**TRANSFORMATION TWENTY-ONE TOTAL TECHNOLOGY
NEXT GENERATION (T4NG)
PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS**

**Office of Information & Technology
Enterprise Project Management Office (EPMO)**

VistA Adaptive Maintenance

Date: 8/09/17
TAC-17-42242
Task Order PWS Version Number: 3.1

Contents

1.0   BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Enterprise Project Management Office (EPMO) is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T 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.

The Veterans Information System Technology Architecture (VISTA) is the single, integrated, authoritative, comprehensive, longitudinal veteran health information system of the U.S. Department of Veterans Affairs (VA). For the past thirty-five years, 131 VISTA systems have provided all clinical, financial, and administrative functions to support all clinical and administrative operations of over 1200 VA hospitals and clinics throughout the United States. VISTA should therefore be considered the composite of an integrated electronic health record ("EHR"), and a federal health and resource management system including billing, scheduling, and enterprise resource management (collectively "ERP"). In addition, over three decades of continuous operation and refinement, VISTA has become highly specific to Veteran care, benefits, business processes, government compliance, and regulatory reporting.

VA leadership announced in June 2017 the decision to improve interoperability of the Veterans' health record with Department of Defense by migration to a common commercial EHR. The VISTA Adaptive Maintenance project is designed to support this transformation by identifying, isolating, and modifying the EHR components of VISTA ("EHR") to provide forwards compatibility for this future state, while at the same time providing seamless continuity of care and services (backwards compatibility with) the current clinical functionality of VISTA.

The clinical component of VISTA ("VISTA/EHR") is the Computerized Patient Care System (VISTA/CPRS). This VISTA Adaptive Maintenance thus entails isolating specific clinical components of VISTA/CPRS from the non-clinical ("VISTA/ERP": business, financial, scheduling, resource planning, reporting) and migrating these to a secured, centralized service that can be migrated easily to a centralized, commercial system. In order to support this mandate and transition, the VA Adaptive Maintenance project will:

1. Surface specific VISTA/CPRS clinical function and business logic, and emulate with an industry-standard, model-driven, secure service interface with no legacy Massachusetts General Hospital Utility Multi-Programming System (MUMPS) code dependencies while keeping CPRS operational (supporting both backwards and forwards compatibility).
2. Provide enhanced Veteran data security via (1) access control, (2) auditing, and (3) Remote Procedure Call (RPC) content encryption so that CPRS is adequately

secured well beyond the level currently available in VISTA, enabling seamless, secure migration.
3. Address any security vulnerabilities that do not meet the enhanced security requirements.
4. Provide a foundation to more easily migrate to a commercial cloud-based EHR solutions enterprise wide
5. Enhance ability to implement open-source Government Off The Shelf (GOTS), and Commercial Off The Shelf (COTS) applications enterprise wide within a cloud-based, commercial EHR environment.
6. Reduce need for site by site accommodations for enterprise wide releases of selected functionality
7. Reduce costs by reducing site specific technical support needs.

If this project is not implemented, migration of VISTA to support newer commercial offerings, and to provide required urgent security to veterans data, will be impeded. This will adversely impact Veterans' access to healthcare services, and congressional mandates for VA IT modernization will not be met in a timely manner.

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 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; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), 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 provide services including manage, plan, develop, design, integrate, test, and implement centralized services that provide the adaptive maintenance required for the selected VistA functional domains such that the result provides both backwards- and forwards-compatible centralized services compatible with both with VistA and new commercial products. The Contractor shall support Project Management, Application and Platform Architecture, Requirements Analysis, Build/Sprint Planning, Software Design and Development, System Engineering, Configuration Management, Unit Testing, Functional Testing, System Testing, Cybersecurity Testing and Remediation, Acceptance Testing, Performance & Regression Testing, System and Software Documentation, Risk and Defect Management, System and Performance Metrics Capture, Release and Deployment, and support Authority to Operate (ATO) assessment.

The Contractor shall follow an Agile Methodology and follow the Veteran focused Integration Process (VIP) established by OI&T EPMO. The Contractor shall comply with any applicable VA/VHA or other Government mandates, as necessary.

3.1   APPLICABILITY

This Task Order (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 from date of award, with one 12-month option period and one two-month optional task. The overall Task Order period of performance shall not exceed 26 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 in support of the program related meetings for this effort is four trips per period of performance (eight trips overall) with two contractors traveling per trip. Anticipated location includes the following, estimated at for four days in duration:

    1. Washington, DC

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

VA shall provide metadata from production clones for testing and Github repository.

4.6 SECURITY AND PRIVACY

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,

a. 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.

b. 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 based upon the requirements identified 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)

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	☐	☒	☐

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.4	☐	☒	☐
5.5	☐	☒	☐
5.6	☐	☒	☐
5.7	☐	☒	☐
5.8	☐	☒	☐

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

Agile project management is evolutionary (iterative & incremental) which regularly produces high quality results in a cost effective, timely, and highly collaborative manner via the Veteran Focused Integration Process (VIP) value driven lifecycle. This requires open lines of communication among all participants contributing to a project/program/portfolio that include multiple consumers within the contracts and with other VA offices/activities.

The foundational structure for VA agile development and project management can be found in the VIP Guide. For delivery of all project artifacts, the Contractor shall utilize Rational for managing project execution details and for the management and storage of artifacts using approved VIP and/or EPMO website templates.

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.

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. The report shall include detailed instructions and or 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 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. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables provided during the reporting period. 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. Monthly Progress Report

5.1.3 RATIONAL TOOLS USAGE

The Government will provide access to VA's IBM Rational Collaborative Application Lifecycle Management (CALM) Toolset (hereafter referred to as Rational) to provide a single agile project/product application lifecycle management toolset to track execution details. Contractors shall complete the training as required below in order to access VA's IBM Rational. If the mandated toolset changes throughout the period of performance of this contract, then the Government will provide access to the new toolset.

The Contractor shall use the VA's implementation of the Rational Toolset. The Rational Project/Product Data and Artifact Repository will be used to provide a single authoritative project and product data and artifact repository. All OI&T project data and artifacts will be required to be managed in this data and artifact repository daily. All checked out artifacts shall be checked back in daily and any data updated daily. Rational synchronizes all changed information immediately for all team members to access work proficiently without the concern of working on aged information.

