PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Enterprise Cloud Solutions Office

VA Enterprise Cloud
Veterans Health Information Systems
Technology Architecture
Adaptive Maintenance

VA Enterprise Cloud Security

Task Order PWS Version Number: 1.8
Date: 12/24/18

Contents

1.0 BACKGROUND

The Veterans Health Information Systems Technology Architecture (*VISTA*) is the comprehensive, integrated, nationwide, longitudinal Veteran health information system of the U.S. Department of Veterans Affairs (VA). For the past thirty-five years, 130 *VISTA* systems have provided all clinical, financial, and administrative functions to support the operations of the 1250 VA healthcare facilities throughout the United States. During these three decades of continuous operation, *VISTA* has evolved to become highly specific to the needs of Veteran care, benefits, business processes, government compliance, and reporting. *VISTA* therefore remains one of VA's most essential systems requiring adaptive maintenance to ensure seamless continuity of Veteran care and services as VA progresses with its information technology modernization program.

VA currently operates its *VISTA* systems within legacy, custom-built, government-run data centers. More than half of VA's *VISTA* systems (over 70) are hosted at the Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) in St Louis. In compliance with Federal mandates to consolidate government data centers, DISA announced that it will be closing the St. Louis Defense Enterprise Computing Center by early 2020. VA is therefore required to migrate all these *VISTA* systems, in compliance with the U.S. Cloud-First directive, to the VA's Enterprise Cloud (VAEC).

To modernize the management of Veteran health data and secure it as is migrated and operationalized in the VA Enterprise Cloud, the VA Office of Information and Technology, as the technology agent for the Veterans Health Administration, requires professional services to comprehensively audit, secure, and monitor VISTA's enterprise interface. This is essential to modernize and upgrade the security for veterans data management using modern state-of-the-art commercially-supported cloud-native solutions, and to provide comprehensive, real-time 24/7 monitoring, surveillance, and security for all Veteran data as it is modernized and migrated to the VA Enterprise Cloud.

VISTA's enterprise-wide remote access interface - the remote procedure call (RPC) interface – connects all end-user clients (CPRS, JLV, CAPRI, and 45 others) running on all 380,000 Windows desktop computers across VA to all 130 VA VISTA transactional database systems, and supports all of the 50+ million transactions of the 150,000 clinical end-users of the VISTA database each day.

VHA requires professional services to comprehensively audit, analyze, and secure the complete VISTA RPC interface. The RPC interface is currently comprised of over 5,500 distinct Massachusetts General Hospital Utility Multi-Programming System (MUMPS) code modules. To audit the interface, the definitions of all these RPC modules must be translated into a single modern, maintainable, machine-processable industry standard model. This RPC model will then be configured and operationalized within the VAEC's commercial monitoring tool (Amazon Web Services CloudWatch) to provide comprehensive, real-time 24/7 surveillance, monitoring, and security for all Veteran data for all *VISTA* systems migrated to the VAEC. VHA requires completion and production deployment to secure all 70 *VISTA* systems migrating to the VAEC starting in Calendar Year 2019.

The VA Enterprise Cloud VISTA Adaptive Maintenance (VAM) project accelerates and enables VA Modernization by (1) modernization of the management of veteran health data, taking full advantage of the features, scaling, and security of VA's new commercial cloud capabilities, (2) resolving the severe and outstanding security vulnerabilities of all remote data access for all *VISTA* systems, (3) reducing the cost and complexity of maintenance of all *VISTA* systems (4) ensuring the safe, secure, and seamless continuity of veteran care and services as the veterans health information is migrated to modern cloud-based commercial platforms and (5) providing a roadmap and method for retirement of VISTA functionality using a cloud-based enterprise-wide approach (rather than a one VISTA at a time) enabling a more reliable and rapid VA health record modernization.

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. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010
2. VA Directive 6066, "Protected Health Information (PHI) And Business Associate Agreements Management", September 2, 2014

3.0 SCOPE OF WORK

The Contractor shall complete the audit, analysis, and translation of the entire *VISTA* RPC interface into a modern machine-processable form, to be operationalized and scaled for production enterprise use on the VAEC AWS CloudWatch monitoring tool in order to provide a comprehensive cloud-based *VISTA* RPC Interface monitoring and security for all *VISTA* systems migrated to the VAEC.

