PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology (OI&T)
DevSecOps, Software Product Management
Health, Clinical Services, Diagnostics Sub-Product Line

Community Image Exchange Service

Date: June 16, 2022
VA-22-00069519
PWS Version Number: 0.5

Request for Information (RFI)

****This posting is not a formal request for quote, but rather a market research request to determine if there are viable sources to provide the above requirement.****

Contents

1.0 BACKGROUND 4
2.0 APPLICABLE DOCUMENTS 5
3.0 SCOPE OF WORK 5
3.1 APPLICABILITY 6
3.2 ORDER TYPE 6
4.0 PERFORMANCE DETAILS 6
4.1 PERFORMANCE PERIOD 6
4.2 PLACE OF PERFORMANCE 6
4.3 TRAVEL 6
4.4 CONTRACT MANAGEMENT 7
4.5 GOVERNMENT FURNISHED PROPERTY 7
4.6 SECURITY AND PRIVACY REQUIREMENTS 8
4.6.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 8
5.0 SPECIFIC TASKS AND DELIVERABLES 9
5.1 PROJECT MANAGEMENT 9
5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN 9
5.1.2 REPORTING REQUIREMENTS 9
5.1.3 TECHNICAL KICKOFF MEETING 11
5.1.4 ONBOARDING 11
5.2 ARCHITECTURE SUPPORT 13
5.2.1 SOLUTION INTEGRATION DESIGN 13
5.2.2 HOSTING AND OPERATIONS ANALYSIS 14
5.2.3 CONTINUOUS IMPROVEMENT 14
5.3 IMPLEMENTATION SUPPORT 14
5.3.1 VISN DEPLOYMENTS 15
5.3.2 INTERFACE CONNECTIVITY 15
5.3.3 INFORMATION ASSURANCE 15
5.3.4 IOC SUPPORT 17
5.4 OPERATIONS SUPPORT 18
5.4.1 VAEC SOLUTION SUPPORT 18
5.4.2 SOLUTION AVAILABILITY MONITORING AND REPORTING 19
5.4.3 HELP DESK SUPPORT 19
5.4.4 TRAINING MATERIALS 21
5.4.5 EHR TRANSITION SUPPORT 21
5.5 VISTA DEVELOPMENT 21
5.5.1 AGILE DEVELOPMENT 21
5.5.2 IOC 22
5.5.3 DEFECT RESOLUTION 23
5.6 ADDITIONAL VISTA DEVELOPMENT (OPTIONAL TASK #1) 25
5.7 CERNER EHR INTEGRATION (OPTIONAL TASK #2) 25
5.8 CIE SOLUTION FOR ADDITIONAL VISNS (OPTIONAL TASK #3) 26
5.9 NEW CIE SOLUTION FOR ADDITIONAL VISNS (OPTIONAL TASK #4) 26

5.10 OPTION PERIODS 26
6.0 GENERAL REQUIREMENTS 27
6.1 PERFORMANCE METRICS 27
6.2 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS 28
6.2.1 COMPATIBILITY WITH ASSISTIVE TECHNOLOGY 28
6.2.2 ACCEPTANCE AND ACCEPTANCE TESTING 29
6.3 SHIPMENT OF HARDWARE OR EQUIPMENT 29
6.4 ENTERPRISE AND IT FRAMEWORK 29
6.5 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS 29
6.6 ORGANIZATIONAL CONFLICT of INTEREST 29
APPENDIX A 30
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE 32

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information & Technology (OIT), DevSecOps, Software Product Management, Health strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

Implementation of the 2018 VA Mission Act has resulted in large numbers of Veterans obtaining imaging studies outside of VA, while continuing to receive clinical care within VA. Effective and efficient VA-provided care depends upon timely access to these Digital Imaging and Communication in Medicine (DICOM) image-based exams. In addition, large numbers of Veterans obtain their imaging studies and/or specific care within the VA but receive other care outside the VA. To obtain the best possible care, Veterans receiving care outside the VA are entitled and encouraged to share their VA-provided image studies with outside providers. Current image transfer solutions in both directions are cumbersome, inefficient, labor intensive, and often result in substantial delays to patient care.

At present, DICOM images from outside providers are commonly stored onto Compact Discs (CD) and then either mailed or hand-carried from the provider to the VA. The process of then importing the images into specialty Picture Archiving and Communication Systems (PACS) and/or VistA Imaging is time consuming and fraught with delay and misadventure. Lost CDs, dysfunctional CDs that cannot be accessed by VA systems, failures related to network security or systems incompatibility, and a wide variety of other possible problems that each cause delays to patient care.

Diagnostics reports or clinical findings produced by community provider are typically more clinically relevant than the images. The primary means VA receives these reports from community providers uses analog telephone-based facsimile (fax). The fax report is often scanned and/or converted to PDF format and stored within VistA Imaging. While imaging exams performed at VA facilities attach both clinical images and textual reports to radiology accession numbers or specialty consults, these external reports generally get associated with community care notes. A VA provider looking for clinical findings will experience inconsistency and productivity loss when checking multiple locations in the electronic medical record for the patient's results.

For imaging studies taken by the VA and shared with outside providers, the process described above runs in reverse but has the same inherent risks. In addition, there are significant supply, mailing, and staffing costs when using CDs for VA image sharing with community providers.

A minority of VHA (Veterans Health Administration) healthcare facilities have successfully integrated commercial cloud-based DICOM image sharing solutions. These products eliminate the troublesome DICOM CDs and provide industry standard based

methods to securely and efficiently transfer imaging exams bidirectionally between disparate systems at both VA and partnered community providers. Unfortunately, the burdensome process to show conformance with VA Information Technology security standards have resulted in several VHA imaging entities abandoning efforts to integrate these solutions. The lack of dedicated OI&T enterprise level support for these initiatives has led to limited adoption of these innovative cost and time saving solutions.