The Contractor shall use VA Rational tools in accordance with the VA Rational Tools Guide to:

    1. Input and manage scheduled project/product sprints and backlog
    2. Input and manage project/product agile requirements
    3. Input and analysis project/product risks and issues

4. Input and manage project/product configurations and changes
5. Input and manage project/product test plans, test cases/scripts, and results
6. Input and manage project/product planning and engineering documentation
7. 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.

The Contractor shall record all agile requirements, changes, tests performed in VA provided environments, and test results (see master test plan) in Rational to show evidence of code coverage and test coverage of all the requirements specified. This expectation will allow VA to have high confidence in a fully documented Requirements Traceability Matrix (RTM), as evidenced by data recorded in the tools.

The Contractor and VA PM shall determine which team members require access to the Rational Tool Suite. All Contractors that require access shall complete all of the following VA Talent Management System (TMS) training courses before access can be granted to the Rationale tools:

1. TMS ID 3878248 - IBM Rational Team Concert - Agile Sprint, Configuration/Change Management Level 1
2. TMS ID 3878249 - IBM Rational Team Concert - Agile Sprint, Configuration /Change Management Level 2
3. TMS ID 3878250 - IBM Rational DOORS Next Generation - Requirements Management Level 1
4. TMS ID 3897036 - IBM Rational DOORS Next Generation - Requirements Management Level 2
5. TMS ID 3897034 - IBM Rational Quality Manager - Quality Management Level 1
6. TMS ID 3897035 - IBM Rational Quality Manager - Quality Management Level 2

Contractors who have completed these VA training courses within the past 24 months and have furnished Rational Training Certificates will not be required to re-take the training courses.

Deliverable:

A. Rational Training Certificates

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 in ProPath.

The Contractor shall submit a Weekly Onboarding Status Report of all onboarding activities for all staff supporting this effort. This 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 task order, the Contractor shall be responsible for executing and managing the Contactor requirements for off-boarding in the CONB process in ProPath.

Deliverable:

A. Weekly 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 calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM. It is desirable that key Contractor team members join the meeting in person (i.e. Scrum Master and project lead).

5.1.7 CONFIGURATION MANAGEMENT (CM)

The Contractor shall:

1. Identify the standard and unique aspects of Configuration Management (CM) to be performed that meets the project, EPMO and VIP requirements*.*
2. Identify types of configuration items pertaining to each product to be placed under configuration management.
3. Create and incorporate the CM Plan (CMP) into Rational and specify how all software source code and electronic artifact configuration and version

management will be managed. The COR and VA PM will approve the Configuration Management Plan.

4. Use VA PM approved tools to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes.
5. Ensure that all project software and non-software artifacts are versioned correctly and follow a build release promotion versioning approach which identifies all major, minor, and update changes to the components.
6. Create Project and Product Artifacts baselined and versioned in the CM repository in order to allow the tool to show active and past histories of the check-ins and check-outs of all software components, data, and software project engineering documents. Maintain all baselines of software, software builds, and electronic artifacts in the repository, labeling updates and versions according to CM procedures. Ensure all code is checked in with a frequency compliant with the approved CM Plan.
7. Establish and maintain status reporting on change and configuration management activity, and ensure data records and artifacts are filed and updated daily.
8. Ensure all off-boarding Contract staff has checked in all code, documents and other project artifacts.
9. Develop and manage a CM Process that supports all necessary changes for the project including changes to Definition of Done, Acceptance Criteria and any other items deemed necessary.
10. Use Rational Team Concert as the VA approved tool and repository for all software source code and electronic artifact configuration and version management. The Contractor shall use IBM Rational Team Concert tool to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes.
11. Develop, verify and submit with all project build deliveries, a Version Description Document (VDD) that conforms to EPMO Website standard templates and addresses the manifest of the contents of all software builds created for project releases outside the development environment.

Deliverables:

A. Configuration Management Plan
B. Version Description Document

5.2   ADAPTIVE MAINTENANCE SERVICES (BASE & OPTION PERIOD)

The Contractor shall provide adaptive sustainment services to enable VA to migrate VISTA off of its MUMPS infrastructure to provide backwards and forwards compatibility for VistA domains and use cases including Patient Data Entry and Pharmacy Computerized Physician Order Entry (CPOE), as described in PWS 5.2.1 and 5.2.2.

The Contractor shall:

1. Surface specific VISTA/CPRS clinical function and business logic, and emulate with an industry-standard, model-driven, secure service interface with no legacy MUMPS code dependencies, while keeping CPRS operational (supporting both backwards and forwards compatibility).
2. Provide enhanced Veteran data security via (1) access control, (2) auditing, and (3) RPC content encryption so that CPRS is adequately secured well beyond the level currently available in VISTA, enabling seamless, secure migration.
3. Address any security vulnerabilities that do not meet the enhanced security requirements.
4. Provide a foundation to more easily migrate to a commercial cloud-based EHR solutions enterprise wide.
5. Enhance ability to implement   open-source, GOTS, and COTS applications enterprise wide within a cloud-based, commercial EHR environment.

In order to adapt VistA to make it usable in a changed or changing environment, the Contractor shall provide operational analysis, system administration, adaptive maintenance, and end user support as indicated by the services and intended outcomes addressed by PWS 5.2.1 and 5.2.2.

5.2.1 ISOLATE CPRS FROM VISTA MUMPS FOR SELECT PATIENT DATA ENTRY FUNCTIONS (BASE PERIOD)

The Contractor shall migrate the functional domains of CPRS activity including Patient Vitals Data Entry, Patient Allergy Data Entry and Patient Problem Data Entry from VistA into distinct Veteran Integrated Care Services (VICS) as annotated by PWS 5.2.1.1 – 5.2.1.3. The Contractor's solution shall replace the CPRS Remote Procedure Call (RPC) interface and any dependent CPRS RPCs (such as the Virtual Patient Record (VPR) RPC) with a service emulation layer which provides compatibility with web-friendly interfaces for new clients. The Contractor's solution shall also address issues that arise with a centralized service including location, time management, and synchronization.