The Contractor shall support Project Management, Software Design and Development, System Testing, Cybersecurity Testing and Remediation, Performance & Regression Testing, System and Software Documentation, Risk and Defect Management, Release and Deployment, and support Authority to Operate (ATO), and A&A assessment.

3.1 APPLICABILITY

This TO effort PWS is within the following T4NG Basic PWS scope of paragraphs

4.1.6 Program Management Support
4.2.1 Design and Development
4.2.4 Enterprise Application/Services
4.2.9 System/Software Integration

4.2.12 Engineering and Technical Documentation
4.4 Test & Evaluation (T&E)
4.8 Operations and Maintenance (O&M)
4.9.1 Information Assurance (IA)

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 12 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 OR SPECIAL REQUIREMENTS

The Government anticipates travel to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips and anticipated locations in support of the program related meetings for this effort is shown below.

1. Washington, DC or other VA location as appropriate - two trips with two contractors traveling per trip for 3 – 4 days per trip.

4.4 CONTRACT MANAGEMENT

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; 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. 10 developer-grade laptops
2. 0 desktops.

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

All requirements in Section 6.0 of the PWS apply to this effort. Specific 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 30 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 30 days.

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	□	☒	□
5.2	□	☒	□
5.3	□	☒	□
5.4	□	☒	□
5.5	□	☒	□
5.6	□	☒	□

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

Project management shall be according to the VA Integration Process (VIP).

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 this TO effort. 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 TO. The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP.

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.

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word. These reports shall reflect data as of the last day of the preceding calendar month. The Monthly Progress Reports 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 the plan and timeframe for resolving the issue.

Deliverable:

A. Monthly Progress Report

5.1.3 PROJECT MANAGEMENT TOOLS

Contractors shall use the Project Repository as defined in the Data Rights (Section 7) of this Task Order for all project management tasks, including storage, tracking, and version control of all documents, reports, issues, and artifacts. Contractor is encouraged to leverage the best available industry-standard extensions available for the Project Repository to facilitate project management tasks, tracking, and documentation automation. Should project management artifacts contain confidential or sensitive information, these will be stored and protected per guidance in the Data Rights section. The Contractor may use additional tools if available and approved in the VA Enterprise Cloud with approval of the Project Manager and/or Business Owner.

The Contractor shall use Project Management Tools to:

1. Input and manage project/product test plans, test cases/scripts, and results
2. Deliver code, configurations, documentation in the Project Repository as defined in the data rights section of this task order.

The Contractor and VA PM shall determine which team members require access to the Project Repository.

5.1.4 PRIVACY & HIPAA TRAINING

The Contractor shall submit TMS VA Privacy and Information Security Awareness and Rules of Behavior Training Certificates and Health Insurance Portability and Accountability Act (HIPAA) Certificate of Completion, and 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”.

Deliverables:

A. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate
B. Signed Contractor Rules of Behavior
C. VA HIPAA Certificate of Completion

5.1.5 ONBOARDING STATUS

The Contractor shall be responsible for executing and managing the Contractor requirements in the Contractors Onboarding/Off-Boarding (CONB) process. The Contractor shall submit a weekly Onboarding Status Report of all onboarding activities for all staff supporting this project until such time as all team members are on board. After all team members are on board, reporting shall be on an as-needed basis only.

The onboarding process shall include VA Privacy and Information Security Awareness training, Rules of Behavior, finger prints, background investigation submission and status, Rational Access Requests, VISTA account request, Personal Identity Verification (PIV) card, Active Directory account, Remote Access Request, Elevated Privileges Request per environment, VA Tools training, and any other information deemed necessary for tracking by the Contractor, VA PM and COR.

At the conclusion of this TO, the Contractor shall be responsible for executing and managing the Contactor requirements for off-boarding in the CONB process.

Deliverable:

A. Onboarding Status Report

5.1.6 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five (5) calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three (3) calendar days after the meeting). The Contractor shall invite the VA Contracting Officer, COR, PM, VAEC Director, and VHA Architect/Business Owner. It is desirable that key Contractor team members join the meeting in person.