2.0 APPLICABLE DOCUMENTS

The Contractor shall comply with the following documents, in addition to the documents in Paragraph 2.0 in the T4NG Basic Performance Work Statement (PWS), in the performance of this effort:

1. Digital Imaging and Communications for Medicine (DICOM) Standard Version 3.0 https://www.dicomstandard.org
2. Integrating the Healthcare Organization Radiology Profile for Infrastructure: Cross-Community Access for Imaging and Cross-Enterprise Reliable Document Interchange for Imaging https://wiki.ihe.net/index.php/Profiles#IHE_Radiology_Profiles
3. VA Enterprise Cloud Technical Reference Guide, Version 1.3 July 2018

3.0 SCOPE OF WORK

The Contractor shall deploy, integrate, and maintain commercial image sharing solutions at Veterans Health Administration (VHA) facilities utilizing VistA which have not yet migrated to the Cerner Electronic Health Record (EHR). The commercial products to be deployed shall be Life Image Interoperability Suite by Life Image and Imagex by Medicom, and shall be provided by VA.

The Contractor shall provide architectural design expertise, documentation, and associated diagrams to integrate the commercial image sharing solutions with existing VA systems. The Contractor shall provide architectural services including designs, specifications, and requirements needed for the VAEC (VA Enterprise Cloud) to host software and services needed by each image sharing solution.

Each product shall be hosted in the VAEC Amazon Web Services (AWS) environment. VA will furnish VAEC capacity as Government Furnished Equipment (GFE), thus the Contractor shall not be responsible for providing or acquiring cloud capacity or server hosting infrastructure. The Contractor shall configure the deployed product to be interfaced with both commercial PACS and VistA Imaging to bidirectionally share DICOM images, exams, and related clinical findings between VA and community providers.

The Contractor shall provide ongoing application installation, configuration and patching support of Community Image Exchange (CIE) solutions hosted in the VAEC. The Contractor shall provide solution monitoring to ensure availability and performance and provide outage alerting services. The Contractor shall provide help desk support utilizing the Service Now (SNOW) or the VA's preferred incident management solution. The Contractor shall provide transition of image sharing services if the need arises to offboard an existing VHA site or Veterans Integrated Service Network (VISN) customer to the Cerner EHR.

The Contactor shall provide software enhancements to specific areas of VistA and VistA Imaging software to support the streamlining of exam or consult registration, completion, and the effective transfer of clinical findings and/or reports to and from the Radiology/Nuclear Medicine, and Consult/Request Tracking (GMRC) VistA packages.

3.1 APPLICABILITY

This Task Order (TO) effort PWS is within the scope of paragraph(s) 4.1 Project Management, 4.2 Software Engineering, 4.3 Software Demonstration and Transition, 4.4 Test & Evaluation, 4.8 Operation & Maintenance, 4.9 Cyber Security, and 4.10 Training of the T4NG Basic PWS.

3.2 ORDER TYPE

The effort shall be proposed on a Firm Fixed Price (FFP) basis.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be a 12-month base period with four 12-month option periods and five (5) optional tasks. Optional Task Five is for Transition and Orientation Support with a 60-day PoP. The overall PoP of this effort shall not exceed 60 months.

4.2 PLACE OF PERFORMANCE

Efforts under this TO shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their Task Execution Plan submission.

4.3 TRAVEL

The Government does not anticipate any travel to perform the tasks associated with this effort.

4.4 CONTRACT MANAGEMENT

All requirements of Sections 7.0 and 8.0 of the T4NG Basic PWS apply to this effort. This TO shall be addressed in the Contractor's Progress, Status and Management Report as set forth in the T4NG Basic contract.

4.5 GOVERNMENT FURNISHED PROPERTY

The Government has multiple remote access solutions available to include Citrix Access Gateway (CAG), Site-to-Site Virtual Private Network (VPN), and RESCUE VPN.

The Government's issuance of Government Furnished Equipment (GFE) is limited to Contractor personnel requiring direct access to the network to development environments; install, configure and run Technical Reference Model (TRM) approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner); upload/download/ manipulate code, run scripts, and apply patches; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

When necessary, the Government will furnish desktops or laptops, for use by the Contractor to access VA networks, systems, or applications to meet the requirements of this PWS. The overarching goal is to determine the most cost-effective approach to providing needed access to the VA environment coupled with the need to ensure proper Change Management principles are followed. Contractor personnel shall adhere to all VA system access requirements for on-site and remote users in accordance with VA standards, local security regulations, policies, and rules of behavior. GFE shall be approved by the COR and Program Manager on a case-by-case basis prior to issuance.

Based upon the Government assessment of remote access solutions and requirements of this TO, the Government estimates that the following GFE will be required by this TO:

1. Ten (10) standard laptops
2. Cloud capacity in and connectivity to the VA Enterprise Cloud (VAEC) environment
3. VA Enterprise Cloud Operational Tools (VAECOT) comprised of a suite of COTS cloud management tools as identified in the VAEC Technical Reference Guide
4. Enterprise Development Environment (EDE) and Tools as identified in the VAEC Technical Reference Guide

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop

bags, extra charging cables, extra Personal Identity Verification card readers, peripheral devices, or additional Random-Access Memory (RAM). The Contractor is responsible for providing these types of IT accessories in support of the TO as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

The Status of Government Furnished Equipment Report under the T4NG Basic Contract requirements is applicable to this TO and shall be delivered to the COR/VA PM as required.

4.6 SECURITY AND PRIVACY REQUIREMENTS

All requirements in Section 6.0 of the T4NG Basic PWS apply to this effort. Specific TO requirements relating to Addendum B, Section B4.0 paragraphs j and k supersede the corresponding T4NG Basic PWS paragraphs, and are as follows,

j. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than two (2) days.

k. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to 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 two (2) days.

