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

**PERFORMANCE WORK STATEMENT (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**

**Office of Information & Technology**

**Product Development**

**Medical Appointment Scheduling System (MASS)**

**Date: September 9, 2014**

**TAC-15-16846** **PWS Version Number: 1.17**

Contents

[1.0 BACKGROUND 5](#_Toc398632962)

[2.0 APPLICABLE DOCUMENTS 9](#_Toc398632963)

[3.0 SCOPE OF WORK 10](#_Toc398632964)

[3.1 MASS SOLUTION 11](#_Toc398632965)

[3.1.1 MASS OBJECTIVE 11](#_Toc398632966)

[3.1.2 MASS MAJOR SYSTEM COMPONENTS 13](#_Toc398632967)

[3.1.3 MASS COTS SCHEDULING APPLICATION 13](#_Toc398632968)

[3.1.4 ENTERPRISE SHARED SERVICES INFRASTRUCTURE 13](#_Toc398632969)

[3.1.5 VA SYSTEMS 14](#_Toc398632970)

[4.0 PERFORMANCE DETAILS 16](#_Toc398632971)

[4.1 CONTRACT TYPE 16](#_Toc398632972)

[4.2 PERIOD OF PERFORMANCE 17](#_Toc398632973)

[4.3 PLACE OF PERFORMANCE 17](#_Toc398632974)

[4.4 TRAVEL 17](#_Toc398632975)

[4.5 METHOD AND DISTRIBUTION OF DELIVERABLES 17](#_Toc398632976)

[4.6 FACILITY/RESOURCE PROVISIONS 17](#_Toc398632977)

[4.7 MATERIALS, EQUIPMENT AND FACILITIES 18](#_Toc398632978)

[4.7.1 Government-Furnished 18](#_Toc398632979)

[4.7.2 Contractor-Furnished 18](#_Toc398632980)

[4.7.3 Non-Developmental Items and Commercial Processes 18](#_Toc398632981)

[4.7.4 Connectivity 18](#_Toc398632982)

[4.8 SECTION 508 REQUIREMENTS 19](#_Toc398632983)

[4.9 SAFETY AND ENVIRONMENTAL 19](#_Toc398632984)

[4.10 PMAS/PROPATH 19](#_Toc398632985)

[4.11 ENTERPRISE AND IT FRAMEWORK 19](#_Toc398632986)

[4.12 TRANSITION AND ORIENTATION SUPPORT AT END OF CONTRACT 20](#_Toc398632987)

[5.0 SPECIFIC REQUIREMENTS, TASKS, AND DELIVERABLES 20](#_Toc398632988)

[5.1 PROGRAM MANAGEMENT, STRATEGY, AND PLANNING SUPPORT 20](#_Toc398632989)

[5.1.1 CONTRACT PROJECT MANAGEMENT PLAN 20](#_Toc398632990)

[5.1.2 SOFTWARE CONFIGURATION MANAGEMENT 21](#_Toc398632991)

[5.1.3 ORGANIZATIONAL CHANGE MANAGEMENT 21](#_Toc398632992)

[5.1.4 INTEGRATED PROJECT/BUSINESS TEAM SUPPORT 21](#_Toc398632993)

[5.2 MASS STRATEGY AND PLANNING 21](#_Toc398632994)

[5.2.1 REQUIREMENTS ELABORATION, ANALYSIS and VALIDATION SUPPORT 22](#_Toc398632995)

[5.2.2 STUDIES AND ANALYSES 22](#_Toc398632996)

[5.3 MASS Prototyping Environments 22](#_Toc398632997)

[5.4 MASS Systems/Software/HARDWARE Engineering 23](#_Toc398632998)

[5.4.1 MASS DESIGN AND DEVELOPMENT 23](#_Toc398632999)

[5.4.2 MASS ARCHITECTURE DEVELOPMENT 23](#_Toc398633000)

[5.4.3 MASS SYSTEM/SOFTWARE INTEGRATION 24](#_Toc398633001)

[5.4.4.1 DATA MIGRATION 24](#_Toc398633002)

[5.5 Test & Evaluation 24](#_Toc398633003)

[5.6 Independent Verification and Validation (IV&V) SUPPORT 25](#_Toc398633004)

[5.7 CYBER SECURITY 25](#_Toc398633005)

[5.7.1 Information Assurance (IA) 25](#_Toc398633006)

[5.7.2 Logical Security 25](#_Toc398633007)

[5.7.3 Security Operating Support 26](#_Toc398633008)

[5.7.4 Assessment and Authorization 26](#_Toc398633009)

[5.8 HARDWARE, SOFTWARE, LICENSE, AND MAINTENANCE PROCUREMENT 27](#_Toc398633010)

[5.9 INSTALLATION, CONFIGURATION AND IMPLEMENTATION 27](#_Toc398633011)

[5.10 Operations and Maintenance (O&M) 27](#_Toc398633012)

[5.10.1 SYSTEMS ADMINISTRATION 28](#_Toc398633013)

[5.10.2 DISASTER RECOVERY AND CONTINUITY OF OPERATIONS 29](#_Toc398633014)

[5.10.3 CAPACITY/AVAILABILITY PLANNING AND MANAGEMENT 29](#_Toc398633015)

[5.10.4 TIERS I, II, III, AND HELP DESK SUPPORT 29](#_Toc398633016)

[5.10.5 IT SERVICES MANAGEMENT GUIDANCE 29](#_Toc398633017)

[5.11 Training 30](#_Toc398633018)

[5.12 CONTRACT MANAGEMENT 31](#_Toc398633019)

[5.12.1 GOVERNMENT SUPPORT 31](#_Toc398633020)

[5.12.1.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR) 31](#_Toc398633021)

[5.12.1.2 COR – TASK ORDERS 31](#_Toc398633022)

[5.12.5 CONTRACTOR SUPPORT 31](#_Toc398633032)

[5.12.5.1 CONTRACTOR PROGRAM MANAGEMENT 31](#_Toc398633033)

[5.12.5.2 POINTS OF CONTACT 31](#_Toc398633034)

[5.12.5.3 WORK CONTROL 32](#_Toc398633035)

[5.13 GOVERNMENT RIGHTS 32](#_Toc398633036)

[5.13.1 TECHNOLOGY INSERTION 32](#_Toc398633037)

[6.0 GENERAL REQUIREMENTS 32](#_Toc398633038)

[6.1 MONTHLY CONTRACT STATUS REPORT 33](#_Toc398633039)

[6.2 STATUS OF GFE REPORT 33](#_Toc398633040)

[6.3 PERSONNEL CONTRACTOR MANPOWER REPORT 34](#_Toc398633041)