The Contractor shall identify all affected business processes functioning in RPCs for a Vitals, Allergy, and Problem VICS as the basis for designing and providing an adaptive maintenance solution for these VistA functions on an individual, unique basis. The Contractor shall provide all documentation associated with this lifecycle process consistent with PWS Sections 5.3 through 5.6.

After migration, CPRS shall continue to perform as before, but against single instances of centralized services, permitting the retirement of the equivalent function in the 131 VistA systems.

5.2.1.1 PATIENT VITALS DATA ENTRY VICS

Consistent with the guidance in PWS 5.2.1, the Contractor shall develop a VICS service layer that supports patient vitals entry and retrieval by CPRS and web-friendly interfacing by new clients. The Contractor shall reroute the service layer to a node.js-

supporting, industry-standard database. RPCs will be routed to the centralized service, while maintaining backwards compatibility with the FileMan Data Dictionary.

The Contractor shall deliver:

1. A node.js-based, Node Package Manager (NPM)-installable VICS service that supports all RPCs used by CPRS for Vitals entry and Retrieval and Equivalent representational State Transfer (REST)-based calls to enable new clients.
2. Regression Test Suite to cover all CPRS vital interactions.
3. Configuration of a VistA Test System (production clone) to validate interfaces to Vitals VICS.

5.2.1.2 PATIENT ALLERGY DATA ENTRY VICS

Consistent with the guidance in 5.2.1, the Contractor shall develop a VICS service layer that supports patient allergy entry and retrieval by CPRS and web-friendly interfacing by new clients. The Contractor shall reroute the service layer to a node.js-supporting, industry-standard database. RPCs will be routed to the centralized service, while maintaining backwards compatibility with the FileMan Data Dictionary.

The Contractor shall deliver:

1. A node.js-based, NPM-installable VICS and Reference Implementation that supports all RPCs used by CPRS for Allergy entry and retrieval and equivalent REST-based calls to enable new clients.
2. Regression Test Suite to cover all CPRS allergy interactions.
3. Configuration of a VistA test system to contrast and test against the Allergy VICS

5.2.1.3 PATIENT PROBLEM DATA ENTRY / RETRIEVAL

Consistent with the guidance in 5.2.1, the Contractor shall develop a VICS service layer that supports patient problem entry and retrieval by CPRS and web-friendly interfacing by new clients. The Contractor shall reroute the service layer to a node.js-supporting, industry-standard database. RPCs will be routed to the centralized service, while maintaining backwards compatibility with the FileMan Data Dictionary.

The Contractor shall deliver:

1. A node.js-based, NPM-installable VICS and Reference Implementation that supports all RPCs used by CPRS for Problem entry and retrieval and equivalent REST-based calls to enable new clients.
2. Regression Test Suite to cover all CPRS problem interactions.
3. Configuration of a VistA test system to contrast and test against the Problems VICS.

5.2.2 ISOLATE CPRS FROM VISTA MUMPS FOR OUTPATIENT PHARMACY CPOE (BASE PERIOD)

CPRS allows a Provider to order a variety of items and activities including medications, lab tests and consultations. Orders lead to activity both inside and outside a hospital, in

the pharmacy, labs and radiology departments. Typically, Outpatient Pharmacy represents one third of the orders of a VA Hospital.

Unlike Patient Data Entry, Computerized Physician Order Entry (CPOE) involves non-CPRS as well as CPRS users. For Outpatient Pharmacy, Providers use CPRS while Pharmacists use a legacy roll and scroll interface built into VistA. In addition, a third party service provides drug checking functionality.

The Contractor shall develop a VICS service for Outpatient Pharmacy to segregate CPOE for operation outside of VistA RPCs. The Contractor's solution shall replace CPRS's RPC interface with a service emulation layer and any dependent CPRS RPCs (such as the Virtual Patient Record (VPR) RPC), which provides compatibility with web-friendly interfaces for new clients. RPCs will be routed to the centralized service, while maintaining backwards compatibility with the FileMan Data Dictionary. Such a VICS will demonstrate that VistA's pharmacy can be replaced by third party solutions without affecting veteran care and the integrated veteran patient record now visible to VA providers and Pharmacists.

The Contractor shall:

1. Develop a node.js-based, NPM-installable Outpatient Pharmacy VICS for Outpatient Pharmacy that allows a CPRS Provider and typical VA Pharmacist to manage medication orders (Prescriptions)
2. Isolate and document VA-specific from general purpose functionality in VA Outpatient Pharmacy
3. Ensure CPRS works as now for VA providers managing outpatient medications
4. Demonstrate, via a web client, a capability that allows VA Pharmacists to manage outpatient medications and to illustrate Pharmacist interactions
5. Isolate the drug checking interface called from VistA to allow it to be used in the VICS service layer
6. Provide a Regression Test Suite that covers all CPRS-based Provider and Roll and scroll based Pharmacist interactions.
7. Deliver a VistA configured for Pharmacy for testing and contrasting the VICS-based Pharmacy service to the current VISTA Pharmacy.

5.3   SUSTAINMENT SUPPORT FOR THE PATIENT DATA ENTRY AND PHARMACY CPOE FUNCTIONS (BASE AND OPTION PERIOD)

The Contractor shall also perform lifecycle sustainment support for Patient Data Entry and Pharmacy CPOE functions, which include:

1. Corrective Sustainment, which is the diagnosis and correction of program errors after software release. The Contractor shall gain access to the VA Computer Associates Service Desk Manager (CA SDM) web page to log, track, update, and reference work ticket requests.

2. Preventive Sustainment, which is the modification of software to improve future maintainability or reliability as a result of a requirement to perform a hardware re-platform or operating system/system software upgrade.
3. Perfective Sustainment, which is the modification of the software to improve future functionality based on best practices recommended by VistA Subject Matter Experts, sustainment staff and business users. This shall include software patches, code optimization and incorporation of upgraded and effective software or plugins to improve performance and usability. The perfective sustainment scope shall be coordinated with relevant business and technical stakeholders and confirmed through a user acceptance test process.
4. Sustainment services shall include Contractor provision of Tier 2 and Tier 3 escalation support according to the Response Times indicated in Table 5.6.1. Tier 2 and 3 support shall include maintenance and repair of software bugs until software is transitioned to VA's IT/OPS (previously Service, Delivery and Engineering).