All requirements in Section 6.0 of the T4NG Basic PWS apply. Addendum B requirements have been tailored to reflect the security and privacy requirements of this specific TO.

It has been determined that protected health information may be disclosed or accessed, and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the Request for Task Execution Plan (RTEP) and shall comply with VA Directive 6066.

4.6.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity, and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	X		
5.2	X		
5.3			X
5.4			X
5.5	X		
5.6			X
5.7	X		
5.8			X
5.9			X

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide a Monthly Progress Report in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for

each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding month.

The Monthly Progress Report shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall provide monthly representation at the CIE Integrated Product Team (IPT) virtual meetings with government staff. The IPT meetings will provide a means to interactively answer questions and provide feedback regarding project status as well as a forum for the Contractor to clarify project requirements with business owners and Subject Matter Experts (SMEs).

The Contractor shall use VA's implementation of Jira, GitHub, or other VA-approved toolset to provide a single, authoritative Agile product lifecycle management tool to track execution details in a Product Data and Artifact Repository. All OIT product data and artifacts shall be required to be managed in this repository daily to synchronize work and ensure version control.

The Contractor shall utilize the VA-approved toolset to:

1. Input and manage scheduled product sprints and backlog
2. Input and manage product Agile requirements
3. Input and manage product risks and issues
4. Input and manage product configurations and changes
5. Input and manage product test plans and execution
6. Input and manage product planning, design, and engineering documentation
7. Input and manage product user guides and training materials
8. Input and manage linkages to correlate requirements to change orders to configurable items to risks, impediments, and issues to test cases and test results to show full traceability

All project electronic communications will be accomplished using VA network accounts.

Deliverables:

A. Monthly Progress Report

5.1.3 TECHNICAL KICKOFF MEETING

A technical kickoff meeting shall be held within 10 days after TO award. The Contractor shall coordinate the date, time, and location (can be virtual) with the Contracting Officer (CO), as the Post-Award Conference Chairperson, the VA PM, as the Co-Chairperson, the Contract Specialist (CS), and the COR. The Contractor shall provide a draft agenda to the CO and VA PM at least five (5) calendar days prior to the meeting. Upon Government approval of a final agenda, the Contractor shall distribute to all meeting attendees.

During the kickoff-meeting, 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 via a Microsoft Office PowerPoint presentation. At the conclusion of the meeting, the Contractor shall update the presentation with a final slide entitled "Summary Report" which shall include notes on any major issues, agreements, or disagreements discussed during the kickoff meeting and the following statement "As the Post-Award Conference Chairperson, I have reviewed the entirety of this presentation and assert that it is an accurate representation and summary of the discussions held during the Technical Kickoff Meeting for the Community Image Exchange."

The Contractor shall submit the final updated presentation to the CO for review and signature within three (3) calendar days after the meeting. The Contractor shall also work with the CS, the Government's designated note taker, to prepare and distribute the meeting minutes of the kickoff meeting to the CO, COR and all attendees within three (3) calendar days after the meeting. The Contractor shall obtain concurrence from the CS on the content of the meeting minutes prior to distribution of the document.

5.1.4 ONBOARDING

The Contractor shall manage the onboarding of its staff. Onboarding includes steps to initiate secure timely background investigations, complete required training, obtain a VA PIV card, network, and email accounts, and gain physical and logical access.

The Contractor shall identify individuals who may require elevated privileges to necessary development and test environments for the various systems to be enhanced. After review between the Contractor and VA COR, a government decision will be made as to the necessity of obtaining GFE for the onboarding staff. If approved, the Contractor shall follow the appropriate steps to obtain the equipment.

A single Contractor Onboarding point of contact (POC) shall be designated by the Contractor that tracks the onboarding and offboarding status of all Contractor personnel. The Contractor Onboarding POC shall be responsible for coordinating all required onboarding paperwork is properly completed and submitted within three (3) business days from start date provided to the VA COR. The Contractor shall be responsible for

tracking the status of all its staff onboarding activities to include the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. The Contractor Onboarding POC and Contractor PM of the TO shall communicate any issues with in-processing/onboarding of an incoming Contractor resource and shall follow-up with the VA POC of the status as required. The Contractor shall include a monthly Staffing Status as a section of the Monthly Progress Report to include outstanding onboarding requests for review by the COR and VA PM and required offboarding PIV and GFE (if applicable) confirmed return/turn-in dates. The monthly Staffing Status section of the Monthly Progress Report shall include the certifications, education and other information that adequately establishes the Contactor staff employee's credentials and Service Contract Act status (exempt or non-exempt).

The Contractor and VA lead(s) shall determine which team members require access to the VA network. All Contractors that require access shall complete all required VA Talent Management System (TMS) training courses within 14 days of the identification of the access need. The Contractor shall work with its respective point of contact to obtain access to TMS to complete the mandatory courses.

As an action under the Continuous Readiness in Information Security Program (CRISP), VA's Assistant Secretary for Information and Technology issued a memorandum requiring all VA Government and contract staff to complete information security awareness and applicable role-based training.

The Contractor shall submit TMS Training Certificates of completion for VA Privacy and Information Security Awareness (PISA), Rules of Behavior (ROB), Health Insurance Portability and Accountability Act (HIPAA), and role-based trainings. The Contractor shall provide signed copies of the Contractor Rules of Behavior in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security."