[6.4 SMALL BUSINESS PARTICIPATION REPORT 35](#_Toc398633042)

[6.5 MEETINGS AND REVIEWS 35](#_Toc398633043)

[6.5.1 POST AWARD CONFERENCE 35](#_Toc398633044)

[6.5.2 TASK ORDER KICKOFF MEETINGS 35](#_Toc398633045)

[6.5.3 PROJECT PROGRESS REVIEWS 35](#_Toc398633046)

[6.5.4 ORGANIZATIONAL CHART 36](#_Toc398633047)

[6.5.5 PRIMAVERA 37](#_Toc398633048)

[6.5.6 PRIVACY TRAINING 37](#_Toc398633049)

[6.5.7 PRODUCT DATA 37](#_Toc398633050)

[7.0 DELIVERABLES 38](#_Toc398633051)

[7.1 Products 38](#_Toc398633052)

[7.2 Data 38](#_Toc398633053)

[8.0 SECURITY 38](#_Toc398633054)

[8.1 Systems Security 38](#_Toc398633055)

[8.2 Personnel Security 38](#_Toc398633056)

[8.2.1 Position Risk Level and Contractor Personnel Security Requirements 38](#_Toc398633057)

[8.2.2 Security Requirements 40](#_Toc398633058)

[8.3 METHOD AND DISTRIBUTION OF DELIVERABLES 42](#_Toc398633059)

[8.4 PERFORMANCE METRICS 42](#_Toc398633060)

[8.5 FACILITY/RESOURCE PROVISIONS 43](#_Toc398633061)

[ADDENDUM A 45](#_Toc398633062)

[ADDENDUM B 50](#_Toc398633063)

[ADDENDUM C 62](#_Toc398633064)

# 1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA) is to provide benefits and services to Veterans of the United States.  In meeting these goals, VA strives to provide high quality, effective, timely Veteran-centric services.  The VA Office of Information & Technology (OI&T) supports those responsible for providing care to the Veterans at the point-of-care as well as throughout the Veterans’ experience with VA. VA depends on best in class Information Management/Information Technology (IM/IT) systems, compassionate, skilled heath care professionals and industry best practices to meet mission goals.

**The need for VA Medical Appointment Scheduling System (MASS)**

VA serves America’s Veterans and is their principal advocate to ensure that they receive medical care, benefits, social support, and lasting memorials.  VA promotes the health, welfare, and dignity of all Veterans in recognition of their service to this Nation.

VA is comprised of a Central Office (VACO), which is located in Washington, DC, and field facilities throughout the Nation, as well as the U.S. territories and the Philippines.  Programs are administered by its three major line organizations: Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA).

VHA operates the largest integrated health care delivery system in America with more than 1,700 hospitals, clinics, community living centers, domiciliaries, readjustment counseling centers, and other facilities.  VHA provides a broad range of primary care, specialized care and related medical and social support services.  VHA is also the Nation’s largest integrated provider of health care education and training for physician residents and other health care trainees. VA advances medical research and development in areas that most directly address the diseases and conditions that affect Veterans and eligible beneficiaries.

Access to VHA services is at the center of the VHA mission to provide exceptional healthcare that improves the Veterans’ health and well-being. To accomplish its mission, VHA needs to ensure that there is consistency and expediency in providing needed services to our Veterans; timely access to care where and when needed, equity across VHA in the number and types of services available, and consistency in access to those services. The mission has become even more of a challenge as demand for VA healthcare services has increased.

In order to consistently and reliably meet access commitments, VHA will need to ensure standardization of operational policies for clinic management related to patient scheduling and wait times. This will require updating the current scheduling system and modernizing operations, as well as consistently managing workload demand and consult request and tracking across the enterprise. More importantly, VHA will be enabling transition from a face-to-face appointment model to a sustained relationship model using multiple forms of access and engagement.

There is no single VHA entity responsible for these activities, therefore VHA’s Office of the Deputy Under Secretary for Health Operations and Management (DUSHOM) established a program office to define, standardize and coordinate system-wide administrative clinic operations and management. This program is designated as the Access and Clinic Administration Program (ACAP). The scope of ACAP will include outpatient access standards and workload capacity alignment; with the highest order being Primary Care and Mental Health, and call center operations to include triage, queuing and standard operating procedures. Specialty Care clinic access will include the aforementioned plus consult management, including establishment of tracking and monitoring standards. The ACAP will also serve as VHA’s business owner and manager in collaboration with OI&T in matters regarding appointment scheduling. Additionally, the ACAP will bridge the gaps and disconnects between policy and operations necessary to comprehensively define and coordinate the transformation of clinic operations which will require standardization through policies that are consistently implemented, performance measures that are reliable and actionable and reporting structures that facilitate accountability. These initiatives will result in fundamental business processes that will ensure standardization of clinic practices across VA Healthcare systems and proactively and strategically focus on systemic improvements to Veterans’ access to care.

VHA is currently utilizing several data extracts to assess clinic appointment waiting; however, due to a lack of standardization across VHA facilities, this measurement is not accurate for National Wait Time reporting. Challenges with wait time estimates include, but are not limited to: the inability to distinguish between new and follow-up visits, inconsistent use of Decision Support Services (DSS) Identifiers (used for wait time extracts), inability to document a patient or provider’s desired date for a future appointment, and the inability to calculate the total time interval between the request and when the appointment was actually made or has been rescheduled several times.

**Current VistA Scheduling**

Veterans Health Information Systems and Technology Architecture (VistA) is the VA Electronic Health Record (EHR) and includes many applications such as registration, enrollment and eligibility systems, health provider systems (including Laboratory and Computerized Patient Record Service (CPRS)), management and financial systems, health data systems, and cross cutting infrastructure systems.

The MASS project will replace the current outpatient scheduling system to provide more efficient access to care for Veterans. Medical outpatient scheduling is complex in that it requires coordination across medical practices while enforcing clinical delivery business rules. VistA Scheduling was built in the early 1980’s as an inpatient care scheduling system with few embedded clinical delivery business rules. Today’s VHA care delivery is dramatically different from the past with the majority of appointments scheduled for outpatient care. Recent movements towards home healthcare, telehealth and Veteran self-scheduling has illuminated the limitations of VistA Scheduling. In FY2013 approximately 8.9 million of the 21.9 million living Veterans in the nation were enrolled in the VA health care system. VHA’s 50,000 users schedule over 85 million appointments a year for this Veteran population. Serving this volume requires state of the art capacity management tools and a solution that provides for efficient scheduling to meet Veteran demands.

