|  |
| --- |
| VeteransAffairs-Seal.JPG |

**PERFORMANCE WORK STATEMENT (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**

**Office of Information & Technology**

**Product Development**

**Open Source Technical Support and Working Group Services for VA VistA**

**Date: July 27, 2015**

**TAC-15-25343**

**PWS Version Number: 1.8**

Contents

[1.0 BACKGROUND 2](#_Toc425768116)

[2.0 APPLICABLE DOCUMENTS 4](#_Toc425768117)

[3.0 SCOPE OF WORK 6](#_Toc425768118)

[4.0 PERFORMANCE DETAILS 7](#_Toc425768119)

[4.1 PERFORMANCE PERIOD 7](#_Toc425768120)

[4.2 PLACE OF PERFORMANCE 7](#_Toc425768121)

[4.3 TRAVEL 7](#_Toc425768122)

[5.0 SPECIFIC TASKS AND DELIVERABLES 8](#_Toc425768123)

[5.1 PROJECT MANAGEMENT (BASE AND OPTION PERIODS) 8](#_Toc425768124)

[5.1.1 TECHNICAL KICK OFF MEETING 8](#_Toc425768125)

[5.1.2 CONTRACTOR PROJECT MANAGEMENT PLAN 8](#_Toc425768126)

[5.1.3 MONTHLY PROGRESS REPORTING REQUIREMENTS 9](#_Toc425768127)

[5.1.4 QUARTERLY REVIEW MEETINGS 10](#_Toc425768128)

[5.1.5 PRIVACY TRAINING 10](#_Toc425768129)

[5.2 TECHNICAL SUPPORT SERVICES for VA VistA (BASE AND OPTION PERIODS) 11](#_Toc425768130)

[5.2.1 ASSESS OPEN SOURCE PRODUCT CANDIDATES FOR VA VISTA INTAKE 11](#_Toc425768131)

[5.2.2 CERTIFICATION TESTING 13](#_Toc425768132)

[5.3 TECHNICAL WORKING GROUP SERVICES (BASE AND OPTION PERIODS) 15](#_Toc425768133)

[5.3.1 VA TECHNICAL WORKING GROUP (TWG) CHARTER DEVELOPMENT AND TWG FACILITATION 15](#_Toc425768134)

[5.3.2 EHR ORIENTATION AND VISUALIZATION MODELS 16](#_Toc425768135)

[5.4 TRANSITION SUPPORT (OPTIONAL TASK) 16](#_Toc425768136)

[6.0 GENERAL REQUIREMENTS 17](#_Toc425768137)

[6.1 ENTERPRISE AND IT FRAMEWORK 17](#_Toc425768138)

[6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 19](#_Toc425768139)

[6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 19](#_Toc425768140)

[6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 20](#_Toc425768141)

[6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 22](#_Toc425768142)

[6.4 PERFORMANCE METRICS 22](#_Toc425768143)

[6.5 FACILITY/RESOURCE PROVISIONS 23](#_Toc425768144)

[6.6 GOVERNMENT FURNISHED PROPERTY 24](#_Toc425768145)

[ADDENDUM A 24](#_Toc425768146)

[ADDENDUM B 29](#_Toc425768147)

# BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T) 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.

VA OI&T is responsible for the development and maintenance of the Veterans Health Information Systems and Technology Architecture (VistA), VA’s Electronic Health Record (EHR). VistA is built from more than 100 discrete applications that together comprise our highly integrated and fully- automated health information system. VistA is the electronic information service that enables clinical care delivery at 152 VA Medical Centers (VAMCs) and 928 ambulatory care and community-based outpatient clinics worldwide. VistA is central to the quality of care that VA delivers to Veterans.

Designed by clinicians for clinicians, VistA is patient-centric and embodies the clinical workflow processes that support VA’s models of care. It has enabled measurable improvements in the quality of care we provide. VistA is stable and reliable; it is available 99.95% of the time and performs well in both large hospital and small office settings. VistA’s capabilities evolved within VA over the many years it has been in use, and are the result of the contributions of many innovations, including most that came from within VA itself. However, today’s health care environment – in which new models of care are continuously developed and deployed, is utterly dependent upon the accelerating technological development of new medical devices, improved IT infrastructure, services, and wireless communications. In order to sensibly benefit from these advances, VA must address fundamental technical structural constraints that will inhibit its ability to keep pace with health services delivery and meet growing expectation of veterans for efficient service, including self-service. In addition, VA must continue to evolve VistA to meet changing clinical and regulatory requirements. The requirements of Public Law 113-066 (P.L. 113-066), SECTION 713 – “ELECTRONIC HEALTH RECORDS OF THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF VETERANS AFFAIRS,” of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2014 state that by December 31, 2016, VA must achieve an interoperable EHR with an integrated display of data with the Department of Defense (DoD) and private providers. The interoperable EHR must provide all relevant health care data of DoD and Veterans Affairs (VA), computable in near real time and comply with the national standards and architectural requirements identified by a jointly staffed and managed Interagency Program Office (IPO).