The Contractor shall complete the appropriate VA TMS role-based training courses for all Contractors with required access to Elevated Privileges:

1. TMS ID 3197: Information Security Role-Based Training for IT Specialist (Web Based Training [WBT])
2. TMS ID 3867205: Training for Elevated Privileges for System Access (WBT)
3. TMS ID 1016925: Information Security Role-Based Training for Software Developers (WBT)
4. TMS ID 1357076: Information Security and Privacy Role-Based Training for System Administrators (WBT)
5. TMS ID 1357084: Information Security Role-Based Training for Data Managers (WBT)

6. TMS ID 1357083: Information Security Role-Based Training for Network Administrators (WBT)
7. TMS ID 64899: Information Security Role-Based Training for IT Project Managers (WBT)

The Contractor shall complete the following Agile training courses, and other emerging PLM and SAFe courses as necessary:

1. TMS ID 4533235: Product and Product Line Management: Creating and Managing the Product Back Log
2. TMS ID 4533231: Product and Product Line Management: Overview of Product Line Management
3. TMS ID 4551891: Introduction to Agile
4. TMS ID 4551982: Product Owner

The Contractor shall complete emerging training requirements for GitHub, Jira, or other VA-approved tools as appropriate or required.

Contractors who have completed these VA training courses within the past 12 or 24 months, depending on the training requirements, and have furnished training certificates to VA, will not be required to re-take the courses.

Deliverable:

A. Training Certifications

5.2 ARCHITECTURE SUPPORT

5.2.1 SOLUTION INTEGRATION DESIGN

Using standards-based solutions available to each image sharing solution, the Contractor shall select and document the best methods to interface the products with the PACS, VistA Imaging, and other related VistA packages. The Contractor shall develop an Integration Control Document (ICD) per VISN and associated architectural diagrams for each solution and update as required.

The Contractor shall create an overarching CIE Standard Operating Procedure which defines the process for intake at a VHA facilities. This intake process shall state which information must be provided by a VHA site to make use of the image sharing solutions.

Deliverables:

A. Life Image Interoperability Suite ICD
B. ImageX ICD
C. CIE Standard Operating Procedure

5.2.2 HOSTING AND OPERATIONS ANALYSIS

The Contractor shall develop an overarching VAEC Implementation Plan for components and services to be implemented based off both Life Image Interoperability Suite and ImageX solutions. The VAEC Implementation Plan shall include hosting architecture designs, diagrams, monitoring and test plans. During hosting design, the Contractor shall at a minimum consider: high availability across multiple availability zones; elastic capacity and dynamically adapt to system load and onboarding new VHA customers; geographic location and network performance between VHA sites, COTS Image sharing services, and other partner systems in order to optimize the solution performance; and specifications for conducting realistic load testing of the solution for use in capacity planning and iterative improvement.

Deliverable:

A. VAEC Implementation Plan

5.2.3 CONTINUOUS IMPROVEMENT

The Contractor shall regularly review system performance, user feedback, and maintain relevant situational awareness within VA and the overall medical imaging community. The Contractor shall produce a Quarterly Architecture Report with recommendations for improving solution performance, ease of use, and level of integration. The Quarterly Architecture Report shall include, but not be limited to, the following elements:

- Updates to or widespread adoption of medical imaging informatics standards, such as:
  - Digital Imaging Communication in Medicine (DICOM)
  - Health Level Seven (HL7)
  - Integrating the Healthcare Enterprise (IHE)
- New Image sharing solutions
- Enhanced functionality of related VA developed or COTS solutions
- Site or VISN installation of a new PACS or other VA system requiring integration with community image sharing

Deliverable:

A. Quarterly Architecture Report

5.3 IMPLEMENTATION SUPPORT

5.3.1 VISN DEPLOYMENTS

The CIE IPT will select one VISN for interface deployment of the Life Image Interoperability Suite and one VISN for interface deployment of the ImageX solution at the beginning of the base period, and each option period, if exercised. The following is a list of planned VISNs to be deployed to; this list can be adjusted over time:

- VISN 1: VA New England Healthcare System
- VISN 4: VA Healthcare
- VISN 5: VA Capitol Healthcare Network
- VISN 7: VA Southeast Network
- VISN 8: VA Sunshine Healthcare Network
- VISN 15: VA Heartland Network
- VISN 16: South Central VA Healthcare Network
- VISN 17: VA Heart of Texas Healthcare Network
- VISN 22: Desert Pacific Healthcare Network

Deployment shall be completed no later than six months after notification to the Contractor of the product, Life Image or Medicom, and VISN that requires the interface. The Contractor shall install and configure applications and services in the VAEC required to support the CIE project.

5.3.2 INTERFACE CONNECTIVITY

The Contractor shall implement the design as described in the ICD for each solution. The Contractor shall work with Life Image, Medicom, local VISN VHA staff, and regionalized IT support to help connect the interfaces. The Contractor shall test bidirectional communications, which will include realistic data that will be sent to/from VA and outside providers. To ensure successful integration of image sharing solutions within VA, the Contractor shall provide the results for approval by VA in an Interface Connection Test Report. The Contractor shall create and maintain an inventory of all IT and medical devices interfaced with the image sharing solutions in an Interface Inventory.

Deliverables:

A. Interface Connection Test Report
B. Interface Inventory

5.3.3 INFORMATION ASSURANCE

The Contractor shall ensure deployed CIE solutions and services comply with VA policies, procedures, and tooling.

The Contractor shall:

1. Obtain, support, and maintain Authority to Operate (ATOs). The ATO is granted based on satisfactory evaluation of numerous required documents; demonstrable compliance with relevant laws, regulations, and guidelines, adherence to VA policies and procedures and documented consistent timely remediation of scans for vulnerabilities and audit findings.
2. Remediate security vulnerabilities to meet or exceed time frames established in VA 6500 (30/60/90 days for critical, high, and medium severity)
3. Create, verify, and upload required documents to the VA approved Risk Management tool (e.g. Enterprise Mission Assurance Support Service [eMASS])
4. Manage and ensure vulnerability remediation status and perform tracking with a VA-provided tool (e.g. Information Central Analytics and Metrics Platform [ICAMP])
5. Provide eMASS support, applicable documentation, and coordinate with data center partners to ensure consistency with all VA ATO requirements for certification to ensure the product meets VA's information security policies and standards to ensure the successful completion of the Assessment and Authorization (A&A) process and obtain an ATO
6. Support Field Security Services Information Security Officers (ISOs) and Office of Cyber Security (OCS) Security Control Assessment (SCA) team for assessment requirements as detailed in VA Directive and Handbook 6500 Information Security Program, VA Handbook 6500.3 Certification and Accreditation of VA Information Systems
7. Conduct cybersecurity software code quality testing and validation of all software code and provide certified scan reports validating the required code quality to the extent possible
8. Perform Vector Penetration (Pen-Tests)
9. Perform Web Accessibility (Web Application Security Assessment [WASA]) scans in compliance with the top Open Web Application Security Project [OWASP]
10. Conduct and participate in vulnerability scans and tests and best practice quality checks and reviews as detailed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4. Analyze Security Controls for Federal Information Systems and Organizations, if/when requested by the COR or System Owner. Security scanning shall be performed by multiple methods and shall be done multiple times throughout the course of a project with methods such as infiltration testing (WASA, Penetration Tests), and code analysis tools (Fortify), etc.
11. Remediate critical and high vulnerabilities identified in Government scans, quality checks, or reviews / audits within required time frames based on severity (critical=30 days, high=60 days, medium=90 days)
12. Create Plan of Actions and Milestones (POAM) for any finding or vulnerability that cannot be addressed or remediated within required time frames based on Severity
13. Provide vulnerability scanning reports and assessments as detailed in NIST SP 800-30 Rev 1 Guide for Conducting Risk Assessments

14. Provide support as needed for security and non-security audits
15. Identify, document, review, update, and maintain the A&A Artifacts as needed to support an ATO request in accordance with VA policy and Federal Law and guidelines, as detailed in NIST SP 800-37 Rev 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Additionally, the Contractor shall update Product documentation based on comments from the A&A review process conducted. A&A Artifacts include, but are not limited to the following listed artifacts:

    a. System Security Plan (SSP)
    b. Security Configuration Plan (SCP)
    c. Security Configuration Management Plan (CMP)
    d. Information System Contingency Plan (ISCP) to include Business Impact Assessment (BIA)
    e. Incident Response Plan (IRP) and Test
    f. Privacy Impact Assessment (PIA)
    g. Privacy Threshold Analysis (PTA)
    h. Risk Assessment (RA)
    i. Security Configuration Checklist (SCC)
    j. Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA)
    k. Signatory Authority (SA)
    l. Disaster Recovery Plan (DRP)
    m. Database Scan Vulnerability Remediation Plan
    n. Plan of Action and Milestones (POAM) Section 508 Compliance

Deliverable:

A. A&A Artifacts

5.3.4 IOC SUPPORT

An Initial Operating Capability Evaluation is a limited production evaluation that is required for all system solutions that will be released to multiple locations. The evaluation occurs after all testing has been completed and user acceptance has been granted. The Contractor shall observe and support IOC by assisting with the tracking and investigation of issues and remediation of problems as needed. Prior to IOC, the Contractor shall work with each VISN in order to obtain an MOU and Testing Agreement.

The Contractor shall support a 10-day error free IOC at the selected VHA test sites for initial CIE solution deployment. The Contractor shall resolve and track all defects and document the findings in the Issue/Fix Status Report, as well as address all issues and questions identified during IOC. For each defect identified, the Contractor shall log the

defect, identify a resolution for the issue, and provide an Issue Resolution Plan, including timeline and impacts to the schedule and documentation. If an issue cannot be resolved with reconfiguration of existing components or process during the IOC period, it shall be noted in the Issue Resolution Plan and added to the CIE backlog.

Following VA approval of the Issue Resolution plan, the Contractor shall execute the approved plan. The Contractor shall make any necessary configuration, intake process, and supporting documentation changes.

After any issue correction during IOC, IOC shall continue with the updated solutions for a minimum of five business days error free before exiting IOC. The Contractor shall support IOC evaluation activities to ensure IOC Entry and Exit criteria are met and deliver an IOC Entry Request and Exit Summary.

Deliverables:

A. Issue/Fix Status Report
B. Issue Resolution Plan
C. IOC Entry Request and Exit Summary

5.4 OPERATIONS SUPPORT

The Contractor shall support the ongoing IT operations for the COTS image sharing software and related applications hosted in the VAEC and integrated with systems deployed at VHA facilities. The Contractor shall comply with all applicable VA Change Management procedures, directives, and best practices throughout the project lifecycle.

5.4.1 VAEC SOLUTION SUPPORT

The Contractor shall maintain applications and services in the VAEC required to support the CIE project. All VAEC instances, deployed solutions or software, or other CIE systems supported by the Contractor shall be documented in a Component System Inventory Spreadsheet. As detailed in the VAEC Implementation Plan, the Contractor shall execute load testing to produce system Capacity Baseline and Performance Baseline reports.

The Contractor shall perform application-level patching or recommended configuration changes as needed to address security vulnerabilities, application bugfixes, software version updates, or enhancements.

Deliverables:

A. Component System Inventory Spreadsheet
B. Capacity Baseline Report
C. Performance Baseline Report

5.4.2 SOLUTION AVAILABILITY MONITORING AND REPORTING

The Contractor shall provide continuous uptime monitoring support of VAEC resources. The Contractor shall support the Enterprise Monitoring team by allowing access and/or implementing changes required for external monitoring.

Solution system monitoring shall utilize full end-to-end testing to accurately represent the system availability and directly related services and have the information available in a CIE Monitoring Dashboard. The Contractor shall notify VHA customers, project or related operations staff, and VA enterprise monitoring within 30 minutes of relevant system and component outages that impact the use of community image sharing services.