The Contractor shall document the resources, allocations, and activities to execute sustainment support in Rational.

The Contractor shall provide a Bi-Weekly (every two weeks) Sustainment Summary Report detailing the status and disposition of reported issues to include the status of the tickets in the National Service Desk tickets

Deliverable:

A. Bi-weekly Sustainment Summary Report

5.4   PLANNING (BASE & OPTION PERIOD)

The Contractor shall coordinate project planning with VA stakeholders, to include requirements assessment, design, development, and testing. The Contractor shall collect, draft, coordinate, enter, and update project planning data in the Rational tool.

The Contractor shall continuously support the build and development methodology described within Section 5.5 in order to complete the scope of RPC emulation requirements identified from the backlog.

The Contractor shall complete the Planning State subtasks described below.

5.4.1 AGILE REQUIREMENTS ELABORATION

The Contractor shall perform an assessment to quantify the number of RPCs containing Patient Data Entry functions and Pharmacy CPOE business logic. The Contractor shall perform backlog grooming sessions with the VA team to properly understand and elaborate business agile requirements. The outcome of these sessions shall be a review of, and agreement to, the quantity of RPCs containing Patient Data Entry functions and Pharmacy CPOE business logic and the percentage completion of RPC

emulation planned for each build.

The Contractor shall:

1. Ensure all RPC emulation requirements are identified, included, prioritized, and sized as appropriate within the overall product backlog grooming effort.
2. Coordinate with VA in populating and updating the product backlog during planning sessions, identifying all business logic the Government considers relevant to the RPC emulation.
3. Assign a Unit of measurement by which to quantify the relative complexity of RPC business logic to be emulated.
4. Facilitate any stakeholder briefings, meetings and backlog grooming sessions.
5. Execute requirements reviews with stakeholders and record results of reviews using Rational DOORS Next Generation, updating requirements data as a result of the reviews.
6. Identify the development and test environment access that is needed 30 days prior to development start.
7. Ensure all sources of requirements information (e.g., identification of RPCs containing Patient Data Entry functions and Pharmacy CPOE business logic) for functional and non-functional requirements are input and maintained in Rational. All requirements data is under change control and is fully linked to work items that show traceability to design changes, configurable items, test cases and test results.
8. Create and maintain the Requirements Traceability Matrix (RTM).

Any attributes that may be identified as new requirements (outside the scope of the work during the backlog grooming sessions) may not be incorporated into the Backlog without discussion with the COR for approval and submittal to the Contracting Officer for contract modification prior to any execution of effort. If the result of the backlog grooming session(s) determines that there are additional requirements that are out of scope of adaptive maintenance, the Contractor shall notify the Contracting Officer.

Deliverable:

A. RTM

5.4.2 BUILD PLANNING

The Contractor shall develop a Build Plan in Rational prior to the start of each build. Each build shall be up to three months in duration and shall be made up of two to four week sprints. The Contractor shall work with the VA PM and the VA Business Owner to review and determine the percent of RPC business logic that is to be emulated and that should become part of the build.

The Build Plan shall include:

1. The number of RPCs containing Patient Data Entry and Pharmacy CPOE business logic
2. Alignment of the RPC emulation work scope to a build and allocation of that scope to a percent (%) of RPC work completion planned for each build, indicating progress to 100% complete
3. Relationship Traceability
4. Performance Metrics
5. Acceptance Criteria
6. Identified Dependencies (internal and external)
7. Approved wireframes (if needed)
8. Functional Design
9. Technical Approach
10. Definition of Done

The Contractor shall perform backlog grooming and prioritization continually throughout the product life cycle and the aggregate period of performance of this task order. Based on the scope of work established in the backlog and VIP, development builds shall last three months or less. The Build Plan is the scope of work which will be completed in the agreed upon build timeframe. Each build ends with a new release candidate or push to production. The Contractor shall follow the standard development cycle as outlined below in PWS Sections 5.4 through 5.6 and all subparagraphs.

The Contractor shall develop the program/project Backlog and update it continuously for each build, in every release and throughout the life of the period of performance of this task order within Rational Team Concert.

All activity scheduled in each build and backlogs will be captured and have status showing percent (%) completion of work items in the build plan, and any changes, impediments, and retrospectives affecting the planned percent complete. All data and artifacts in Team Concert shall be fully linked to requirements data and test data.

Build planning activities shall consist, at minimum, of the following:

1. Conduct additional analysis to the extent necessary to identify and quantify RPCs with Patient Data Entry and Pharmacy CPOE business logic in order to develop a Build Plan and maintain the backlog. Teams will review, elaborate, and prioritize the backlog. This backlog grooming will occur continuously throughout the build to ensure the customer's highest priorities are being met.
2. Backlog grooming and Build Planning sessions, facilitated by the Contractor, that outline the intent of the build, are not a formal commitment. The Contractor shall update the resulting Build Plan within Rational Team Concert.
3. Identification of the RPC emulation work scope aligned to a build and allocation of that scope to a percent (%) of RPC work completion planned for each build, the agreement of acceptance criteria for each build.
4. Joint determination of the Definition of Done for the RPC emulation requirements within the build.

5. Identification of field sites (if needed), acceptance criteria, and ATO requirements.
6. Coordinate and validate Memorandum of Understandings (MOUs) and Service Level Agreements (SLAs) for partner dependencies that specifically highlight the commitment of partners to associated release.
7. Conduct backlog prioritization meetings with OI&T and VA Business representation with results updated into backlog.

Deliverable:

A. Build Plan
B. Backlog

5.5   BUILD AND DEVELOPMENT (BASE & OPTION PERIOD)

The Contractor shall provide build and development support services to include the following:

1. Application and Platform Architecture
2. Software Development
3. System Engineering
4. Configuration Management
5. Unit Testing
6. Functional Testing
7. System Testing
8. Cybersecurity Scanning, Remediation, and Report
9. Acceptance Testing
10. Performance Testing
11. System and Software Documentation
12. Defect Management
13. System and Performance Metrics Capture

The Contractor shall develop software agreed to in the Build Plan. Should the Contractor or the Government determine that the Acceptance Criteria, Feature Specifications or the Definition of Done requires updating during the Sprint cycles, all changes will be managed under a fully documented Change Control Process consistent with the Configuration Management Plan in PWS 5.1.7, and the Build Plan shall be updated.