VA wishes to accelerate its rate of innovation for VistA so that it may be better integrated with private sector components, technology, and deliver outcome-improving impact. VA’s VistA Evolution strategy, as elaborated in the VistA 4 Product Roadmap and VistA 4 Product Architecture, includes the creation of a structured, deliberate, and predictable migration path from our custom and proprietary EHR software to an openly architected, modular, and standards-based platform. To address this issue, VA requires support of an open source agent that opens the aperture to broader-based public and private sector open source contributions that can facilitate modernization of VistA as part of VA’s VistA Evolution strategy. This effort is expected to drive VA achievement of the following objectives:

1. Facilitate EHR innovation consistent with industry best practices inside VA.
2. Release VA’s captive dependency on any particular component or service and give VA access to the best available open source tools and solutions to improve VistA EHR performance.
3. Reduce the costs and risks of reliable implementation (and integration) of new functional modules that improve VA VistA’s capabilities and further interoperability with DoD and private healthcare provider Electronic Health Record systems.
4. Measurably improve health outcomes for our nation’s Veterans.

# APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. 10 U.S.C. § 2224, "Defense Information Assurance Program"
4. 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
5. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
6. **42 U.S.C. § 2000d “**Title VI of the Civil Rights Act of 1964”
7. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
8. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
9. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
10. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
11. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
16. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
17. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
18. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
19. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
20. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
21. VA Handbook 6500.6, “Contract Security,” March 12, 2010
22. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at <https://www.voa.va.gov/>)
23. OI&T ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at <https://www.voa.va.gov/>) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
24. Technical Reference Model (TRM) (reference at <https://www.voa.va.gov/>)
25. National Institute Standards and Technology (NIST) Special Publications (SP)

VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008

VA Directive 6300, Records and Information Management, February 26, 2009

VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

OMB Memorandum, “Transition to IPv6”, September 28, 2010

VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011

1. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014

OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006

OMB Memorandum 05-24, Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005

OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011

OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011

NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems, November 20, 2008

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

NIST SP 800-63-2, Electronic Authentication Guideline, August 2013

Draft NIST Special Publication 800-157, Guidelines for Derived Personal Identity 523 Verification (PIV) Credentials, March 2014

NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in 525 Mobile Devices (Draft), October 2012

Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014

VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference Enterprise Architecture Section, PIV / IAM https://www.voa.va.gov/)

VA Memorandum, VAIQ # 7100145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM <https://www.voa.va.gov/>)

IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM <https://www.voa.va.gov/>)

# SCOPE OF WORK

The Contractor shall perform research and analysis of open source EHR products and code to facilitate VA’s awareness and decision-making of open source software and product candidates for VA VistA Intake. The Contractor shall perform a Capability Based Assessment (CBA) to identify necessary VA EHR capabilities, identify open source software and product candidates that may fulfill the VA capability gaps, and determine the best approaches at achieving the desired VA capabilities and closing the gaps with available open source software. Based upon the Contractor’s VA open source intake candidates identified and VA’s prioritization of them, the Contractor shall conduct certification testing of any candidates not already certified. The Contractor shall develop a working group charter and facilitate VA VistA-focused Technical Working Groups (TWGs) within which various clinically-focused or technically-focused groups can be managed throughout their life cycle. The Contractor shall provide architecture visualization tools to assist TWG facilitation and decision-making. If exercised, the Contractor shall support an optional Transition Support task.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The period of performance (POP) shall betwelve (12) months from the date of award with two (2), twelve (12)-month option periods to be exercised at the Government’s discretion.