5.2 ADAPTIVE MAINTENANCE SERVICES

The Contractor shall provide *VISTA* adaptive maintenance by providing enhanced Veteran data security via comprehensive *VISTA* RPC content audit and monitoring so that all VAEC-deployed *VISTA* systems are adequately secured. The Contractor shall:

1. Complete the analysis of the MUMPS code for the remainder of the 5500 RPC interfaces and perform modeling to identify, for each RPC:
    a. Types, categories, and volumes of data it accesses (e.g., does the RPC affect pharmacy, laboratory or other clinical applications only or does it affect all/most *VISTA* applications?),
    b. Actions it performs (e.g., does it perform read only functions or does it also allow write access to the patient record?),
    c. Sensitivity of the data it handles (e.g., is the data Protected Health Information (PHI) or is it non-PHI?), and
    d. End-users, applications, and clients accessing the system (e.g., is it a legitimate end user, or a rogue client/intruder?).
2. Provide and document the comprehensive audit of the complete *VISTA* RPC Interface (all 5,500 MUMPS RPC calls), and translation of this MUMPS code into a machine-processable form that is implementable within the VAEC-resident CloudWatch tool. Deliver a MUMPS RPC to JSON model data definition that represents the outcome of the audit and MUMPS to JSON model translation.
3. Provide a quarterly Version Description Document (VDD) which details the progress to completion of the complete audit and model translation for all 5,500 *VISTA* RPCs.
4. Scale the interface monitor for production deployment.
5. Provide an Automated CloudWatch Configuration which automates the capture, storage, monitoring and audit of all RPC traffic in the VAEC-resident CloudWatch COTS tool on a continuous and fully automated basis.
6. Pull RPC traffic from CloudWatch, and based on comprehensive audit, automatically classify and quantify RPC traffic to:
    a. Identify all clients accessing *VISTA* data via the RPC interface.
    b. Identify all users accessing *VISTA* data via the RPC interface
    c. Identify and audit all types, volumes and categories of data being accessed via the RPC interface, with an indication of sensitivity

7. Configure CloudWatch to generate real-time alerts and alarms based on identified vulnerability and sensitivity conditions of RPC traffic. Demonstrate the success of the Automated CloudWatch Configuration operational performance by providing a fully automated validation of the completeness and correctness of the RPC interface audit.
8. Produce a Security Vulnerability Report including:
    - Number and type of clients accessing Veteran data.
    - Number and type of users accessing Veteran data.
    - Volumes and types of data being accessed, and an indication of sensitivity of data accessed.

Deliverables:

A. Comprehensive RPC Interface Audit Report
B. MUMPS RPC to JSON Model Data Definition
C. Version Description Document (VDD)
D. Automated CloudWatch Configuration
E. Security Vulnerability Report

5.3 TESTING

The Contractor shall develop and deliver a Master Test Plan to indicate the methods and tools by which it will perform all testing. The Master Test Plan shall indicate the methods by which VA's expected results will be achieved, associate deliverable artifacts to tests to be performed, and how test results will be validated by the Government.

The Contractor shall provide an RPC Interface Test Suite that provides a fully automated validation of the completeness and correctness of the RPC interface audit. It shall validate completeness (based upon number and % coverage of RPCs audited) and correctness (based upon all RPC attributes, types, users, clients, and sensitivity represented in the audit). This test suite shall be run on a continuous basis (at minimum weekly) to track and assure quality and completeness of RPC interface audit. Ultimately, contractor testing must demonstrate that 100% of *VISTA* RPCs (all 5500) and their attributes are completely and correctly audited. Audit and testing results must be in machine-processable form, so as to properly configure automated monitoring by the CloudWatch tool.

The Contractor-provided RPC Interface Test Suite shall also provide a capability to validate and quantify all RPC volumes and coverage to generate the necessary data for resource planning, optimization, and scaling of the RPC Interface monitoring for all VAEC-hosted *VISTA* systems as required in Section 5.6 (Release and Deployment Support).

Deliverable:

A. Master Test Plan

B. RPC Interface Test Suite

5.4 ASSESSMENT AND AUTHORIZATION (A&A) SUPPORT

The Contractor shall provide support, applicable documentation, and coordinate with VA VAEC data center partners to ensure consistency with VA ATO requirements for certification. This is to ensure the PWS 5.2 component deliveries meet VA information security policies and standards for successful completion of the A&A process.

The VAEC is a fully VA-approved, U.S. FedRAMP, FISMA-HIGH GovCloud certified environment. This project is fully hosted within and inherits all the security controls of VAEC. Should any further documentation regarding security of VAEC-based systems be required, this will be determined and governed by the VAEC security policy, controls, and technical subject matter experts (SME).

