performed before they are securely uploaded to the contractor hosted cloud RT-PACS.

E. The Peer review software application shall be seamlessly interoperable with radiotherapy planning (TPS) and oncology information systems (OIS) that are utilized in the VA Radiation Oncology clinics such as Varian Eclipse/Aria, Phillips Pinnacle, Elekta XiO, Elekta Mosaiq, Raysearch RayStation, Accuray Cyberknife and Accuray Tomotherapy TPS.

1.2 SOFTWARE APPLICATION DATA SECURITY REQUIREMENTS

1.2.1 DATA SECURITY

The software shall meet the following data security criteria:

A. The software capability shall include a secure (access to patient data) and unsecure (access to general information regarding the functionalities of software) section. Access to secure section shall be divided into multiple levels, based on the privilege level assigned to a user. The privilege level shall be assigned based on the need of a user to view clinical data submitted to the RT servers. Each expert reviewing cases will have access to data submitted for his/her domain only. The software shall ensure end-users have access to only their data. Each user will have to register once with the software server and get a user name and user password. Before an account is activated, the software shall send a notification to a VA system administration requesting user credentials verification. Access to data shall be hierarchical. Browsers and Web services shall use a Secure Socket Layer (SSL) for secure communication. The RT servers shall exchange a public key certificate with client applications. The key certificate shall be published for the domain and signed by a certificate authority; the client application (browser) establishes an encrypted connection between itself and the RT servers.

B. Once a user logs in, a unique session shall be created on the server memory. This session shall expire after 30 minutes if there is no activity on the software. Thus, if the user computer is left unattended, the session data cannot be accessed after the expired time by others. In addition, presentation of each dynamic page depends on this unique session.

C. The Contractor shall coordinate with applicable VA stakeholders to obtain an Authority to Operate (ATO) to interface the hosted environments to the VA Network. The Contractor shall provide all Assessment and Authorization (A&A) support and documentation required to achieve and maintain full A&A certification using the process specified in the FedRAMP Program Requirements.

D. Contractor shall be fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, continuous monitoring, system patching and change management procedures and the completion of an acceptable

contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems.

E. Ensure adequate security controls for collecting, processing, transmitting, and storage and removal of Personally Identifiable Information (PII) and Personal Health Information (PHI), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA.

F. Ensure these security controls are to be assessed and stated within the Privacy Impact Assessment (PIA) and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) shall be submitted and approved prior to the collection of PII and PHI.

G. The Contractor shall complete a Third-Party Assessment Organization (3PAO) Security Assessment Plan (SAP) within 75 days after contract award.

H. The Contractor shall complete a 3PAO Security Assessment Report (SAR) within 90 days after contract award.

I. The Contractor shall provide an A&A Authority To Operate (ATO) Package that includes the following security documentation IAW Appendix C Authorization Requirements Standard Operating Procedure (SOP):

1. System Security Plan (SSP),
2. Risk Assessment (RA),
3. Incident Response Plan (IRP),
4. Information Security Contingency Plan (ISCP),
5. Disaster Recovery Plan (DRP),
6. Configuration Management Plan (CMP),
7. Interconnection Security Agreement/Memorandum of Understanding (ISA/MOU),

8. Additional system description/and diagrams required by VA to gain access to VA network and receive an ATO.

Deliverables:

A. ATO Package
B. 3PAO SAP
C. 3PAO SAR
D. Plan of Action and Milestones

1.3.2 ASSESSMENT, AUTHORIZATION, AND CONTINUOUS MONITORING

A. The information system solution selected by the Contractor shall comply with the Federal Information Security Management Act (FISMA).

B. The Contractor shall comply with FedRAMP requirements (https://www.fedramp.gov/agency-authorization/) as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement.

C. Following guidance from the Federal CIO, VA will utilize existing Joint Authorization Board (JAB) ATO or agency ATO issued by another agency as a starting point for FedRAMP requirements. If neither of those exist, VA will sponsor FedRAMP ATO. VA will be using the FedRAMP baselines as a starting point, since they are specifically tailored for cloud services.

D. The Contractor shall, where applicable, assist with the VA Authority to Operate (ATO). Process to help achieve agency authorization of the cloud service or migrated application.

E. The Contractor shall afford VA access to the Contractor's and Cloud Service Provider's facilities, installations,technical capabilities, operations, documentation, records, and databases.

F. If new or unanticipated threats or hazards are discovered by either VA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

G. The Contractor shall not release any data without the consent of VA in writing. All requests for release must be submitted in writing to the COR/CO.

Other considerations:

1. Trusted Internet Connection (TIC) – Include TIC requirements for SaaS that interfaces with VA systems, SaaS must meet all VA Security requirements for non-SaaS.

2. Include Addendum A – Additional VA Requirements, Consolidated

1.3.3 PEER REVIEW APPLICATION - FedRAMP REQUIREMENT

The Peer Review application shall be hosted on a FedRAMP-Low certified cloud solution. The Contractor shall provide a copy of the certificate issued granting Authority to Operate the cloud provider that is hosting the Peer Review application. The Contractor shall maintain its security authorization throughout the contract period of performance.