The development of capabilities to support adaptive maintenance shall be consistent with the objectives set by PWS 5.2. For each agreed release, the Contractor shall perform software maintenance activities including program management, design, development, testing and lifecycle support tasks to produce associated deliverables and software ready for release into production environments.

The Contractor shall identify and develop Build and Development risks that might impact the success of the project, document those risks in the VA approved risk management tool, Build and Development Risk Log, and implement mitigation of identified risks utilizing appropriate strategies. The Contractor shall perform all Build and Development support using an agile methodology and approach, in accordance with any frameworks or architectures required by the VA.

Deliverable:

    A. Build and Development Risk Log

5.5.1 SOFTWARE DESIGN

The Contractor shall provide support in analyzing, documenting, and managing the architecture for the entire program and present a methodology for knowledge dissemination throughout each Scrum team to achieve program level execution adherence to the architecture. The Contractor, in conjunction with the VA OI&T PM and the VA Business Owner, shall examine the functionality, purpose, and integration of existing and planned architecture to determine and document the business, data, application and technology principles that will drive the system architecture and design. The Contractor shall develop application and platform architecture that is consistent with the architectural framework and methodologies established by Enterprise Architecture. The Contractor shall participate in the design of interfaces between platforms, systems, services and the databases the system will access and assist in the identification of needed processes and structures to ensure proper system performance.

High level technical approach shall be approved by VA OI&T PM prior to the deployment of the build. Any changes determined necessary during Build Planning shall be approved by VA OI&T at the conclusion of the Build Planning event prior to any actual development work commencing. The Contractor shall prepare a Technical Roadmap in Rational of modifications to architecture features needed to ensure a cohesive, integrated, reusable, stable, scalable, performant, secured product architecture.

The Contractor's Technical Roadmap shall ensure that the architecture features are sufficiently detailed to represent the development of detailed data and process models, screen and report designs, interface specifications and control specifications. The Contractor shall update the Build and Development Risk Log to reflect any inherent risks in the design affecting other VistA applications and develop mitigation plans to address them.

Deliverable:

    A. Technical Roadmap

5.5.2 SPRINT PLANNING

A build will consist of a series of sprints (typically 2-4 weeks' duration). Leveraging the accepted Build Plan, the Contractor shall perform Sprint Planning for the sprint(s) within the build and coordinate with the VA Business representatives throughout each sprint planning sequence. Once the Sprint Plan is approved by the Government, the Government will establish when the sprint is complete. All activity planned in each sprint shall be captured and have status showing all work items, changes, and impediments. All data and artifacts in Rational Team Concert shall be fully linked to requirements data and test data.

The Contractor shall:

1. Initiate and participate in a Sprint Planning Meeting, at the beginning of each sprint. The Contractor shall update the Sprint Plan in Rational Team Concert at the conclusion of the Sprint Planning.
2. Support, coordinate and provide input for the Sprint Acceptance Criteria in Rational Team Concert. The Sprint Acceptance Criteria shall be coordinated and approved for every sprint.

Deliverable:

A. Sprint Plan

5.5.3 SPRINT EXECUTION

All activity executed in each sprint shall be captured and have status showing all work items, changes, risks, issues, impediments, and retrospectives. All data and artifacts in Rational Team Concert shall be fully linked to requirements and test data. All project artifacts and source code will be under change and configuration management as specified by the COR using Rational.

The Contractor shall:

1. Provide a certified Scrum Master to provide the following functions including, but not limited to: facilitate all ceremonies, ensure Rational is updated daily, enforce scrum framework, track and assist with removing impediments, and facilitate integration across sprint teams.
2. Develop the features and capabilities as work items in Rational Team Concert that were established in the Sprint Plan.
3. Work with VHA business personnel to ensure the capability being developed in the sprint is meeting user needs by providing wireframes, story boards, user interface mock-ups, demonstrations, etc. during the sprint execution.
4. Complete sprint development including disciplined testing (unit, functional, regression) and reviews as a continuous process, to avoid finding issues at the end of sprint development.
5. Initiate and conduct daily scrums (typically 15 minutes) to show the team progress, impediments and daily plans.

6. Update Rational daily, to include progress on tasks during sprints, blockers and dependencies.
7. Conduct a Sprint Review to coordinate and support demonstration of the sprint activities with the project team and Users at the end of each sprint. The Sprint Review will result in Customer Acceptance of the Sprint.
8. Develop and deliver Source Code for every sprint. Build tools shall be in compliance with the approved list from the One-VA Technical Reference Model (TRM) and code shall be demonstrable and stable enough to be promoted to another environment without issue by evidence of the status of tests and results in the Rational Tools.
9. Initiate and facilitate a Sprint Retrospective meeting at the end of the Sprint to capture team performance lessons learned. The Contractor shall capture lessons learned in the Monthly Progress Report delivered in PWS 5.1.2.

Deliverable:

A. Source Code

5.5.4 SYSTEM ADMINISTRATION AND ENVIRONMENT SUPPORT

The Contractor shall provide system administration for all required environments (Dev/Pre-Prod/Prod), DevOps processes, Continuous Integration (CI) Processes and Tools, and Automated Build Tools and Scripts. The Contractor shall refer to the Master Test Plan, as per PWS 5.5.5.1, for identification of environment ownership and support needs.

The Contractor shall configure the individual development, integration, testing, preproduction and production environments. The Contractor shall establish and configure all of the environments required for the continuous integration pipeline including all phases of development, testing, integration, release and production. The Contractor shall define and configure these environments consistent with the Configuration Management Plan delivered in PWS 5.1.7 to ensure their availability. The Contractor shall secure the environment against disruption or infiltration by unknown and or unapproved third parties. The Contractor shall manage environment access for both Contractor and Government staff and perform appropriate audits every 90 days to ensure only authorized individuals have access to the environment(s). The Contractor shall indicate the results of this quarterly audit in the Monthly Progress Report delivered in PWS 5.1.2.