The current VHA Medical Scheduling system is outdated and outmoded. VHA’s current scheduling processes do not meet the needs of patients, providers and the VHA scheduling staff. Modernization of the system across the enterprise is required in order to meet ambulatory and patient appointment needs of VHA today. In the current state clinic grids are inflexible, productivity is not measurable, there is no method for scheduling resources (staff, rooms, equipment), and there are no links between scheduled appointments and ancillary appointments, i.e. lab and radiology. These broken links cause unnecessary bookings and rebookings as well as increased travel costs and patient dissatisfaction with VHA scheduling practices.

**VistA Evolution**

On February 5, 2013, the Secretary of VA (SECVA) announced VA has committed to utilizing the VistA as its EHR system. VA will enhance, or evolve, its VistA EHR to achieve its interoperability, clinical and technical objectives. As a result, VA will continue to utilize and improve VistA, which is considered to be one of the best EHR systems available today. The VistA EHR is vital to VA’s ability to deliver care to Veterans, Service Members, and their dependencies.

VA will deliver VistA enhancements, including the MASS, under the VistA Evolution (VE) Program. The VistA Evolution Program’s chief goal is achieving seamless interoperability with DoD and other healthcare partners; this goal is supported by clinical goals to enhance VistA to support a patient-centric, team-based healthcare delivery model, and technical goals to establish a robust Information Technology (IT) architecture to underpin current usage and future innovation.

The VE Program Plan defines VA’s structured approach to the development and deployment of an interoperable EHR that exchanges computable health information with DoD and other healthcare partners. The VE architecture will adhere to key open architecture tenets, open interface specifications, and design patterns that enable an open a scalable solution for the VistA EHR. The VistA 4 Roadmap is a supplement to the VE Program Plan and provides an overview of the functional capabilities that will be delivered for the VE Program.

**Future MASS and System Integration**

VA requires a commercially available off-the-shelf (COTS) based medical appointment scheduling solution that incrementally improves scheduling as it is integrated with VistA and deployed across the enterprise. The COTS scheduling system described in this subsection shall include mechanisms to achieve the following:

From the Goals/Objectives/Outcomes section in the Business Requirements Document (BRD):

* Improved Veteran service through appropriate, timely, and efficient appointment and visit scheduling.
* Web enablement to allow patients to request or view information via the Internet.
* Improved utilization of provider and clinic resources to include equipment and rooms.
* Accurate, maintainable system and user documentation.
* A formalized repository of scheduling business rules maintainable without developer intervention to promote standardization of business practices across VHA.
* Web based Graphical User Interfaces (GUIs).
* Open connectivity promoting regular upgrades and enhancements.
* Improved IT support of VHA’s shift to ambulatory care.
* Linkage to all VA systems.
* Provide scheduling appointment data within clinical workflow to provide a seamless interface to clinicians and clerical staff alike.

VA expects to deliver a core capability of the scheduling system within two years (in six month increments) of contract award followed by a series of six month incremental enhancements until full operational capability is reached.

CY20

CY15

CY16

CY17

Figure 1. MASS Notional Timeline

# **2.0** APPLICABLE DOCUMENTS

The documents listed below apply to the performance of this effort. The following documents are referenced for the performance of this effort:

1. VA Enterprise Architecture [<http://www.ea.oit.va.gov/> ]
2. VA ETA Compliance Criteria [<http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp>]
3. VA Technical Reference Model (TRM) [<http://www.va.gov/trm>]
4. VistA Evolution Architecture
5. VistA Evolution Design Patterns, available at: <http://www.techstrategies.oit.va.gov/docs_design_patterns.asp>
6. Preliminary MASS Requirements Specification Document (RSD), Aug. 2014
7. VistA Evolution Program Plan, Feb. 19, 2014 [ <https://vaforumfor.us/docs/DOC-4534> ]
8. VistA4 Product Plan, Jan. 29, 2014 [<https://vaforumfor.us/docs/DOC-4446> ]
9. VHA Business Blueprint Document, July 2014
10. MASS BRD, April 2014
11. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
12. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
13. 10 U.S.C. § 2224, "Defense Information Assurance Program"
14. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
15. **42 U.S.C. § 2000d “**Title VI of the Civil Rights Act of 1964”
16. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
17. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
18. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
19. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
20. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
21. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
22. 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
23. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
24. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
25. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
26. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
27. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
28. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008
29. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
30. VA Handbook 6500.6, “Contract Security,” March 12, 2010
31. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at <https://www.voa.va.gov/>)
32. 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.
33. National Institute Standards and Technology (NIST) Special Publications

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

EO Hosting Services document (provided as attachment to solicitation package)

1. Accreditation Requirements Guide Standard Operating Procedures, June 2014
2. FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
3. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, title IX Information Security Matters
4. Department of Veterans Affairs (VA) Handbook 6102 (Internet/Intranet Services) (<https://www.voa.va.gov/>)
5. Health Insurance Portability and Accountability Act (HIPAA); 45 CFR Part 160, 162, and 164; Health Insurance Reform: Security Standards; Final Rule dated February 20, 2003
6. VHA Security Handbook 1600.01, Business Associate Agreements (<https://www.voa.va.gov/>)
7. U.S.C. Section 552a, as amended
8. Federal Travel Regulation (FTR) ([www.gsa.gov/federaltravelregulation](http://www.gsa.gov/federaltravelregulation))
9. Federal Segment Architecture Methodology (FSAM) v1.0, December 2008
10. National Institute Standards and Technology (NIST) Special Publications 800 series
11. Open Source Electronic Health Record Alliance ([www.OSEHRA.org](http://www.OSEHRA.org))
12. Server Virtualization First Policy: <http://trm.oit.va.gov/files/Server_Virtualize_First_Policy.pdf>

# 3.0 SCOPE OF WORK

This Performance Work Statement (PWS) establishes the requirements for an Indefinite-Delivery/Indefinite Quantity (IDIQ) contract for Contractor-provided solutions in support of MASS. The Contractor shall provide the products and services to support the COTS-based MASS solution that includes configuration, customization, development, integration, installation, testing, implementation (product/service), training, software maintenance, optimization (technical/operational), and infrastructure (hardware and software) sustainment. In addition, the Contractor shall provide operational expertise and support for the business implementation as well as the user support required to ensure a successful implementation and rollout of the new MASS solution. This includes but is not limited to operational processes, organizational change management, training, documentation.

The technical, functional and nonfunctional requirements for the MASS system are captured in this PWS and the associated support documents. The Contractor shall provide the capabilities as outlined in this PWS and the aforementioned business requirements. Specific requirements will be defined in individual Task Orders (TO). The specific tasks may supplement but not replace the task requirements identified in this base PWS. A COTS solution can refer to commercial acquired software, rebranded commercial software, or fully supported open-source software that meets the requirements and objectives of this acquisition.