In support of the continuity of the VAEC ATO and as determined by the VAEC technical SMEs, the Contractor shall update the VAEC A&A artifacts quarterly with any particulars to this project. VAEC A&A artifacts include:

1. System Security Plan
2. Security Configuration Plan
3. Information System Contingency Plan
4. Incident Response Plan
5. Privacy Impact Assessment
6. Risk Assessment
7. Security Configuration Checklist (SCC)
8. System Interconnection Agreements (MOU and Interconnection)
9. Interconnection Security Agreement
10. Signatory Authority

5.5 INITIAL OPERATING CAPABILITY (IOC) SUPPORT

The Contractor shall perform IOC testing for a period of one month in the VAEC environment against the complete RPC traffic of an unmodified production *VISTA* in the VAEC environment.

The Contractor shall identify security anomalies leveraging the CloudWatch tool (with appropriate triggers and logic configured) indicating all conditions, reasons, severity, and sensitivity of RPC traffic and content. The Contractor shall update the Security Vulnerability Report provided in PWS 5.2 with each release.

Following IOC, the Contractor's update to the Security Vulnerability Report shall include at least one month of full RPC traffic monitoring of at least one VAEC-based production *VISTA*. This report shall be provided to the VA Office of Information Security (OIS) and VAEC leadership.

The Contractor shall develop and finalize the Production Operations Manual (POM), which shall include regular maintenance and operations information, Responsibility, Accountability, Consulted, and Informed (RACI) information, process flowcharts, dataflow diagrams, key monitoring indicators, and troubleshooting information.

The Contractor shall develop the Deployment and Installation Guide which includes back-out and rollback procedures.

The Contractor shall develop a User Manual which addresses procedural information for the business users on daily operational use of the CloudWatch monitoring software.

The Contractor shall provide all required documentation and receive approval for ATO as specified in the Enterprise Program Management Office (EPMO) Website. Upon successful completion of IOC, the Contractor shall notify the VA PM to approve the IOC release for further scalability testing and implementation.

Deliverables:

A. Production Operations Manual
B. Deployment and Installation Guide
C. User Manual

5.6 RELEASE AND DEPLOYMENT SUPPORT

The Contractor shall provide release and deployment assessment services and optimization to scale the IOC solution for future, enterprise-wide deployment for all *VISTA* systems in VAEC.

The Contractor shall produce a Capacity, Performance and Scalability Assessment for National Deployment of the *VISTA* Adaptive Maintenance (VAM) VAEC security and monitoring solution for all VAEC-hosted *VISTA* systems. This assessment shall include the required VAEC infrastructure growth necessary to scale the VAM-VAEC IOC deployment solution for nationwide deployment. This assessment shall encompass:

(a) scaling the VAM security solution from monitoring a single VAEC-based *VISTA* to a solution monitoring all VAEC-based *VISTA* systems. The fully scaled VAM solution shall provide sufficient capacity for auditing and monitoring all RPC traffic of all *VISTA* systems in VAEC, including at a minimum the 70+ *VISTA* systems migrated from the St. Louis DISA DECC, and

(b) testing and performance-tuning the VAM solution design against an increased volume of RPC traffic that indicates optimized utilization of VAEC resources to a government-defined response time for deployment across all 70+ *VISTA* systems hosted in VAEC.

The Contractor shall perform capacity and performance tuning using VAEC-specific tools. The Contractor shall specify VAEC resources required for network, storage, server processing and memory, etc. The Contractor's assessment shall position VA to deploy the fully scaled VAM VAEC security solution across all (at minimum 70) *VISTA* systems in VAEC at a future time.

Deliverable:

A. Capacity, Performance, and Scalability Assessment for National Deployment

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. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Quick response capability 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 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 TO 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 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 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

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

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology. These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards. The Contractor shall comply with the technical standards as marked:

☐ § 1194.21 Software applications and operating systems
☐ § 1194.22 Web-based intranet and internet information and applications
☐ § 1194.23 Telecommunications products
☐ § 1194.24 Video and multimedia products
☐ § 1194.25 Self-contained, closed products
☐ § 1194.26 Desktop and portable computers
☒ § 1194.31 Functional Performance Criteria
☒ § 1194.41 Information, Documentation, and Support

7.0 RIGHTS IN DATA AND COMPUTER SOFTWARE

7.1 DATA RIGHTS

The Government retains full and unlimited rights to all artifacts (code, documents, materials) produced under this contract. All artifacts are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government.