The Contractor shall provide a Monthly Usage Report for each COTS image sharing solution interfaced with discrete reporting for the following:

- DICOM Images/Exams shared by VA to community providers per site and imaging specialty
- DICOM Images/Exams shared by community providers to VA per site and imaging specialty
- Clinical and/or diagnostic reports shared by VA to community providers, per site, per format/method, and imaging specialty
- Clinical and/or diagnostic reports shared by community providers to VA, per site, per format/method, and imaging specialty

To verify the CIE solution(s) have adequate capacity to meet performance expectations, the Contractor will utilize the Performance and Capacity baselines developed during the original solution deployment. The Contractor shall compare the current production load and performance experienced by VHA users the baselines and provide the results in a Monthly Performance and Load Report.

Deliverables:

A. CIE Monitoring Dashboard
B. Monthly Usage Report
C. Monthly Performance and Load Report

5.4.3 HELP DESK SUPPORT

After each CIE solution is deployed, the Contractor shall provide problem and defect management support and coordination. This will include Tier 2/3 IT support of systems or technologies directly managed by the project during Weekdays from the hours of 8:00AM – 5:00PM of the time zone applicable to the selected VISN. The Contractor shall respond in accordance with the table below:

Response Times for Tier 2/3

Severity Code	Tier 2 initial response to customer	Tier 2 escalates to Tier 3 for initial contact	Tier 3 response to Tier 2
1 – Critical	15 minutes	0-15 minutes	15 minutes
2 – Serious	1 hour	30 minutes	1 hour
3 – Moderate	4 hours	1 hour	4 hours

The Contractor shall utilize the Service Now (SNOW) help desk software or VA's preferred IT incident management product to intake and track reported problems with the CIE solutions. The Contractor shall create relevant Help Desk Knowledge Base Articles for Tier 0/1 support staff. For related partner systems and technologies supported by other parties, the Contractor shall provide triage support and direct support requests to the appropriate OI&T, VHA, or external entity.

Tiers 0-3 are defined as:

- Tier 0 (Username and password problems, User Box Configuration, low level instructions on how to use the applications) – Handled by OIT Enterprise Service Desk (ESD)
- Tier 1 (Application Error Messages) – Handled by ESD
- Tier 2 (Report generation, Production Research, Database Updates, Batch job support) – Handled by Contractor
- Tier 3 (Changes to application code or configuration) – Application defects, etc. – Handled by Contractor

The Contractor shall report all ongoing and completed support requests in a Monthly Help Desk Report. Outside of the standard SNOW metrics, this report shall also include the number of support requests referred to external partners and its relevant status.

Problems resulting from a defect within the Contractor's provided or managed solution will be remediated with a configuration change or deployed with a software patch, as appropriate. If the problem requires long-term resolution, it will be placed in the product backlog. Defects may be identified by the Government Product Manager, users, Help Desk, or Business/Product Owners. For each defect identified, the Contractor shall deliver a Defect Resolution Plan. It shall include the Product team's (including the Contractor) triage of the defect in accordance with the table below and a plan for resolution, including timeline and impacts to the code and updates to Jira, GitHub, or other VA approved tools. Following the VA's approval of the Contractor Defect Resolution Plan, the Contractor shall execute the approved plan.

Deliverables:

A. Help Desk Knowledge Base Articles
B. Monthly Help Desk Report
C. Defect Resolution Plan

5.4.4 TRAINING MATERIALS

The Contractor shall provide a Training Plan for the design and functionality of the training modules to include storyboards. The Contractor shall provide End User and Application Administrator PowerPoint-based training documents to support the deployment of the CIE solution. Upon approval by the VA, training documentation shall be integrated into existing VistA application training documentation where applicable.

The Contractor shall present draft Training Plans and storyboards to the Business Owner for review, and feedback shall be incorporated as directed. The training documentation shall meet Section 508 certification criteria. The final Training documentation shall be stored in the VistA Documentation Library.

Deliverables:

A. Training Plan
B. End User Training Document
C. Application Administrator Training Document

5.4.5 EHR TRANSITION SUPPORT

The VHA enterprise is in the process of migrating to Cerner EHR solutions. While the CIE solutions will integrate VistA EHR sites not migrating to Cerner in the near future, offboarding an existing VHA site or VISN to Cerner, including Cerner's preferred community image sharing solutions may be required over the project lifecycle. If a site or VISN is converting to the Cerner EHR which has already integrated with CIE, the Contractor shall support the transition of that site/VISN to the Cerner EHR solution. The Contractor shall make all VAEC hosted solution reconfigurations needed, provide integrated system inventory, and support the customer with their VHA hosted system reconfiguration to ensure a successful transition to the Cerner EHR.

5.5 VISTA DEVELOPMENT

5.5.1 AGILE DEVELOPMENT

The Contractor shall create, maintain, analyze, and report Solution Roadmaps and Agile Release Train Schedules in the VA-approved toolset. The Contractor shall provide schedule updates within the VA-approved toolset on a weekly basis.

Schedule support shall include management of related associated patches to mitigate collisions in addition to tracking the product solution. Project schedule shall be planned/coordinated to ensure optimized sequencing of releases and/or deployments to avoid collisions.

The Contractor shall configure, develop, enhance, maintain, test, and deploy software modules for the VistA Image DICOM Importer III and VistA Image Clinical Display application on a continuous basis no shorter than two weeks but no longer than three months in duration. The Contractor shall provide deliverable packages/artifacts specified herein that meet documentation and delivery requirements of activities specified in the CIE Backlog and are VIP/VA PARS/EPMO compliant. The Contractor shall leverage and reuse relevant content and pre-existing product documentation as appropriate to satisfy the content of package deliverables.

The Contractor shall utilize DevSecOps principles and SAFe practices in partnership with VA to continuously improve the CIE performance and customer satisfaction. The Contractor shall show all Agile requirements, changes, tests performed, and test results in the VA-approved toolset to show evidence of code coverage and test coverage of all the requirements specified. This will allow VA to have high confidence in a fully documented requirements traceability matrix.