## 3.1 MASS SOLUTION

* + 1. **MASS OBJECTIVE**

The objective of the MASS program is to acquire a COTS scheduling application, integrate it with the VA enterprise, and build out all required portions of the VA infrastructure, and implement it within VHA’s clinical and administrative operations. The MASS Problem/Opportunity Statement is as follows:

|  |  |
| --- | --- |
| Problem/Opportunity statement(s): | * VHA’s current scheduling processes do not meet the needs of patients, providers, VHA’s scheduling staff and VHA management. The processes are unable to meet the supply and demand and the current medical scheduling system is outdated and outmoded. |
| Affects: | Veterans and other healthcare beneficiaries (spouses and dependents), providers and VHA. |
| The impact of which is: | * Financial: costly and resource intensive * Operational: excessive cycle time, waiting time is non-value added, inability to respond to supply and demand, poor visibility which impairs management and improvement of workflow processes and scheduling activities. * Patient Care: scheduling is not patient (Veteran) centric |
| A successful solution would: | * Provide patient centered scheduling services (Veteran centric) * Provide centralized scheduling services * Improve scheduling processes and oversight * Improve resource usage * Reduce administrative costs * Improve waiting time and overall cycle time of scheduling patients * Provide an audit trail of scheduling activities * Increase visibility for management and control of supply and demand * Standardize data collection * Enforce VHA policies, i.e. Business rules * Allow information sharing and data exchanges both internal and external to VHA * Meet Congressional and other external stakeholder reporting requirements |

VistA Scheduling is dependent upon approximately 31 current VistA Packages and 71 current VistA packages are dependent upon VistA Scheduling. These dependencies represent over a thousand individual integration points. Data synchronization between the COTS and VistA must be maintained, to support business processes dependent on appointment information. MASS shall enable current and future applications to access all required scheduling and related data.

The Unique/High Priority Business Needs of MASS are contained in the VHA Business Blueprint.

* + 1. **MASS MAJOR SYSTEM COMPONENTS**

The diagram below depicts the conceptual MASS architecture.

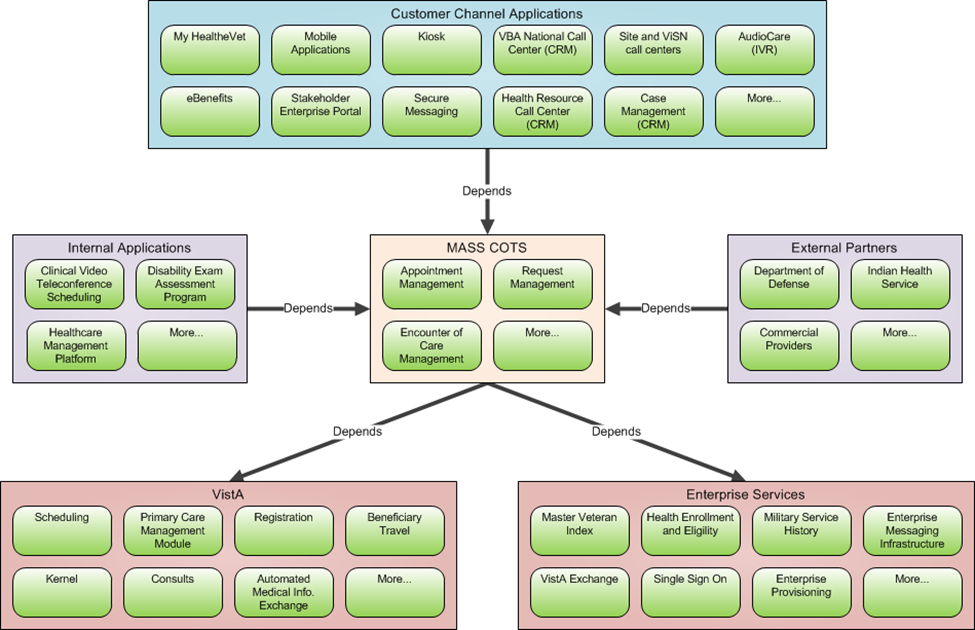


Figure 2. MASS Conceptual Architecture

* + 1. **MASS COTS SCHEDULING APPLICATION**

The MASS will include a COTS solution which meets the functional requirements for MASS project as identified in the BRD, Blueprint, and RSD. The COTS tools shall be configurable and able to support the integration of content sources and data elements into common services that can be leveraged by other MASS system components, such as Web or Service Interfaces, as well as external system components.

* + 1. **ENTERPRISE SHARED SERVICES INFRASTRUCTURE**

As shown in the notional architecture, COTS web applications services layer shall communicate with VA Enterprise Services and lower level services to provide comprehensive medical scheduling capabilities. Some services are existing and some will be created as part of the MASS.

The primary core enterprise health and information services which will be used by the MASS COTS solutions include but are not limited to:

* Identity Management
* Eligibility and Enrollment Management
* VistA adapters
* VistA patches
* Military Information Services
* Disability Rating Services
* Enterprise Service Bus (ESB)

MASS will use the VA-provided architectures and design patterns. The solution shall connect MASS, databases, existing and future VA applications and IT resources, successfully mediate their incompatibilities, orchestrate their interactions, and make them broadly available as discoverable services on the VA provided Enterprise Service Bus. This includes the integration for new capabilities, web services, and other technologies; including but not limited to current and future batch files, application servers, middleware products, and packaged applications in support of MASS.

* + 1. **VA SYSTEMS**

MASS shall integrate with existing and to be developed VA Systems required to provide the necessary data to support the scheduling solution.

The diagram below depicts the projected system boundaries for MASS.