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day January 1

Independence Day July 4

Veterans Day November 11

Christmas Day December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday Third Monday in January

Washington's Birthday Third Monday in February

Memorial Day Last Monday in May

Labor Day First Monday in September

Columbus Day Second Monday in October

Thanksgiving Fourth Thursday in November

## PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at Contractor facilities.

## TRAVEL

The Government anticipates travel under this effort to attend program-related meetings or conferences throughout the period of performance.  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 (4) trips for three (3) days in duration per trip, for each of the base and option periods.  Washington, DC is the anticipated location for travel.

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

## PROJECT MANAGEMENT (BASE AND OPTION PERIODS)

### TECHNICAL KICK OFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after contract 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 Contracting Officer (CO), Contract Specialist (CS), COR, and the VA Program Manager.

### CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) to outline an overall plan/strategy to accomplish the tasks outlined in this PWS. At a minimum, the PMP shall include the risk, quality and technical management approach, work breakdown structure (WBS), schedule management approach, schedule, cost requirements, and proposed staffing plan. The CPMP shall follow the VA protocols to the extent possible, or as otherwise agreed by the VA PM or COR. In addition, the CPMP shall identify and define in the CPMP recommended Key Performance Indicators (KPIs) and the means of measurement that provide VA visibility to: 1) the quantity of open source EHR products, code, and toolsets identified that align to, or would further enhance/expand upon, the feature set requirements as defined in VistA 4 Product Roadmap, as identified in PWS Section 5.2.1 and 2) the extent to which open source open source EHR products, code, and toolsets meet VA VistA Intake requirements, as identified by Capability Based Assessments (CBAs) performed in PWS Section 5.2.1, 3) the quantity of open source EHR products, code, and toolsets tested and certified for VA VistA Intake, as validated by PWS Section 5.2.2.

Once agreed by the VA PM, the Contractor shall track and report those metrics in the Monthly Progress Report. The Contractor shall update and maintain the VA PM-approved CPMP throughout the period of performance and report KPIs in the Monthly Progress Report (PWS 5.1.3).

**Deliverables:**

1. Contractor Project Management Plan

### MONTHLY PROGRESS REPORTING REQUIREMENTS

The Contractor shall deliver Monthly Progress Reports. These reports shall provide accurate, timely, and complete project information supporting PD reporting Requirements. The Monthly Progress Report shall include the following data elements.

1. Contract Activities Report:
2. Project Name and <Contract/Task Order> Name
3. Overview and description of the <Contract/Task Order>
4. Overall high level assessment of <Contract/Task Order> progress
5. All work in-progress and completed during the reporting period
6. Identification of any <Contract/Task Order> related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
7. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
8. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
9. Work planned for the subsequent four (4) reporting periods, when applicable
10. Current <Contract/Task Order> schedule overlaid on original <Contract/Task Order> schedule showing any delays or advancement in schedule
11. Current definition of user requirements / function points overlaid over the original function points and the last reported function points to specifically identify changes in the function points to be delivered since the previous report.
12. Original schedule of deliverables and the corresponding deliverables made during the current reporting period.

2) Monthly Communications Progress Report

1. Summary of each month’s communications in relation to tasks performed in support of PWS Tasks 5.2.1 – 5.2.3.
2. Work Group Progress Report
3. Summary of each month’s work group tasks performed in support of PWS Task 5.2.4.
4. Monthly Progress Report on Licensing Activities and Issues
5. Summary of each month’s licensing activities and issues performed in support of PWS Task 5.3.2.
6. Key Performance Indicators (KPI) Progress Report
7. A baseline set of KPIs shall be established and reported, once defined in the CPMP and as approved by the VA PM. In all subsequent reports, incremental updates to KPIs shall be reported and tracked to show progress from the baseline on a month-to-month basis.

These reports shall not be the only means of communication between the Contractor, COR and the Program/Project Manager to advise of performance/schedule issues and to develop strategies for addressing the issues. The Contractor shall continuously monitor performance and report any deviation from the CPMP or previous Monthly Progress Report to the COR and Program/Project Manager during routine, regular communications.

**Deliverables**:

1. Monthly Progress Report

### QUARTERLY REVIEW MEETINGS

The Contractor shall conduct quarterly review meetings with VA by which to report progress against the PWS task requirements and discuss KPI outcomes and opportunities for improvement. The Contractor shall prepare a quarterly In Progress Review (IPR) brief to facilitate conduct of IPRs. The Contractor shall conduct the first IPR at the end of the first three month period following contract award and shall conduct subsequent IPRs every three months thereafter. The Contractor shall coordinate date, time, meeting space and support for the IPR, as required. The Contractor shall provide a Draft IPR Agenda for VA PM approval at least five business days prior to the IPR. The Contractor shall document meeting minutes and distribute to attendees within two business days following the IPR.