The Contractor shall utilize Human Centered Design (HCD) principles as part of all product development and operations efforts. While engaging in the following HCD activities, the Contractor shall:

- Follow the United States Digital Service value: “Design with users, not for them.”
- Provide expert guidance on user experience design direction and strategy.
- Create and maintain documentation for all activities, recommendations, and decisions.

At the start of work on each build, the Contractor shall conduct a product development kickoff meeting with the IPT and designated stakeholders to establish desired outcomes.

Deliverables:

A. Solution Roadmaps
B. Agile Release Train Schedules

5.5.2 IOC

The Contractor shall support a 10-day error free IOC in the production account. After any defect correction during IOC, IOC shall continue with the updated Software Source Code for a minimum of five business days error free before exiting IOC.

The Contractor shall support IOC evaluation activities to ensure IOC Entry and Exit criteria are met and deliver an IOC Entry and Exit Summary. The Contractor shall support installation and configuration at VA test sites, and support identification and development of remediation plans for defects as required.

Deliverable:

A. IOC Entry Request and Exit summary

5.5.3 DEFECT RESOLUTION

The Contractor shall be responsible for resolving defects resulting from changes made as part of base or exercised optional software development tasks within this PWS. Covered defects include items that were not identified or could not be resolved during the development or testing periods. The Contractor shall also address any defects resulting from incomplete software design or requirements gathering.

The Contractor shall resolve and track all defects and document the findings in the Software Defect/Fix Status Report, as well as address all issues and questions identified during IOC. For each defect identified, the Contractor shall log the defect, identify a resolution for the defect, and provide a Software Defect Resolution Plan, including timeline and impacts to the schedule, software code, and documentation. Following VA approval of the plan, the Contractor shall execute the approved plan.

At the completion of each defect correction, the Contractor shall make delivery of any Updates to Software Source Code, Compiled Code, and Supporting Documentation, coordinate the installation of the software update into the test site production accounts, and deliver updated documentation.

The Contractor shall resolve identified software defects within the timeframes in the following tables:

Performance Standards for T3 Incident and Defect Remediation Processing by Incident Defect Priority

Activity	Critical	High	Medium, Low, and Unclassifiable	Maintenance Phase
Incident Referral to Assignment	Assigned Date	Assigned Date	Assigned Date	Null
Temporary Workaround (*see emergency footnote below)	Next Business Day	Next Business Day	Next Business Day	1.Triage
Problem Assessment (Incident Analysis - Traceability, Analysis, Classification & Processing, Reproduce Problem, Code Evaluation & Review)	Same Day plus < 3 Hrs	Same Day plus < 4 Hrs	1 Day	
Propose Solution and Create stub	1 Day, 4 Hrs	12 Days	16 Days	
Obtain Committed Test Site(s)	2 Days	20 Days	26 Days	2.Core Work
Register Release	7 Days	27 Days	36 Days	

Activity	Critical	High	Medium, Low, and Unclassifiable	Maintenance Phase
Problem Remediation (Repair, Internal Testing, Attach Build to Patch Stub, SQA Review)	10 Days	36 Days	47 Days	
MOU Approval. May occur any time after Core Work begins.				3. Test Site Obtained
Occurs when Core Work is complete.				4. Core Work Exit
Conduct IOC	36 Days	79 Days	111 Days	5. IOC Testing
Approval to proceed to release (Submit IOC Findings, integration of findings, release readiness reports, etc.)	43 Days	97 Days	130 Days	6. Release Approval
End State – successful package release or determination that no patch is required				7. Remediation Complete

- Based on 12 hours workdays.
- Days shown are Calendar Days unless otherwise noted.
- Non-Emergency incident are measured against normal working hours.
- Emergency Workarounds will be addressed same day and immediately upon incident assignment to T3 (in cases where T2 passes the workaround)
- Activities are to start on the day shown
- The final Activity – Approval to proceed to release – begins and ends on the same day.

Defects that pose a security risk are held to a higher performance standard, as specified in the table below. This standard is measured from the time of detection of the defect.

Performance Standards for T3 Ticket and Security Defect Remediation Processing by Ticket Defect Priority (calendar days)

Standard Performance Measures	Critical	High	Medium	Low
Time to incident Acknowledgement/Entry	Immediately upon defect Identification	Immediately upon defect Identification	<1/2 day	<1/2 day
Time to Analyze / Determine Resolution	<1 day	<2 day	2 day	3 day
Time to Resolve - Repair (ready for test site)	<5 day	<10 day	<20 day	<45 day /as otherwise agreed
Time to Resolve - Repair (to include deployment)	As Soon As Possible	30 day	45 day	Not to exceed 120 day /as otherwise agreed

Deliverables:

A. Software Defect/Fix Status Report
B. Software Defect Resolution Plan
C. Updates to Software Source Code, Compiled Code, and Supporting Documentation

5.6 ADDITIONAL VISTA DEVELOPMENT (OPTIONAL TASK #1)

If exercised, the Contractor shall provide additional VistA Software Module Development in accordance with PWS 5.5 for one application per exercise (may be exercised for up to 12 months per application during each PoP of the TO). The VistA applications are:

- VistA Radiology/Nuclear Medicine Package
- VistA Imaging DICOM Gateway/Hybrid DICOM Image Gateway (HDOG)
- VistA Imaging Image eXchange Service (VIX), Central VistA Imaging eXchange (CVIX), and the VIX Image Viewer.

The specific application shall be identified upon each exercise of the optional task. The PoP shall be up to a maximum of 12 months per exercise, not to exceed the completion date of the performance period it is exercised within.

5.7 CERNER EHR INTEGRATION (OPTIONAL TASK #2)

Upon execution of this optional task, the Contractor shall perform Sections 5.1-5.4 for the integration of an ImageX solution into the VA implementation of Cerner EHR and the Care Aware MultiMedia (CAMM) products. This solution will be made available for VHA Cerner converted VISNs for onboarding. This optional task may be exercised at any time during the base or option periods up to a total of four (4) times.