The Contractor shall follow the existing VA policies and procedures on system security and data privacy; keep the Program's existing documents on application security, system security, and data protection current; and support any security-related data calls or inquiries as directed by VIP Enterprise Program Management Office (EPMO) ProPath, and VA Information Security Office in responding to the future needs of information security. These changes are anticipated to occur approximately twice in each twelve month period of performance.

The Contractor shall provide continuous integration support to:

1. Provide continuous security monitoring for unauthorized activity (insider and outsider threats)
2. Configure environments based on VA security controls
3. Manage the configuration of the environments through automated scripts
4. Create, update and maintain an Environment Management Plan that includes the environment management approach and detailed environment diagrams
5. Create, update and maintain a Continuous Integration (CI) Master Plan that contains build, configuration and training materials for the CI environment, individual and central build environments and onboard developers and testers
6. Create Automation Build Scripts for local developer environments, integrate unit, functional and performance testing approach into CI pipeline using tests as a gating mechanism for environment promotions
7. Create Automation Build Scripts to central development, integration, testing, performance, pre-production and production environments into CI pipeline processes.

Deliverables:

A. CI Master Plan
B. Automation Build Scripts

5.5.5 TESTING

5.5.5.1 TEST APPROACH

The Contractor shall develop and deliver a Master Test Plan to indicate the methods and tools by which it will perform all testing, and to identify environment ownership and support needs. 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 specifically how test results will be validated by the Government. The Contractor shall perform testing throughout development and shall support Government acceptance testing via Initial Operating Capability (IOC) as referenced in PWS Section 5.5.

The Contractor shall provide all Post Development Test Scripts and create and update a Development Testing Report that includes a status of all testing and all relevant metrics.

The Contractor shall manage, track and remediate findings and defects from all associated tests. Any COR/PM directed vulnerability scans, remediation and reports shall be completed prior to the conduct of the PM/COR acceptance testing. The Contractor shall perform demonstrations to indicate that the new interfaces perform as designed in accordance with system requirements.

The Contractor shall perform:

1. Unit Testing
2. Functional Testing
3. Regression Testing
4. Component/System Testing
5. Performance Testing
6. Cybersecurity vulnerability scans and remediation

The Contractor shall support IOC in the Pre-Production and production environments. VA shall provide metadata from production clones for testing.

Deliverable:

A. Master Test Plan
B. Post Development Test Scripts
C. Development Testing Report

5.5.5.2 DEVELOPMENT TESTING

The Contractor shall adopt agile best practices for integrating testing into each agile development sprint and build. The Contractor shall populate the Master Test Plan in VA's implementation of Rational Quality Manager tool.   The Contractor shall conduct development tests (e.g. unit, functional, accessibility, system, reliability, usability, interoperability, regression, security, performance, and integration) throughout the development lifecycle (e.g. sprint, build, release) using industry best practices of continuous integration methods and automated regression testing utilities using One-VA (TRM approved tools. The Contractor shall conduct testing related to non-functional requirements (e.g. load, performance, installation, back-out, and rollback). The Contractor shall notify the VA at least three days prior to the start of system tests so that VA can observe the testing if desired.

The Contractor shall provide Master Test Plan data as developed in PWS 5.4.5.1 in the Rational Quality Manager following the templates and data requirements appropriate for each test purpose appropriate to each phase of development. The Contractor shall provide test results in the Rational Quality Manager which is the final piece of data that completes the RTM. COR and VA PM acceptance will occur through the Rational Quality Manager approval process.

The Contractor shall conduct or assist the Government in conducting the security scans, accessibility reviews, performance tests, technical standards review, architectural compliance assessments, user acceptance reviews and initial operational capability tests, audits, and reviews. Security scanning is done by multiple methods and is done multiple times throughout the course of a project with methods such as infiltration testing (Web Application Scan (WASA)), code analysis tools (Fortify), etc. Accessibility reviews are performed through a variety of tool based and manual reviews, able to scan web applications and other technologies used for user interfaces.

Performance testing is done through load testing and technical analysis of capacity planning data submitted by the project team. Architectural compliance assessments are done through submission of design materials to confirm compliance with allowed enterprise architecture.

The Contractor shall ensure all tests, compliance review planning, execution details and their testing and compliance results are entered and maintained in Rational Quality Manager and under version control in Rational Team Concert. Specifically, Test Management Data and Artifacts include such items as cases/scripts, configurations, utilities, tools, plans and results. The Contractor shall ensure that results of all assessments of the project performed by the Contractor or by VA offices are consolidated into Rational for planning and status reporting.

When a defect is identified during testing, the Contractor shall log it in Rational to establish a Defect Listing, selecting the appropriate severity level. The Contractor shall support the Project Manager in prioritizing the defect in the sprint backlog by participating in the Defect Management Board (DMB). Based on prioritization the defect could be entered into the current sprint or entered into the backlog.

The Contractor shall ensure Rational data is up-to-date on a daily basis so that VA stakeholders can access accurate and timely status.

Deliverables:

A. Test Management Data and Artifacts
B. Defect Listing

5.5.6 ASSESSMENT AND AUTHORIZATION (A&A) SUPPORT

The Contractor shall provide support, applicable documentation, and coordinate with data center partners to ensure consistency with VA ATO requirements for certification to ensure the project meets VA information security policies and standards to facilitate the successful completion of the A&A process and enable VistA to maintain its ATO.

The Contractor shall:

1. Support Field Security Services (FSS) Information Security Officers (ISOs) and Office of Cyber Security (OCS) Security Control Assessment (SCA) team for VistA assessment requirements as detailed in VA Directive and Handbook 6500 Information Security Program, VA Handbook 6500.3 Certification and Accreditation of VA Information Systems.
2. Conduct cybersecurity software code quality testing and validation of all VistA software code and provide Certified Scan Reports validating the required code quality.
3. Conduct and participate in vulnerability scans and tests or VistA best practice quality checks or reviews as detailed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 3 Recommended

Security Controls for Federal Information Systems and Organizations, if/when requested by the COR.