**Deliverables:**

1. Quarterly In Progress Review (IPR) Brief

### PRIVACY TRAINING

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task. The status reporting shall identify; a single Contractor Security POC, the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. This information shall be submitted as part of the Monthly Progress Report.

The Contractor shall submit VA Privacy and Information Security training certificates in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, “Contract Security”.

**Deliverables:**

1. VA Privacy and Information Security Training Certificates

## TECHNICAL SUPPORT SERVICES for VA VistA (BASE AND OPTION PERIODS)

### ASSESS OPEN SOURCE PRODUCT CANDIDATES FOR VA VISTA INTAKE

The Contractor shall conduct “Discovery” activities, performing research and analysis to identify open source EHR products, code, and toolsets that align to, or would further enhance/expand upon, the feature set requirements as defined in VistA 4 Product Roadmap. The Contractor shall perform a capabilities based assessment (CBA) to identify necessary VA EHR capabilities, identify open source candidates that may fulfill the VA capability gaps, and determine the best approaches at achieving the desired VA capabilities and closing the gaps with available open source software and products. The Contractor shall perform the CBA on a cyclical, quarterly basis as prioritized by the VA PM as follows:

* First Quarter following award: Primary Feature Set 3 priorities
* Second Quarter: Secondary Feature Set 3 priorities
* Third Quarter: Primary Feature Set 4 priorities
* Fourth Quarter: Secondary Feature Set 4 priorities
* Option Periods (by quarter): new VistA 4 Feature Sets, VistA 5 Feature Sets, and/or non-VistA Feature sets, as identified and/or prioritized by the VA PM

The Contractor shall perform a SWOT analysis to assess the strengths, weaknesses, opportunities, and threats to VA of the discovered open source software and products to be considered for VA VistA intake. The Contractor shall rank order the products, with the highest functional strengths/opportunities and lowest weaknesses/threats in alignment to VistA 4-required functional feature sets in its SWOT analysis, from which to verify with the VA PM the prioritized sequence of further analysis.

The Government will provide as Government Furnished Information (GFI) the VistA 4 Product Roadmap, VistA 4 Product Architecture Document, Business Requirements Documents (BRDs) and Requirements Specification Documents (RSDs), the latter two as they are elaborated for each VistA 4 application Feature Set. The Contractor shall utilize these documents to produce a Gap Analysis of priority features and functions required to progress VA’s VistA vision, with primary emphasis on how that vision is elaborated in the Feature Set delivery schedule per the VistA 4 Product Roadmap.

The Contractor shall overlay the findings of the Gap Analysis and SWOT to document detailed Open Source Software and Product Selection Criteria which:

* Consolidates and prioritizes with VA the functional, technical, and performance attributes of VistA Feature Set or non-VistA Feature Set variables for further investigation;
* Documents the constraints and assumptions or “boundary conditions” which define imposed limitations that can be physical or programmatic (e.g., Specifying the latest acceptable initial operational capability (IOC) date illustrates a programmatic constraint);
* Elaborates capability gaps identified in the respective BRDs and RSDs;
* Elaborates the extent to which the code has been vetted and tested by the open source community, and the extent to which that code may have been previously certified via automated testing and peer review which has verified the safety, compliance and functionality of the code both prior to and after new code submissions;
* Assigns a quantitative metric by which to measure open source product attributes against functional, technical, capacity, performance, interoperability, and security requirements criteria. Additionally, the Contractor’s assessment shall include implementation criteria by which to assess the ease of integrating the open source code in the corresponding VA VistA application and with the application’s internal VA VistA interfaces.