7.2 PROJECT REPOSITORY

To facilitate the centralized management, reporting, collaboration, and continuity of access of all artifacts and deliverables produced under this contract, all artifacts and deliverables shall be developed, version-controlled, stored, and delivered on a single industry-standard public GitHub repository (“Project Repository”) with clearly designated and appropriate industry-standard licenses and formats. Upon commencement of the contract period, the contractor shall establish the Project Repository, and provide a publicly accessible URL of the Project Repository to the project manager, contracting representative, and relevant government stakeholders.

The Project Repository shall be the complete, authoritative, inclusive, primary source of all artifacts developed under this contract, reflecting in real-time all contributions of all members of the development and management team. Designated developers and managers shall have full read-write (push-pull) privileges and share in real-time all development and management artifacts in progress in this collaborative environment. The government, all necessary stakeholders, and the public shall have contemporaneous read and download access of the same developer artifacts at all times throughout the lifecycle of the contract. All periodic management reports and/or technical artifact submissions to the government shall be derived from, and include the URL link, to the primary source artifacts in the Project Repository. By default, all artifacts of the Project Repository shall be hosted on a public GitHub repository.

Should a subset of content in the Project Repository contain proprietary, protected, or sensitive information or content, contractor may use a private repository for only this subset of content. A private repository shall be created and maintained as (a) either a private repository within the primary public Project Repository, or (b) within a repository managed within the private government network on Github Enterprise.

Should redaction of any code or data be required for any reason (security, privacy, or otherwise) this must be fully documented, fully automated, and nondestructive. A fully functional equivalent of any code or data must be provided as a replacement to maintain full functionality of all code and deliverables as specified. Source code shall be annotated inline to clearly indicate (a) the start and end points of any sections planned for redaction, (b) explanation for redaction (c) substitute code/data to replace reacted code/data with its functional equivalent (d) redaction-replacement scripts based on inline annotation of the source code/data and substitute code/data (e) verification scripts to demonstrate software remains fully functional as originally intended, after redaction-replacement operation. The contractor shall provide the redaction-replacement scripts, and all replacement data/code on the Project Repository along with the source code they are associated with. Redaction-replacement scripts shall be run on a regular basis (at minimum once per week) such that the private (unredacted), public (redacted), and published list of all redactions are complete, consistent, and up-to-date at all times. To minimize such issues of redaction, developers shall modularize and isolate code from data definitions (such as network addresses) as much as possible via easily-replaceable configuration files.

All repositories, whether private and public, shall be maintained consistent and up-to-date by fully automated means. Independent of whether segments of the Project Repository are hosted on separate public and private repositories, the Project Repository shall be managed and considered as a single, inclusive logical unit spanning all repositories and artifacts. The government and authorized stakeholders shall have full access to all repositories, private and public, original and redacted-replaced, and an index of all artifacts and code, private and public, redacted-replaced, that correctly and comprehensively describes all artifacts.

All artifacts in the Project Repository shall have the following properties and data rights:

1. All data and metadata produced under this contract must be provided in nonproprietary industry-standard machine-processable, structured form on the Project Repository and carry an AGPL version 3 (or later) license. All data must include its corresponding, complete, correct, current operational metadata (schemes, models, data dictionaries) in machine-processable form, such that fully automated machine interpretation, extraction, translation, loading, and migration of all data to any future data storage system may be accomplished by a third party using industry-standard tools without any loss of information content or context. If the data is tabular, CSV is required; for all other data structures JSON is required. For metadata JSON-LD is required.

2. All code (software) produced under this contract shall be developed, version-controlled, and delivered in source code form with associated documentation in the Project Repository, such that real-time, contemporaneous third-party review and validation of all code in progress is possible. (i) The contractor shall clearly identify all source code as either original or derivative. All code that constitutes original works shall carry an AGPLv3 license. All code that constitutes derivative works must carry a compatible Open Source Initiative (OSI) approved free and open source license. (ii) All source code, dependent code, libraries, or third-party code shall be in portable, industry-standard languages. If the source code requires compiling or assembling, these shall be either industry-standard open-source compilers or assemblers, or shall be provided with the software under an OSI-approved license. (iii) All code must have corresponding documentation, version-controlled in markdown in the same repository as the source code, and contain at minimum an Installation Guide and a User Guide for the final delivered source code such that a third party may download, install and make full functional use of the delivered code as specified and intended. The Installation Guide must list all required third-party code, libraries or other dependencies.