4. Security scanning shall be performed by multiple methods and is done multiple times throughout the course of a project with methods such as infiltration testing (WASA), code analysis tools (Fortify), etc.
5. Remediate critical and high vulnerabilities identified in Government scans or quality checks or reviews.
6. Provide Vulnerability Scanning Reports and Assessments as detailed in NIST SP 800-30 Rev 1 Guide for Conducting Risk Assessments.
7. Support VistA by identifying, documenting, reviewing, and maintaining 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 any aspect (e.g. documentation, code, etc.) of the development based on comments from the A&A review process conducted.
8. Provide continued security Plan of Actions and Milestones (POAM) support. Any COR/PM directed VistA vulnerability scans, remediation and reports shall be completed prior to the conduct of the PM/COR acceptance testing / IOC demonstration, in accordance with PWS Section 5.5.

A&A Artifacts include the following:

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

Deliverables:

A. Certified Scan Report
B. Vulnerability Scanning Reports and Assessments
C. A&A Artifacts

5.6   IOC SUPPORT (BASE AND OPTION PERIOD)

Following Contractor component integration/system testing (CI/ST), the Contractor shall support IOC Testing. The IOC shall be conducted at one or more test sites using formal

Government acceptance test policies and procedures as defined in ProPath and the Master Test Plan.

The Contractor shall provide and execute an Implementation Plan, planning for contingencies during the IOC release of software and supporting all aspects of software deployment within the development/test platform and pre-production platform. This shall include installing new product builds in development/test platforms, providing new product builds and tracking installation into pre-production and production platforms for IOC testing purposes.

The Contractor shall support IOC entry efforts to include patch notification messages and patch installation tracking. The Contractor shall resolve, track and respond to all defects, as well as address all issues and questions identified during the IOC evaluation, to include security defect resolution. This may require the Contractor to provide revised software code, repeat testing, and respond to IOC testing until IOC is successfully completed. For each defect identified, the Contractor shall log the defect by establishing an IOC Defect Log. When a defect is identified during testing, the Contractor shall log it in Rational, selecting the appropriate severity level. The Contractor shall support the Project Manager in prioritizing the defect in the sprint backlog by participating in the DMB. Based on a prioritization the defect could be entered into the current sprint or entered into the backlog. The Contractor shall identify a resolution for the defect, and provide a Defect Resolution Plan, including timeline and impacts to the schedule, software code and documentation. The IOC Defect Tracking Spreadsheet shall include: Defect identification, Identification Date, Defect Reporter, Test Phase found in, Status, Severity and Priority, what subsequent build it will be fixed in, and assignee for fixing. The Contractor shall use the IOC Defect Tracking Spreadsheet to facilitate the weekly DMB for adjudication and concurrence from all DMB members. Following Government review of the identified defects and COR concurrence of the Defect Resolution Plan; the Contractor shall execute the approved plan. At the completion of each defect correction (or each group of defects), the Contractor shall make delivery of any updates to Software Source Code, coordinate the installation of the software update into the test site production accounts, and deliver updated documentation as identified in below paragraph. After any defect correction in IOC, the updated Software Source Code shall remain in the production account for an additional five days error free.

The Contractor shall prepare/update as appropriate, the following documentation upon successful completion of IOC Testing:

1. Initial Operating Entry Request and Exit Summary.
2. IOC Defect Tracking Spreadsheet
3. IOC Defect Log
4. IOC Evaluation Summary
5. IOC Execution Log
6. Defect Status Report.
7. Package/Patch Completion Transition Document.

8. Lessons Learned Report.
9. National Release Checklist.
10. Operational Ready Review Checklist.
11. Updated and finalized Software Code Package, to include the software code, materials, installation guide, technical manuals, release notes, security guide, user guide, and release notes for each enhancement.

In addition, the Contractor shall develop and deliver a Deployment Plan upon completion of IOC.

Deliverables:

A. Implementation Plan
B. Defect Resolution Plan
C. IOC Defect Tracking Spreadsheet
D. IOC Operating Entry Request and Exit Summary
E. IOC Defect Log
F. IOC Evaluation Summary
G. IOC Execution Log
H. Defect Status Report
I. Package/Patch Completion Transition Document
J. Lessons Learned Report
K. National Release Checklist
L. Operational Ready Review Checklist
M. Deployment Plan
N. Software Code Package

5.7   RELEASE AND DEPLOYMENT SUPPORT (OPTION PERIOD)

The Contractor shall provide all services required to support deployment of the VistA domains and use cases of Patient Data Entry and Pharmacy Computerized Physician Order Entry (CPOE) products for installation into a VA-provided, FedRAMP approved, industry-standard, commercial cloud-based production environment. The Contractor shall collaborate with, problem solve, trouble shoot, and provide technical support to affected VistA project, Software Quality Assurance (SQA) and release managers.

POLARIS calendaring process and tool (or equivalent) will be used to track software installations, hardware replacements, system upgrades, patch release and implementation, special works in progress, and other deployment events in the VA production environment. The Contractor shall provide data for populating and updating the POLARIS calendaring process for each release and deployment. The Contractor shall provide data and information to support ATO approval as specified in the EPMO Website.

In accordance with the VIP Guide, Release and Deployment support begins upon successful completion of National Deployment for the first release and ends after the warranty period of the final release.

The Contractor shall update the Production Operations Manual (POM). The POM shall be updated, as applicable, to include updates to regular maintenance and operations information, Responsibility, Accountability, Consulted, and Informed information, process flowcharts, dataflow diagrams, key monitoring indicators, and troubleshooting information.

The Contractor shall develop the Deployment, Installation, Back-out, Rollback Plan.

The Contractor shall update the User Manual, if applicable, should the adaptive maintenance impact the end users' approach to use of the software.

The Contractor shall hold test site calls with VA staff to include Release Coordinators and VIP Release Agents once the product is approved for IOC production testing.

Deliverable:

A. Deployment, Installation, Back-Out, Rollback Plan

5.7.1 POST-DEPLOYMENT WARRANTY SUPPORT

For a period of 90 days after the final National Deployment release is completed the Contractor shall warrant all requirements and deliverables in the scope of this contract. Defects may be identified by the Government and its designees, to include all necessary personnel as designated by the COR. For each defect identified, the Contractor shall triage the defect, identify a resolution for the defect, and provide a Post-Deployment Warranty Support Defect Resolution Plan for resolution, including timeline and impacts to the code and updates to Rational.