The Contractor shall utilize its documented Open Source Software and Product Selection Criteria from which to again scour the open source EHR software community to expand upon and further analyze the detailed functional, technical, capacity, performance, interoperability, and security attributes of open source candidates that may fulfill the capability gaps. The Contractor shall utilize the VA open source software selection criteria to measure the degree to which open source candidates that may fulfill the capability gaps. Upon completion of analysis and measurement, the Contractor shall document its findings in a Prioritization Description Document for VA Open Source Intake Candidates. For each open source candidate, the Contractor shall, at a minimum:

* Provide a mapping and functional description of open source software features proposed for VA VistA intake as they correlate to defined VA VistA 4 Feature Sets;
* Elaborate how the alternatives for the same VistA feature set compare to one another
* Identify and size the scope of additional development required to meet VA requirements
* Provide supporting technical detail regarding supported and/or required/missing components (such as client and server operating systems, database managers, application program interfaces, etc.);
* Provide recommendations regarding any required/missing components necessary for full operation of VA VistA that may be addressed through either open source or other channels;
* Identify the level of maturity and supportability requirements associated with the intake of the respective open source code;
* Identify any licensing implications affecting intake;
* Identify risks (technical, operational, programmatic) for each open source alternative
* Identify proposed mitigation strategies for risks associated with VA VistA intake that may affect national deployment at VAMCs nation-wide.

The SWOT Analysis, Gap Analysis, Software/Product Selection Criteria, and Prioritization Description Document for VA Open Source Intake Candidates shall comprise the CBA package. At least three (3) CBAs shall be produced quarterly as aligned to the quarterly priority schedule depicted in this section above. As the project progresses through each quarterly CBA cycle, the Contractor shall again scour the open source community to identify if any new code has been added for a prior quarter’s software or products already evaluated (e.g., new enhancements, bug fixes, new availability of software tests) to ensure that CBAs reflect the current state quarterly.

As this project evolves and CBAs are completed for VistA 4 products, the Contractor’s research shall identify non-VistA 4-related open source EHR products, code, and toolsets which may provide functionality and features not yet planned for VA VistA 4 or a subsequent VistA 5, but which may further the goals elaborated in PWS Section 1.0, Background. Alternatively, should there be compelling rationale to shift analysis priorities at any time during the execution of the project, the Contractor shall recommend to the VA PM and provide supporting justification for its proposed sequence of CBAs for the continued evolution of VA VistA consistent with industry best practice EHR capability sets, for VA PM approval.

The Contractor shall review the results of the CBAs produced quarterly during the Quarterly Review Meeting (In Progress Review (IPR)) with the VA PM and VA-designated project stakeholders. Stakeholder review shall include, but may not be limited to the relevant VHA business stakeholder(s), the VistA Evolution PM, Director of Product Development for Open Source, and the VistA Intake PM. The IPR will serve to confirm the Contractor’s analysis of priority candidates for VA VistA intake to be tested for preliminary certification, if not previously certified by the open source community.

As the open source codebase evolves on a quarterly basis with new features and enhancements, the Contractor shall continue its Discovery activities and perform a SWOT analysis of the new open source candidates identified. The Contractor shall review the results of this analysis with the VA PM monthly by which to prioritize or re-prioritize the list of CBAs to be performed during the given quarter.

**Deliverables:**

1. SWOT Analysis
2. Gap Analysis
3. Software/Product Selection Criteria
4. Prioritization Description Document for VA Open Source Intake Candidates

### CERTIFICATION TESTING

VA has developed an extensive set of processes and procedures that are currently used to certify software for internal use. Certification testing is not intended to replace or replicate that testing. Rather, the level of testing defined herein is meant to ensure that code considered for VA VistA Intake is:

* Safe - Individual code units do not cause errors in other components of the system and the code is robust through all code paths and conditions.
* Compliant - Code meets agreed-upon interface specifications.
* Functional - Code has a defined set of requirements that are met when the code executes.

Based upon the Contractor’s VA open source intake candidates identified in PWS 5.2.1 and VA’s prioritization of them at the IPR, the Contractor shall conduct certification testing of any candidates not already certified. VA will provide a redacted copy of the VA VistA code as GFE against which the Contractor shall perform certification testing.

The Contractor shall elicit any tests and test results from the open source software provider for code made available to the open source community. The Contractor shall utilize a code certification testing framework and process to perform automated unit, functional and regression tests by which to verify the safety, compliance and functionality of the code. The Contractor shall maintain a testing environment capable of ensuring successful execution of unit, integration, and regression testing of open source software and products being examined for certification and their compatibility to existing VistA products when interfaced to or co-residing in the same production environment. Testing environment shall include a test data bed of operational data that can represent complex patient demographic, patient health data relationships, and health care business and operational data in order to provide assurances that testing and certification is being performed on data representative of a VA production environment. Testing Environment shall include utilities already existing in VistA as well as utilities provided by the Contractor that can ascertain compliance to VA programming standards, VA development standards for use of application programming interfaces and data usage across products, at a minimum. The Contractor shall also assess the degree of test coverage to evaluate how much of the code base is visited and exercised during the testing activities.