Cerner EHR Integration Requirements

Functional Requirements
Business Objective: VA performed imaging exams shall be efficiently exported from the electronic medical record to community providers caring for VA patients.
The solution shall allow the users to: • export DICOM image-based exams from Cerner EHR/CAMM to community providers utilizing the COTS image sharing product • optionally export reports and relevant clinical findings for imaging exams from the Cerner EHR to community providers utilizing the COTS image sharing product • export radiology reports or consult based clinical results as DICOM Structured Reporting Diagnostic Reports • export radiology reports or consult based clinical results as non-image Portable Document Format (PDF) files with discrete text • export radiology reports or consult based clinical results as DICOM Encapsulated PDF files
Business Objective: Community acquired imaging exams shall be efficiently stored to the electronic medical record, consistent with imaging exams performed at VA.

Functional Requirements
The solution shall allow the user to: • import a DICOM image-based exam from a community provider to the Cerner CAMM product and associate it with a Cerner EHR clinical encounter • enter the external report and impression text to the associated Cerner radiology exam, if the report is available in text form • interpret DICOM Structured Reporting (SR) diagnostic reports and allow the user to store the report text to the Cerner clinical encounter associated with the DICOM images • if discrete selectable text is available, the solution shall read radiology exam reports within a PDF formatted file and allow the user to store the report text to the Cerner clinical encounter associated with the DICOM images • read radiology exam reports within a DICOM encapsulated PDF and allow the user to store the report text to the Cerner clinical encounter associated with the DICOM images

5.8 CIE SOLUTION FOR ADDITIONAL VISNS (OPTIONAL TASK #3)

If exercised, the Contractor shall provide the technical support needed to integrate additional VISNs not selected in the base tasks. This optional task may be exercised at any time during the base or option periods for one (1) additional VISNs, up to a maximum of 7 additional VISNs during the base and option periods. The CIE IPT will determine the priority and specific COTS image sharing products to integrate at the additional VISNs.

Deliverables:

A. Updated deliverables from Sections 5.1-5.4

5.9 NEW CIE SOLUTION FOR ADDITIONAL VISNS (OPTIONAL TASK #4)

If exercised, the Contractor shall perform 5.1-5.4 for an alternate COTS image sharing solution (Nuance Powershare or Vaultara Flight). This optional task may be exercised up to a maximum of three (3) times during the base and option periods.

Deliverables:

A. Updated deliverables from Sections 5.1-5.4

5.10 OPTION PERIODS

If Option Periods One (1) through Four (4) are exercised by the Government, all the tasks and deliverables in Section 5.1 through 5.5 shall apply.

6.0 GENERAL REQUIREMENTS

6.1 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 5. Incorporates “ease of use” Human Centered Design principles in any software developed.	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate to perform tasks required 2. Personnel possess necessary knowledge, skills, and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

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

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.

The following Section 508 Requirements supersede Addendum A, Section A3 from the T4NG Basic PWS.

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 Services and Documentation Requirements

6.2.1 COMPATIBILITY 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.

6.2.2 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 delivery.

6.3 SHIPMENT OF HARDWARE OR EQUIPMENT

Not Applicable.

6.4 ENTERPRISE AND IT FRAMEWORK

The required Assurance Levels, in reference to the Federal Identity, Credential, and Access Management (FICAM) requirements set forth in Section 3.8.2 of the T4NG Basic PWS, are Identity Assurance Level (IAL) 3, Authenticator Assurance Level (AAL) 3, and Federation Assurance Level (FAL) 3 for this specific TO.

6.5 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

Not Applicable.

6.6 ORGANIZATIONAL CONFLICT OF INTEREST

Not Applicable.

APPENDIX A

CONTRACTOR NON-DISCLOSURE AGREEMENT

This Agreement refers to Contract/Order _____ entered into between the Department of Veterans Affairs and _____ (Contractor).

As an officer of *<fill in name of Contractor>*, authorized to bind the company, I understand that in connection with our participation in the *<fill in program>* acquisition under the subject Contract/Order, Contractor's employees may acquire or have access to procurement sensitive or source selection information relating to any aspect of *<fill in program>* acquisition. Company *<fill in name>* hereby agrees that it will obtain Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements from any and all employees who will be tasked to perform work under the subject Contract/Order prior to their assignment to that Contract/Order. The Company shall provide a copy of each signed agreement to the Contracting Officer. Company *<fill in name>* acknowledges that the Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements require Contractor's employee(s) to promptly notify Company management in the event that the employee releases any of the information covered by that agreement and/or whether during the course of their participation, the employee, his or her spouse, minor children or any member of the employee's immediate family/household has/or acquires any holdings or interest whatsoever in any other private organization (e.g., contractors, offerors, their subcontractors, joint venture partners, or team members), identified to the employee during the course of the employee's participation, which may have an interest in the matter the Company is supporting pursuant to the above stated Contract/Order. The Company agrees to educate its employees in regard to their conflict of interest responsibilities.

Company ***<fill in name>*** further agrees that it will notify the Contracting Officer within 24 hours, or the next working day, whichever is later, of any employee violation. The notification will identify the business organization or other entity, or individual person, to whom the information in question was divulged and the content of that information. Company ***<fill in name>*** agrees, in the event of such notification, that, unless authorized otherwise by the Contracting Officer, it will immediately withdraw that employee from further participation in the acquisition until the Organizational Conflict of Interest issue is resolved.

This agreement shall be interpreted under and in conformance with the laws of the United States.

_____
_____
Signature and Date Company

_____
_____
Printed Name Phone Number

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 Directive 1605.05, *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 10 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 two (2) 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 two (2) 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 VA Information Security Rules of Behavior, 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 2.0 # VA 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.