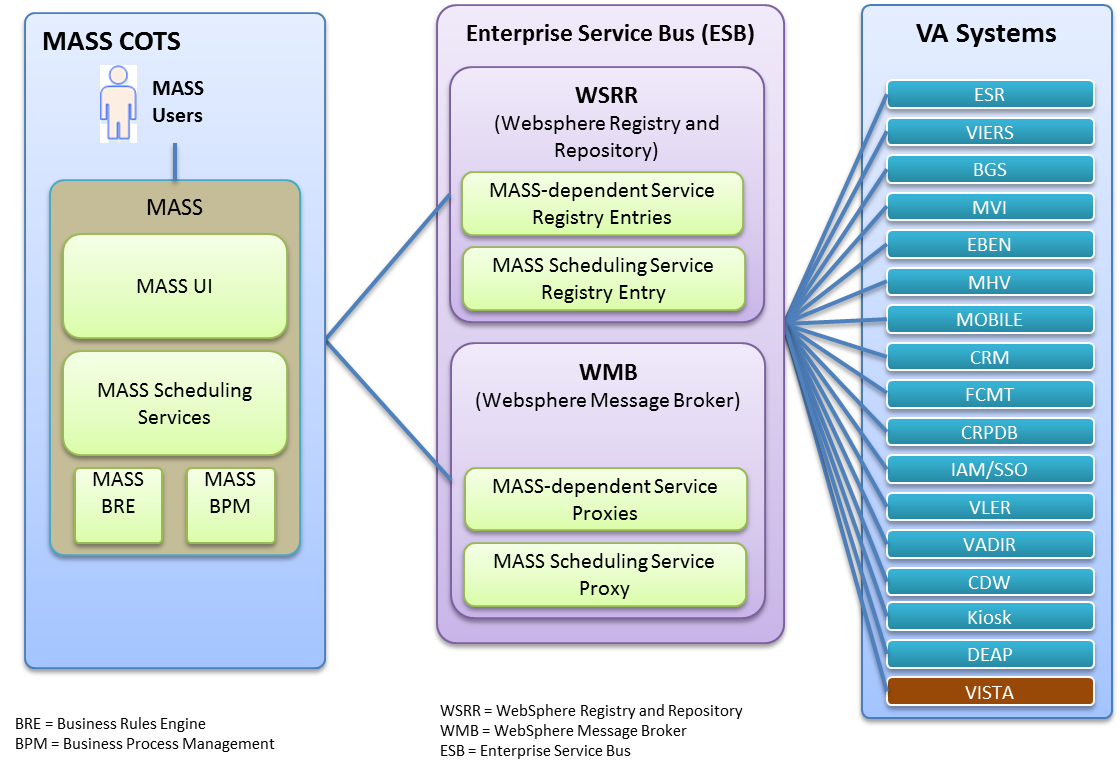
****

Figure 3. MASS System Boundaries

The VA enterprise wide area network (WAN) provides connectivity to all VA business units, such as VHA, VBA, NCA, etc. In addition, the network provides connectivity to all internal VA datacenters, and four Internet facing TIC gateways. All business partners external to VA enter the VA intranet via a Business Partner Extranet (BPE). The VA gateways also support connectivity to Tier 1 Internet providers, and host Virtual Private Network (VPN) access from external authorized users.

VA utilizes GSA NETWORX Universal Carriers to provide dual carrier fault tolerant MPLS WAN services that provide connectivity between the various VA business units, facilities, data centers, and national TIC compliant gateways. The VA intranet Specific WAN performance parameters for latency, jitter, and packet loss conform to the GSA NETWORX SLA as published under the GSA document. <http://www.gsa.gov/graphics/fas/NetworxSLAManagementGuide.pdf>

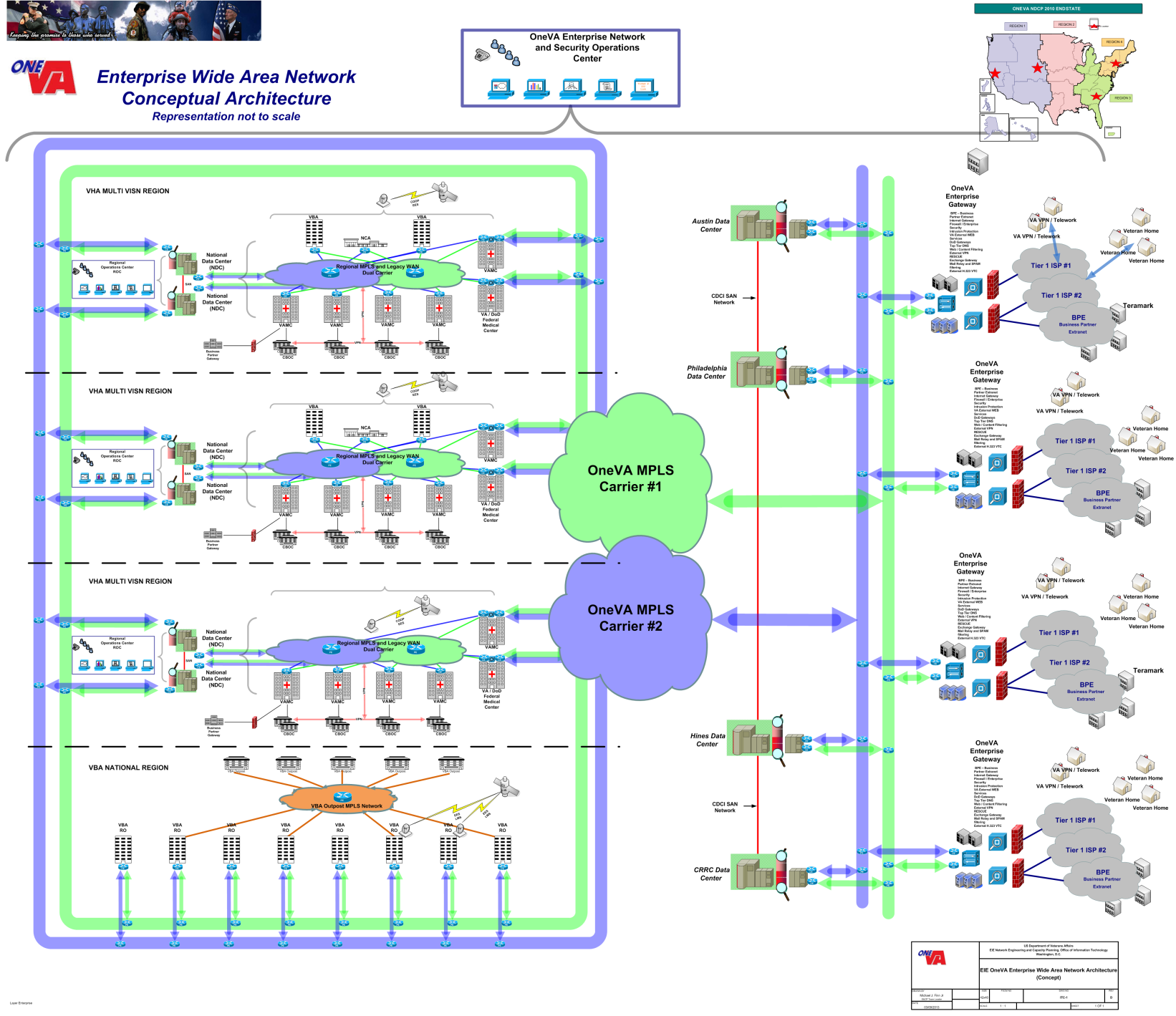
****

Figure 4: Enterprise Network Conceptual Architecture

# PERFORMANCE DETAILS

The Contractor shall provide and/or acquire the services, hardware, and software required by individual Task/Delivery Orders pursuant to the general requirements specified below throughout the period of performance.