3. All documentation and reports produced under this contract must be created, updated, and managed as text files in machine-processable industry-standard markdown, be under continuous version control on the Project Repository, and carry an AGPLv3 license. All documentation and artifacts must be fully accessible and readable without any special tools using only a web browser. The authoritative and most up-to-date version of all documentation is the markdown source on the Project Repository. Should a static snapshot of the documentation be required for offline use at any time (such as Word or PDF format), contractor shall use a fully automated documentation generator to produce static snapshots from the markdown source. All edits, updates, and amendments to any documentation must be through changing the markdown source - not by editing the generated static documents - and then regenerating the static document. All generated static documentation must have clearly printed date-of-generation on each page to identify the date of the snapshot. Approved markdown formats include GitHub Markdown and Docbook.

ADDENDUM A - VA INFORMATION AND INFORMATION SYSTEM SECURITY / PRIVACY LANGUAGE

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

B.1 GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B.2 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 Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor’s employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B.3 VA INFORMATION CUSTODIAL LANGUAGE

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

b. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor’s information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA’s information is returned to 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.

c. 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 Contracting Officer within 30 days of termination of the contract.

d. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. 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.

f. 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.

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

h. 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.

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

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA’s prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. 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.

B.4 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

N/A

B.5 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

N/A

B.6 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.

B.7 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.

B.8 SECURITY CONTROLS COMPLIANCE TESTING

N/A

B.9 TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior, updated version located at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848, relating to access to VA information and information systems;

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

3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

b. The Contractor shall provide to the contracting officer 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.

CONTRACTOR EMPLOYEE
PERSONAL FINANCIAL INTEREST/PROTECTION OF SENSITIVE INFORMATION AGREEMENT

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

As an employee of the aforementioned Contractor, I understand that in connection with my involvement in the support of the above-referenced Contract/Order, I may receive or have access to certain "sensitive information" relating to said Contract/Order, and/or may be called upon to perform services which could have a potential impact on the financial interests of other companies, businesses or corporate entities. I hereby agree that I will not discuss or otherwise disclose (except as may be legally or contractually required) any such "sensitive information" maintained by the Department of Veterans Affairs or by others on behalf of the Department of Veterans Affairs, to any person, including personnel in my own organization, not authorized to receive such information.

"Sensitive information" includes:

(a) Information provided to the Contractor or the Government that would be competitively useful on current or future related procurements; or

(b) Is considered source selection information or bid and proposal information as defined in FAR 2.101, and FAR 3.104-4; or

(c) Contains (1) information about a Contractor's pricing, rates, costs, schedule, or contract performance; or (2) the Government's analysis of that information; or

(d) Program information relating to current or estimated budgets, schedules or other financial information relating to the program office; or

(e) Is properly marked as source selection information or any similar markings.

Should "sensitive information" be provided to me under this Contract/Order, I agree not to discuss or disclose such information with/to any individual not authorized to receive such information. If there is any uncertainty as to whether the disclosed information comprises "sensitive information", I will request my employer to request a determination in writing from the Department of Veterans Affairs Contracting Officer as to the need to protect this information from disclosure.

I will promptly notify my employer if, during my participation in the subject Contract/Order, I am assigned any duties that could affect the interests of a company, business or corporate entity in which either I, my spouse or minor children, or any member of my immediate family/household has a personal financial interest. "Financial interest" is defined as compensation for employment in the form of wages, salaries, commissions, professional fees, or fees for business referrals, or any financial investments in the business in the form of direct stocks or bond ownership, or partnership interest (excluding non-directed retirement or other mutual fund investments). In the event that, at a later date, I acquire actual knowledge of such an interest or my employer becomes involved in proposing for a solicitation resulting from the work under this Contract/Order, as either an offeror, an advisor to an offeror, or as a Subcontractor to an offeror, I will promptly notify my employer. I understand this may disqualify me from any further involvement with this Contract/Order, as agreed upon between the Department of Veterans Affairs and my company.

Among the possible consequences, I understand that violation of any of the above conditions/requirements may result in my immediate disqualification or termination from working on this Contract/Order pending legal and contractual review.

I further understand and agree that all Confidential, Proprietary and/or Sensitive Information shall be retained, disseminated, released, and destroyed in accordance with the requirements of law and applicable Federal or Department of Veterans Affairs directives, regulations, instructions, policies and guidance.

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

I agree to the Terms of this Agreement and certify that I have read and understand the above Agreement. I further certify that the statements made herein are true and correct.

____
Signature and Date Company

____
Printed Name Phone Number