The Contractor shall depict the results of testing in a testing dashboard in which the status of the current codebase is displayed. The Contractor dashboard shall display, at a minimum, the product build nomenclature, errors identified during the code configuration and build process, and the results (pass/fail) of the automated tests. Any issues found during Contractor testing shall be documented in an Issue Tracker application.

Upon completion of testing, the Contractor shall produce a Test Results Report to document the level to which the candidate open source software or product meets the defined standards for certification of code relevant for VA VistA intake. The Contractor shall update the Prioritization Description Document for VA Open Source Intake Candidates, henceforth re-named Recommended VA Open Source Intake Candidates, to elaborate and provide substantiating evidence regarding the extent to which the candidate software meets the software selection criteria, is certified at a particular level of certification, and which identifies any remaining issues, gaps, or risks that should be fulfilled and/or resolved to fully meet VA VistA Intake requirements. The Contractor shall append the Test Results Report to the Recommended VA Open Source Intake Candidates to centralize and support its recommendation.

The Contractor shall vet and attempt to minimize any identified risks to VA Open Source Intake Candidates through its established open source Working Groups, per PWS 5.3.

**Deliverables:**

1. Posting of Test Results to Test Results Dashboard
2. Test Results Report
3. Recommended VA Open Source Intake Candidates Automated Test Scripts

## TECHNICAL WORKING GROUP SERVICES (BASE AND OPTION PERIODS)

### VA TECHNICAL WORKING GROUP (TWG) CHARTER DEVELOPMENT AND TWG FACILITATION

The Contractor shall provide a working group charter for the establishment and/or continuity of VA VistA-focused Technical Working Groups (TWGs) within which various clinically-focused or technically-focused groups can be managed throughout their life cycle (from initial charter through dissolution). The TWG Charter shall include appendices identifying these groups relevant to the CBAs planned and/or performed, VA stakeholders (e.g., VHA business stakeholder(s), the VistA Evolution PM, Director of Product Development for Open Source, and the VistA Intake PM) which are voting decision makers, and open source community members which are active participants in development of open source code and products relevant to the CBA. The purpose of the TWGs shall be to:

* Enable VHA business stakeholders to elaborate upon requirements in VA BRDs and to elicit feedback from working group members on the improvement of BRDs based on new EHR technologies and/or enhanced business processes that may enhance clinical decision support;
* Enable the Contractor to elaborate and share with the VA and open source community any gaps identified in the CBAs performed in PWS Section 5.2.1;
* Facilitate open source community visibility to VA VistA software gaps and/or issues preventing certification, for subsequent open source software development planning and open source code submission to be considered for VA VistA;
* Capture and prioritize issues for review, discussion and action by the respective TWG;
* Increase the level of open source code submissions that meet VA VistA Intake requirements due to TWG collaboration.

The Contractor shall conduct no less than three (3) TWGs quarterly for clinically and/or technically-focused working groups as aligned to the quarterly priority schedule depicted in PWS 5.2.1. The Contractor shall utilize Contractor-provided online web service and collaboration tools to provide meeting facilitation and management. The Contractor shall provide support for preparation of meeting facilitation materials and capture/dissemination of meeting minutes.

The Contractor shall develop and provide an online TWG website and corresponding working group landing pages for each TWG through which group members can communicate and download relevant group information.

**Deliverables:**

1. Technical Working Group Charter
2. Meeting Facilitation Materials
3. Meeting Minutes
4. TWG Website

### EHR ORIENTATION AND VISUALIZATION MODELS

The Contractor shall provide and maintain a current architecture visualization toolset that supports web content and architecture visualization of the current VistA and planned VistA 4 and beyond application, service, data, platform, and system architectures. These toolsets shall be utilized to facilitate interaction with and feedback from the VA VistA TWGs.

**Deliverables:**

1. Current Architecture Visualization Toolset

## TRANSITION SUPPORT (OPTIONAL TASK)

The Contractor shall document and execute a Phase–Out Transition Plan that defines the tasks, schedule, and responsible parties to conduct transition to the Government or selected Contractor of GFI/GFE, licenses, software, hardware, and data developed and/or collected for analysis under this contract. The Contractor shall submit a Phase-Out Transition Plan, and execute the Plan upon COR approval.