## 4.1 CONTRACT TYPE

This is an IDIQ contract. Individual TOs shall be issued on a performance-based Firm-Fixed-Price (FFP) basis and/or Time and Materials (T&M) basis.

## 4.2 PERIOD OF PERFORMANCE

The ordering period for the basic contract shall be sixty (60) months from the effective date of award with two twelve (12) month optional ordering periods.

## 4.3 PLACE OF PERFORMANCE

The place of performance shall be identified in individual TOs. Locations will be Government or Contractor sites within the continental United States (CONUS) and/or outside the continental United States (OCONUS) at VA locations. VA locations may also include Federal, State, or military data centers, facilities, treatment facilities, health clinics and Tricare facilities as defined in individual TOs. A current map of VA locations is available at <http://www2.va.gov/directory/guide/division.asp?dnum=1>.

## 4.4 TRAVEL

Travel shall be in accordance with individual TO requirements. Travel details must be provided to and approved by the Contracting Officer’s Representative (COR) or the Government designee prior to the commencement of travel. All travel shall be in accordance with the Federal Travel Regulations (FTR). OCONUS travel may require additional authorization and approvals as specified in the individual TO. Local travel within a 50-mile radius from the Contractor’s facility is considered the cost of doing business and will not be reimbursed.

## 4.5 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format that must be electronically searchable and allow cutting and pasting of content, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media includes: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007, MS PowerPoint 2000/2003/2007, MS Project 2000/2003/2007, MS Access 2000/2003/2007, MS Visio 2000/2002/2003/2007, AutoCAD 2002, and Adobe Portable Document Format (PDF).

## FACILITY/RESOURCE PROVISIONS

The Government may 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 within 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 shall provide access to VA-specific systems/network, as required, for execution of the task via a site-to-site VPN or other technology, including VA-specific software such as VistA. 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 PWS. The Contractor shall transmit, store or otherwise maintain sensitive data or products within VA firewall in accordance with VA Handbook 6500.6 dated March 12, 2010.

## 4.7 MATERIALS, EQUIPMENT AND FACILITIES

### 4.7.1 Government-Furnished

Government Furnished Property (GFP) which includes Government Furnished Material (GFM), Government Furnished Information (GFI), and Government Furnished Equipment (GFE) may be provided if identified in the individual TO. The Contractor shall be responsible for conducting all necessary examinations, inspections, maintenance, and tests upon receipt. The Contractor shall be responsible for reporting all inspection results, maintenance actions, losses, and damage to the Government through the COR.

VA may provide VA-specific software, as appropriate and required, in individual TOs. The Contractor shall utilize VA-provided software development and test accounts, document and requirements repositories and others as required for the development, storage, maintenance and delivery of products. Contractors shall comply with VA security policies and procedures with respect to protecting sensitive data. See Section 8.0 for detailed security requirements.

### 4.7.2 Contractor-Furnished

All equipment, materials, and other property necessary to perform the work requirements and not specified for delivery to VA shall be the contractor’s responsibility.

### 4.7.3 Non-Developmental Items and Commercial Processes

Non-Developmental Items (NDI), COTS and Government-Off-The-Shelf (GOTS) products shall be used to the maximum extent possible. The Contractor shall apply commercially available and industry best processes, standards and technologies to the maximum extent possible.

### 4.7.4 Connectivity

VA will allow the Contractor use of VPN, or equivalent, as appropriate. VA may install equipment at the Contractor’s site to ensure security requirements are in place. The Contractor shall bear the cost to provide external connectivity to VA from a non-Government work site through VPN, and VA will provide the required account access accordingly. Other connectivity to VA systems may be authorized as appropriate in individual TOs.

## 4.8 SECTION 508 REQUIREMENTS

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. The Contractor shall comply with all required Federal or agency standards, as specified in the individual TO. Section 508, the Federal Information Technology Accessibility Initiative (36 CFR 1194), is incorporated into and made a part of this contract. Section 508 applies to all TOs. Specific Section 508 standards or other Section 508 requirements shall be stated in each TO. The standards and information on how to administer the Section 508 requirements are covered at <http://www.section508.gov>. Compliance with the applicable Section 508 standards is a material requirement of the contract.

## 4.9 SAFETY AND ENVIRONMENTAL

Safety and environmental procedures shall be identified in individual TOs.

The Contractor shall comply with the Office of Federal Procurement Policy Green Acquisition initiatives, as identified in individual TOs, in accordance with the policies referenced at <http://www.whitehouse.gov/omb/procurement_index_green>.

## 4.10 PMAS/PROPATH

For VA TOs, the Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality.

For VA TOs, the Contractor shall use the most current version of ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

## 4.11 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. The Contractor shall contact the TO COR as soon as possible with any issues, questions and concerns.

The Contractor shall comply with OI&T Technical Reference Model (One-VA TRM) for VA acquisitions. One-VA TRM is one component within the overall 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. Exceptions to the One-VA TRM shall be submitted to the government for approval.

Additional frameworks may be specified in individual TOs.

## 4.12 TRANSITION AND ORIENTATION SUPPORT AT END OF CONTRACT

The Contractor shall perform transition and orientation services (e.g., develop Phase-In/Phase-Out Transition Plan) to insure continuity of services as specified in the individual TOs upon completion of contract. Transition and orientation support will be needed throughout the period of performance of the contract. Activities required to transition long term operation and maintenance functions to the government or contractor personnel at the end of the period of performance will be more specifically defined in a subsequent TO.

# 5.0 SPECIFIC REQUIREMENTS, TASKS, AND DELIVERABLES

Individual TOs may encompass one or more of the tasks below. Further details are described to provide greater insight into the complexity and uniqueness of some potential TO requirements covered by this PWS. Specific task requirements are not mutually exclusive and may apply across multiple tasks. Specific requirements will be stipulated in individual TOs.

## 5.1 PROGRAM MANAGEMENT, STRATEGY, AND PLANNING SUPPORT

The Contractor shall provide Program and Project Management, monitoring and analysis, strategy, and planning support on an enterprise or individual project level. Program Management support is critical to MASS in achieving strategic goals and fulfilling mission requirements within programmatic constraints.

The Contractor shall provide support to MASS program Development Operations (DEVOPS) and Production Operations (PRODOPS).