Deliverable:

A. FEDRAMP Low Certification

1.4 TRAINING AND TRAINING DOCUMENTS/MATERIALS

The Contractor shall provide two virtual, Instructor led training sessions (on Skype or Webex) for approximately 200 users on the operations and functionality of the software, including a online troubleshooting / FAQs. The training shall also include procedures to submit radiotherapy treatment plans to the Contractor cloud RT-PACS server. The Contractor shall deliver the PowerPoint Training Slide Deck. The Contractor shall record the training session and provide online access to the recorded training session playable on MS Windows10 environment. The Contractor shall coordinate with the COR to schedule the training sessions to be completed prior to software going operational.

The Contractor shall conduct quarterly virtual software update webinar sessions (via Skype or Webex) for approximately 100 users in the VA. The Contractor shall deliver the Quarterly webinar PowerPoint Training Slide Deck. The Contractor shall record the Quarterly webinar training session and provide a online access to the recorded training session playable on MS

Windows10 environment. The Contractor shall coordinate with the COR to schedule the Quarterly webinar training sessions with the VA end users.

Deliverables:

A. PowerPoint Training Slide Deck and Video.
B. Quarterly Webinar PowerPoint Training Slide Deck and Video.

1.5 HELP DESK SUPPORT

The Contractor shall provide Help Desk support to Users to have the ability to operate and resolve problems encountered while using the Radiation Oncology Peer Review software. The Help Desk support shall include users access to live chat, email, toll free telephonic support. The support shall be available Monday through Friday 8 AM to 8 PM Eastern Time.

The Contractor shall maintain a Help Desk trouble ticket log. The trouble ticket log shall log the date and time of each original help desk request, date and time of initial response, detailed description of action(s) taken, including date and time of each action, name of technician, and date and time of final resolution. This information shall be incorporated into the Quarterly Status Report.

1.6 CONTRACT AWARD MEETING

The Contractor shall hold a contract award meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least two calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three (3) calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM. The Contractor shall not commence performance on the tasks in this Product Description until the CO has conducted a kick off meeting.

1.8 QUARTERLY status REPORTS

The Contractor shall submit quarterly status reports to the COR and PM for the present and previous quarter's activities, open issues, risk and mitigation actions, issues closed and Help Desk activities from the trouble ticket log. The Contractor status report should include any action items from the previous quarter's status report.

Deliverable:

A. Quarterly Status Reports

1.9 ACCEPTANCE TESTING

Prior to system "go-live" in a real-world environment, the Contractor shall undergo VA testing review and approval. The Contractor shall support VA conduct Acceptance Testing for the SAAS product based the American Assocication of Medical Physics recommendations in AAPM medical physics practice guideline 5.a.: commissioning and qa of treatment planning dose calculations — megavoltage photon and electron beams (https://aapm.onlinelibrary.wiley.com/doi/full/10.1120/jacmp.v16i5.5768). The plan should test the functionality of the software, connectivity and operational readiness of users. The VA will provide test cases designed to stress the system capabilities. Any problems must be identified and be corrected by Contractor before the system can be re-tested. The system must pass the testing and be accepted prior to commencement of services and invoicing.

2.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508)

On January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

2.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines. A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is available from the Access Board: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule.

The Contractor shall comply with "508 Chapter 2: Scoping Requirements" for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria
- ☐ E206 Hardware Requirements
- ☒ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

2.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

2.3 ACCEPTANCE AND ACCEPTANCE TESTING

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

3.0 GENERAL REQUIREMENTS

3.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (VA TRM). The VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. Moreover, the VA TRM, which includes the Standards Profile and Product List, serves as a technology roadmap and tool for supporting OI&T. Architecture & Engineering Services (AES) has overall responsibility for the VA TRM.

3.3 POINTS OF CONTACT

VA Program Manager:

Name: Edwinette Moses
Address:1201 Broad Rock Blvd
Richmond, VA 23249
Voice: 804.675.6270
Email: Edwinette.Moses@va.gov

Contracting Officer's Representative:
Name: Edwinette Moses
Address:1201 Broad Rock Blvd
Richmond, VA 23249
Voice: 804-675-5000 X 3002
Email: Edwinette.Moses@va.gov

4.0 DELIVERY

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Ship To and Mark For: All delivery will be electronic delivery of software and software licenses to:

	Primary
Name:	Edwinette Moses
Address:	1201 Broad Rock Blvd Richmond, VA 23249
Voice:	804-675-5000 X 3002
Email:	Edwinette.Moses@va.gov

4.1 SPECIAL SHIPPING INSTRUCTIONS

Prior to shipping, Contractor shall notify Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. The Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of products to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall bear the VA IFCAP 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 IFCAP PO number shall indicate total number of containers for the complete shipment (e.g. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))
Project Description: (e.g. Tier I Lifecycle Refresh)

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

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. 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.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the

resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO 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 CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of 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).

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

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become

applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

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

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

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA 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 CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records

and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

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

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

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for

the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

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

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

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**,** but in no event longer than 7 days.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to 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 7 days.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this

paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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

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

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government.

Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

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

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA 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 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 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.

B6. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

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

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have

known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

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

B7. 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 Breaches Involving Sensitive Personal Information*, 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 VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;

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

3) Data breach analysis;

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

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. 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 Information Security Rules of Behavior, updated version located at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848, relating to access to VA information and information systems;

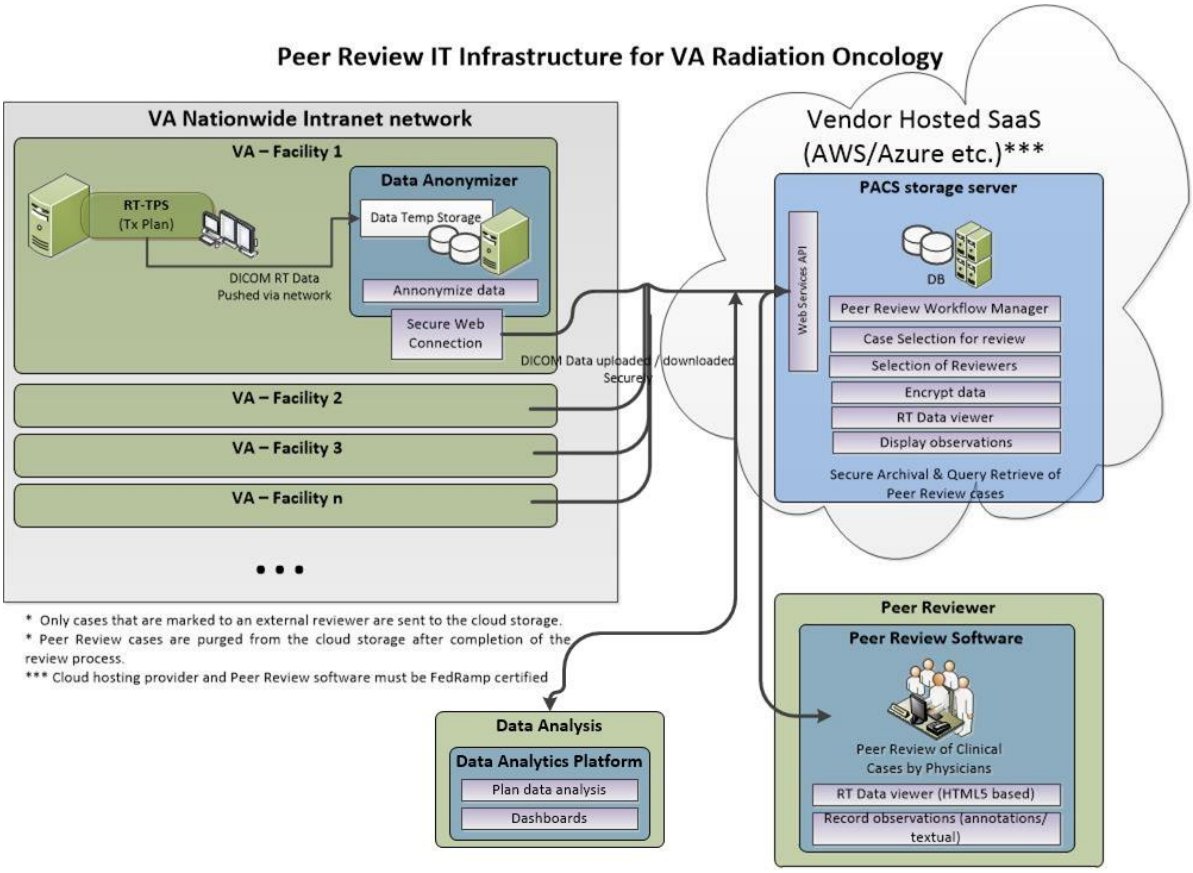
2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;

3) 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 CO 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 CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically 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.

Appendix A


Peer Review IT Infrastructure for VA Radiation Oncology
VA Nationwide Intranet network
VA – Facility 1
RT-TPS
(Tx Plan)
DICOM RT Data
Pushed via network
Data Anonymizer
Data Temp Storage
Annonymize data
Secure Web
Connection
VA – Facility 2
VA – Facility 3
VA – Facility n
• • •
DICOM Data uploaded / downloaded
Securely
Vendor Hosted SaaS
(AWS/Azure etc.)***
PACS storage server
Web Services API
DB
Peer Review Workflow Manager
Case Selection for review
Selection of Reviewers
Encrypt data
RT Data viewer
Display observations
Secure Archival & Query Retrieve of
Peer Review cases
* Only cases that are marked to an external reviewer are sent to the cloud storage.
* Peer Review cases are purged from the cloud storage after completion of the review process.
*** Cloud hosting provider and Peer Review software must be FedRamp certified
Data Analysis
Data Analytics Platform
Plan data analysis
Dashboards
Peer Reviewer
Peer Review Software
Peer Review of Clinical
Cases by Physicians
RT Data viewer (HTML5 based)
Record observations (annotations/
textual)