The Phase-Out Transition Plan shall include, but is not limited to:

* An approach for handoff of legacy program documentation, source code evaluation (to include open source EHR products, code, and toolsets, all versions, maintenance updates and patches) technical data, computer software, and computer software documentation (compiled and un-compiled, including all versions, maintenance updates and patches), written instructions for the source code, metrics and statistics;
* An inventory and transition of historical data (e.g., meeting minutes, deliverable artifacts);
* A Transition/ Knowledge Transfer Schedule to include meetings and briefings with Government and Contractor representatives to explain demarcation of responsibilities, interface points for performance of work elements and explanation of relevant artifacts and materials. The Transition/ Knowledge Transfer Schedule shall include proposed dates, times and required attendees;
* A strategy and approach regarding personnel staffing and training during the transition period;
* Names of the points of contact that will manage and execute the transition activities;
* Risks and associated risk mitigation;
* Lessons learned documentation;
* Method/metrics to demonstrate completion of Knowledge Transfer;
* The transfer of GFE, GFI, and GFE inventory management assistance
* The handover of all Government keys, identification/access cards, and security codes.

**Deliverables:**

A. Phase-Out Transition Plan

# GENERAL REQUIREMENTS

## ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software development is compliant with the VA Enterprise Technical Architecture (ETA), and specifically for compliance and integration with Identity and Access Management (IAM) requirements and IAM enterprise design and integration patterns, <http://www.techstrategies.oit.va.gov/docs_design_patterns.asp>. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145) and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document, <https://www.voa.va.gov/>). The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2 and VA IAM enterprise requirements for both direct and assertion based authentication.  Direct authentication at a minimum must include PKI base authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC).  Specific Identity and Access Management Personal Identity Verification (PIV) requirements as set forth in OMB Memoranda M-04-04 ([http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf)](http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf%29), M-05-24 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>), M-11-11 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.  Assertion authentication at a minimum must include SAML token authentication and authentication/account binding based on trusted headers.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 <http://www-x.antd.nist.gov/usgv6/index.html>), the Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>), and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Information concerning IPv6 transition in addition to OMB/VA Memoranda can be found at <https://www.voa.va.gov/>.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstation shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA’s current desktop application deployment tool. Signing of the software code shall be through a vendor provide certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

## POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

### POSITION/TASK RISK DESIGNATION LEVEL(S)

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

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

|  |  |
| --- | --- |
|  | **Position Sensitivity and Background Investigation Requirements** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Task Number** | Low/NACI | Moderate/MBI | High/BI |
| 5.1 | [x]  | [ ]  | [ ]  |
| 5.2 | [x]  | [ ]  | [ ]  |
| 5.3 | [ ]  | [x]  | [ ]  |
| 5.4 | [ ]  | [x]  | [ ]  |

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

###  CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

1. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
2. The Contractor shall bear the expense of obtaining background investigations.
3. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor’s Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
4. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
5. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
6. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
7. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
8. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
9. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or “Closed, No Issues” (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed “Contractor Rules of Behavior.” However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
10. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
11. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

## METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

##  PERFORMANCE METRICS

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

|  |  |  |
| --- | --- | --- |
| **Performance Objective** | **Performance Standard** | **Acceptable Performance Levels** |
| 1. Technical Needs
 | 1. Shows understanding of requirements
2. Efficient and effective in meeting requirements
3. Meets technical needs and mission requirements
4. Offers quality services/products
 | Satisfactory or higher |
| 1. Project Milestones and Schedule
 | 1. Quick response capability
2. Products completed, reviewed, delivered in timely manner
3. Notifies customer in advance of potential problems
 | Satisfactory or higher |
| 1. Project Staffing
 | 1. Currency of expertise
2. Personnel possess necessary knowledge, skills and abilities to perform tasks
 | Satisfactory or higher |
| 1. Value Added
 | 1. Provided valuable service to Government
2. Services/products delivered were of desired quality
3. KPIs collected demonstrate continuous improvement in VA’s open source evaluation, utilization, and interoperability with key interfaces.
 | Satisfactory or higher |

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

## FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

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

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort.  The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP’s) and Authority to Operate (ATO)’s for all systems/LAN’s accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

## GOVERNMENT FURNISHED PROPERTY

N/A