* Development operations:  DEVOPS includes all activities from requirements identification through initial deployment into production account(s) of a capability.
* Production Operations: PRODOPS includes all activities starting once an initial capability has been developed through the life cycle of that capability.

**5.1.1 CONTRACT PROJECT MANAGEMENT PLAN**

The Contractor shall draft a Contract Project Management Plan (CPMP) following ProPath guidelines which will include the approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial CPMP is required at the kickoff meeting. After the initial CPMP is approved by the government, the Contractor shall update it quarterly.

**Deliverables**:

1. Contract Project Management Plan

### 5.1.2 SOFTWARE CONFIGURATION MANAGEMENT

The Contractor shall participate in the MASS Program Change Control Board, and comply with all MASS Change and Configuration Management plans and policies. The Contractor shall monitor and collaborate with VA to identify changes in VistA that would affect MASS. The Contractor shall develop and maintain Software Configuration Management documentation and institute required change management processes.

### 

### 5.1.3 ORGANIZATIONAL CHANGE MANAGEMENT

The Contractor shall develop and maintain an Organizational Change Management Strategy focused on optimizing user acceptance and technology adoption of the MASS Program.  The Contractor shall define a workforce transition approach; assess current and future scheduling system roles and competencies to create position descriptions needed to successfully adapt to the new system and processes.

The Organizational Change Management Strategy shall address this assessment, preparation for the change, any impacts associated with the change, and steps for execution.

### 5.1.4 INTEGRATED PROJECT/BUSINESS TEAM SUPPORT

The Contractor shall provide Subject Matter Expertise to Integrated Project Teams (IPTs), Integrated Business Teams (IBTs) and any other ad hoc meetings at the discretion of the Government PM or designee as necessary to support the objectives of the MASS program. IPTs and IBTs are cross-functional teams that work collaboratively to develop strategies and approaches to meet particular objectives. IPTs and IBTs bring together the principal stakeholders and focus efforts on establishing critical elements of all phases of the project life cycle. As necessary, the Contractor shall prepare agendas, other required project artifacts, and capture meeting minutes.

## 5.2 MASS STRATEGY AND PLANNING

The Contractor shall provide services that facilitate strategic decisions for MASS with respect to its current and future IT structure and program integration. This includes conducting and/or collaborating with Program Management Office (PMO) resources to perform systematic assessments and redesign of the key technologies, business processes, and organizational structures; streamlining processes, properly aligning the organization to reflect the way work gets done, and deploying proven supporting technologies where appropriate. The outcome of future studies and assessments may contribute to an overarching IT strategy, aligned with business goals and objectives that leverage innovation to define new opportunities for success. The outcome of studies and assessments may also serve as a critical input into designing a set of metrics, which are measureable objectives related to the overall IT strategy and operations.

### 5.2.1 REQUIREMENTS ELABORATION, ANALYSIS and VALIDATION SUPPORT

The Contractor shall provide agile requirements elaboration and analysis support as required by individual TOs. Requirements elaboration shall be structured to meet the incremental delivery needs of MASS.  Requirements support may include, but is not limited to:

* Enterprise requirements/architecture analysis and elaboration
* Business and Application architecture
* Business Process Reengineering
* Alternatives of Analysis and Feasibility studies
* Requirements planning and management
* Requirements gathering, analysis, and elaboration
* Use Case analysis and elaboration
* Peer Reviews
* Business Process Modeling

### 5.2.2 STUDIES AND ANALYSES

The Contractor shall perform and document studies and analyses to support the MASS project, as required by individual TOs. Such studies/analyses may include, but are not limited to logistics/supportability, design and engineering, operations and implementation, and business processes. The Contractor shall perform the evaluation of unproven technology applications and identification of potential risks. The development of pre-production or COTS-based prototypes may be required.

## 5.3 MASS Prototyping Environments

The Contractor shall establish, maintain, and/or collaborate within MASS prototyping environments. The MASS prototyping environments shall provide a MASS application environment to support the MASS program to include but not limited to:

* Functional and nonfunctional requirements validation
* Operational configuration(s) and set up
* Business rules development
* Application/interface design
* Performance modeling
* Development and user/SME training and feedback
* Integration with VA enterprise systems and services
* Integration with external provider systems

Examples of environments are:

* Vendor hosted prototypical environment
* VA hosted prototypical environment (outside the VA firewall)

## 5.4 MASS Systems/Software/HARDWARE Engineering

The Contractor shall provide engineering expertise to analyze system concept, system design and interoperability, and provide recommendations for optimization of the MASS solution.

The Contractor shall provide systems/software engineering support for any or all phases of the MASS system/software lifecycle to include Requirements Development, Requirements Management, Use Case Development, Risk Management, Architecture Design, Performance Engineering, Capacity Planning, System/Software Development, Test and Evaluation, and Sustainment.

During the lifecycle process, hardware and software engineering support includes, but is not limited to design, software system reliability assessments, participation on governance boards and IPTs. The Contractor shall ensure the dependencies, interoperability, availability, reliability, maintainability and performance of the system as a whole within government provided guidelines as specified in the individual TOs.

The Contractor shall install, configure, patch, repair, upgrade, or remove servers, server components and operating systems as necessary.

This area will also include efforts related to analysis of any MASS software and hardware products to determine the gaps in meeting VA needs and analysis of the best ways of meeting those needs.

### 5.4.1 MASS DESIGN AND DEVELOPMENT

The Contractor shall provide services with respect to all aspects of the MASS project life-cycle which includes, but is not limited to planning, requirements analysis, design, coding and unit testing, system integration testing, implementation, maintenance and updating of systems, applications, and/or services. The Contractor shall be fully cognizant of the implications of the VA strategic plan. The contractor shall adhere to the VA Server Virtualization First Policy: <http://trm.oit.va.gov/files/Server_Virtualize_First_Policy.pdf>

The Contractor shall follow an Agile methodology supported by Continuous Development, Continuous Integration, automated testing utilizing Test Driven Development methodologies.

VA is committed to leveraging open source capabilities when and where feasible, and to the extent appropriate, the Contractor’s MASS solution design and development shall consider and/or support open-source contributions from the Open Source community.

### 5.4.2 MASS ARCHITECTURE DEVELOPMENT

The Contractor shall support MASS Architecture enhancement and elaboration. The Contractor shall ensure that the recommended MASS architecture is in alignment with the VA EA and its design patterns. The Contractor shall coordinate and collaborate with system and application development teams to ensure successful MASS integration with "as-built" solutions. The Contractor shall coordinate and collaborate with enterprise, segment, and portfolio architecture teams across VA to ensure coordinated solutions and roadmaps. The Contractor shall support OI&T Office of Architecture Strategy and Design (ASD) infrastructure assessments concerning scheduling.