RESPONSE TIMES FOR TIER 2 AND TIER 3 (Business Hours)

Severity Code	Tier 2 Initial Response to Customer	Tier 2 escalates to Tier 3 for initial contact	Tier 3 response to Tier 2	Tier 2 requests updates from Tier 3 based on SLA resolution	Resolution Time based on SLA from time incident initially reported
1 – Critical	1 hour	2 hours	4 hours	On call until issue resolved or hourly status check	0-4 hours
2 – Serious	2 hours	4 hours	8 hours	On call until issue resolved or hourly status	4-8 hours

Severity Code	Tier 2 Initial Response to Customer	Tier 2 escalates to Tier 3 for initial contact	Tier 3 response to Tier 2	Tier 2 requests updates from Tier 3 based on SLA resolution	Resolution Time based on SLA from time incident initially reported
				check	
3 – Moderate	4 hours	8 hours	24 hours	Daily	4-24 hours

Following COR approval of the Contractor Post-Deployment Warranty Support Defect Resolution Plan, the Contractor shall execute the approved plan.

Deliverable:

  A. Post-Deployment Warranty Support Defect Resolution Plan

5.8   TRANSITION SUPPORT (OPTIONAL TASK 1)

If exercised, this optional task shall be completed no later than 60 days from date of exercise.

If the Optional Task is exercised by VA, the Contractor shall develop, document and monitor the execution of a Transition Plan that may be used to transition tasks and materials to a new Contractor, or to the Government. The Contractor shall provide a plan for 60 days of outgoing transition support upon the approval of the Transition Plan for transitioning work from the current task order to a follow-on task order or Government entity. This transition may be to a Government entity, to another Contractor or to the incumbent Contractor under a new task order. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this contract to the succeeding entity. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This Transition Plan shall include, but is not limited to:

  1. Coordination with Government representatives.
  2. Review, evaluation and transition of current support services.
  3. Transition of historic data.
  4. Transition of Rational accounts.
  5. Transfer of hardware and software warranties, maintenance agreements and licenses.
  6. Transfer of all necessary business and/or technical documentation.

7. Orientation phase and program to introduce Government and Contractor personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes.
8. Disposition of Contractor purchased Government owned assets,
9. Transfer of GFE and Government Furnished Information, and GFE inventory management assistance.
10. Turn-in of all Government keys, Identification/access cards, and security codes.

Deliverable:

A. Transition Plan

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 INFORMATIN TECHNOLOGY (EIT) STANDARDS

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 (EIT). 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 and http://www.section508.gov/content/learn/standards. A printed copy of the standards will be supplied upon request. 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

6.2.1 EQUIVALENT FACILITATION

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

6.2.2 COMPATIBILITY WITH ASSISTIVE TECHNOLOGY

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

6.2.3 ORGANIZATIONAL CONFLICT OF INTEREST

Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

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

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

7.0   APPENDIX B – 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   SOURCE REPOSITORY

To facilitate the management, reporting, collaboration, standardization, and continuity of access of all artifacts and deliverables produced under this contract as a single logical unit, all artifacts and deliverables shall be developed, version-controlled, stored, and delivered on a single industry-standard public Github repository ("Source Repository") with clearly designated and appropriate industry-standard licenses and formats. Upon commencement of the contract period, the contractor shall establish the Source Repository, and provide a publically accessible URL of the Source Repository to the project manager, contracting representative, and relevant government stakeholders. The Source Repository shall be the complete, authoritative, inclusive, primary source of all technical artifacts developed under this contract, reflecting in real-time all contributions of all members of the development team. Developers shall have full read-write (push-pull) privileges and share in real-time all development 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 Source Repository. By default all artifacts of the Source Repository shall be hosted on a public Github repository.

Should a subset of content in the Source Repository contain proprietary, protected, or sensitive information or content, then 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 Source Repository, or
   (b) within a secondary repository managed behind a government firewall on Github Enterprise.

All repositories, whether private and public, shall be maintained consistent and up-to-date by fully automated means.

Contractor shall maintain an always-up-to-date list of any redacted artifacts, with associated documentation on the public Source Repository such that the scope and nature of all redactions are known at all times to the government and stakeholders. Any redaction must be fully documented and fully automated. Source code shall be clearly annotated inline to indicate any section planned for redaction, and the redaction scripts based on this annotation. The contractor shall provide the redaction and indexing script on the Source Repository. These shall be run on at minimum a weekly basis such that the private (unredacted), public (redacted), and published documentation of all

redactions are complete, consistent, and up-to-date at all times. In all cases, government and authorized stakeholders shall have full access to all repositories, private and public, and an index of all content, private and public, that correctly lists and documents all contractually developed artifacts.

For purposes of this contract, independent of whether segments of the Source Repository are hosted on separate public and private repositories, the Source Repository shall be managed and considered as a single, inclusive logical unit comprehensively spanning all repositories and artifacts, and shall be considered Government Furnished Equipment (GFE) in perpetuity to eliminate any ambiguity surrounding ownership of said content.

The artifacts in the Source 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 Source Repository and carry a Creative Commons CC0 license. All data must include its corresponding, complete, correct, current operational metadata (schemes, 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-LD 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 Source Repository, such that real-time, contemporaneous third-party review and validation of all code in progress is possible. The contractor shall clearly identify all source code as either original or derivative. All code that constitutes original works shall carry an Apache 2.0 license. All code that constitutes derivative works must carry an Open Source Initiative (OSI) approved free and open source license.

   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.

   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 provided as machine-processable industry-standard markdown in version-controlled text files on the Source Repository and carry a Creative Commons CCO license. From the most recent version of the markdown source, contractor shall use a documentation generator to produce all documentation in required formats. At minimum contractor shall auto-

generate HTML, Word, and PDF versions of all documentation from the markdown source. All edits, updates, and amendments to any documentation must be through changing the markdown source (not by editing the generated files), and then the documentation shall be regenerated in all required formats. All generated documentation shall reflect the most recent version of the markdown source. Approved markdown formats include Github Markdown and Docbook.