### 5.4.3 MASS SYSTEM/SOFTWARE INTEGRATION

The Contractor shall provide systems/software integration support to include but not limited to planning, updating architecture models, interoperability specifications and analysis, system interface specifications, service definitions, and segmented architecture for the transition, integration, and implementation of the MASS project.

The Contractor shall design and develop interfaces between internal and external application systems and the databases they will access and identify needed processes and structures to ensure proper MASS system performance. Interface design shall be documented in the VA Interface Control Document per ProPath, including interface architecture diagrams.

The Contractor shall develop and deliver integration software (i.e., interfaces between various GOTS, COTS and Custom software) using the Agile Software Development Methodology. This shall include all aspects of the Agile Methodology, within systems and interface documentation, including integration test case development, requirements verification, management, package technical design, development, test, product delivery and documentation.

**5.4.4 MASS Database Design, Standardization and Management**

The Contractor shall provide services and subject matter expertise to support the data design and implementation of a national VA MASS scheduling solution. All data management and implementation work (e.g. data schema, data migration, etc.) shall become the intellectual property of VA. The Contractor shall integrate information from multiple scheduling solutions into a single database per the approved architecture.

### 5.4.4.1 DATA MIGRATION

Data Migration services in support of the MASS program shall be provided as specified in individual TOs.

## 5.5 Test & Evaluation

The Contractor shall provide Test and Evaluation (T&E) support in all phases of the MASS development and operational life cycle, to include preparation of test plans and procedures, design tests cases, conduct tests, witness tests and provide technical support, coordinate test plans in accordance with appropriate regulations, and analyze/evaluate/document test results. The Contractor shall participate in technical analyses, code reviews and other reviews as required.

The Contractor shall provide testing activities in support of continued development, enhancement, and deployment of MASS capabilities within an Agile development methodology.

The Contractor shall provide support to develop, execute, and track all testing efforts to support the end-to-end development, deployment, and maintenance of the solution and shall work with designated VA Subject Matter Experts to develop, enhance, and maintain the necessary testing artifacts, including test plans, test procedures and test scripts for all releases required during this Period of Performance. These testing artifacts shall be produced for each of the defined test types/milestones supporting MASS, as may be applicable to the functionality delivered and/or the impact to the production environment.

## 5.6 Independent Verification and Validation (IV&V) SUPPORT

The Contractor shall support the review, evaluation, validation and verification procedures and methodologies used in developing, testing, maintaining and securing the MASS solution.

## 5.7 CYBER SECURITY

The Contractor shall define and deliver strategic, operational and process aspects of cyber security solutions. The Contractor shall ensure adequate Local Area Network (LAN)/Internet, data, information, and system security in accordance with organization standard operating procedures, conditions, laws, and regulations.

### 5.7.1 Information Assurance (IA)

The Contractor shall follow all applicable organization policies and procedures governing information security, including compliance with VA mandated protection of Personal Identification Information (PII) and Personal Health Information (PHI). The Contractor shall ensure that security controls in VA Handbook 6500 Appendix F (Access to Federal Information and Information Systems), SP 800-53 controls for Federal information systems as well as VA specific requirements, are implemented.

The Contractor shall identify, mitigate and resolve IA issues and concerns, including existing and newly identified information system vulnerabilities.

The Contractor shall develop/contribute to guidelines/plans/policies, analyses and reviews that require IA expertise in areas including but not limited to assessments, monitoring, maintaining, reviewing and processing, assessment/authorization, and other cyber security related activities and mandates.

### 5.7.2 Logical Security

The Contractor shall establish, using National Institute Standards and Technology (NIST) Special Publications as a guide, secure logical and physical infrastructures for Information Systems (IS) environments including, but not limited to security plans, risk assessments, access controls, directory services, security management, compliance monitoring, vulnerability scanning systems, firewalls, intrusion prevention, intrusion detection, anti-virus tools, privacy impact assessment, and PII and other data protection policies. This function includes providing details for security awareness training, personnel security, policy enforcement, incident handling procedures, and separation of duties within an organization. In addition, the Contractor shall recommend and implement current best practices for the widest range of operating systems, databases, networks, and application security (including mobile applications), implementing current best practices, industry standards, and Government regulations and policies.

### 5.7.3 Security Operating Support

The Contractor shall participate in security functions required to ensure the confidentiality, integrity and availability of computer systems including, but not limited to, security safeguard reviews, audits, reporting suspected security violations, acting to secure system environments, monitoring and responding to computer security alerts.

The Contractor shall support investigations related to Litigation Holds and Office of Inspector General.

### 5.7.4 Assessment and Authorization

The Contractor shall provide Assessment and Authorization (A&A) support to ensure the MASS project receives the appropriate security Authorizations by VA’s Designated Approving Authority (DAA). The Contractor shall ensure all security assessments are completed using VA provided tools to include the RiskVision OpenGRC security assessment. The Contractor shall support vulnerability scanning conducted by the Network Security Operations Center (NSOC). The Contractor shall develop and submit all required security document artifacts.

The Contractor shall obtain commercial and/or organization specific certifications/authorizations for new or modified MASS systems, applications, designs, equipment or installations in accordance with applicable organization standards specified by individual TOs. Specific activities include, but are not limited to

security certifications, or comprehensive assessments of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly.

The Contractor shall ensure any findings produced as a result of the security assessments are remediated in order to support A&A. The Contractor shall ensure all other security requirements are met specific to the Federal Information Processing Standard (FIPS) 199 categorization documented as a result of the Risk Assessment and applicable VA policy. The Contractor shall ensure all requirements of the A&A Standard Operating Procedure (SOP) are met, specific to the MASS project type**.**

The Contractor shall provide the services and account for the need to support all certifications/ratings to include Federal Information Security Management Act (FISMA) High.

## 5.8 HARDWARE, SOFTWARE, LICENSE, AND MAINTENANCE PROCUREMENT

The Contractor shall acquire and maintain all necessary commercial, Open Source, and third party hardware and software agreements to include licenses, warranties, and/or commercial maintenance agreements for use on all MASS hardware and software as appropriate.

## 5.9 INSTALLATION, CONFIGURATION AND IMPLEMENTATION

The Contractor shall deploy/implement the Government approved MASS solution to each facility and VISN for each MASS capability increment. The implementation may include Initial Operating Capability IOC, Alpha, and Beta sites, as well as the national rollout. This includes, at a minimum, performing the Installation, configuration, documentation and training tasks on-site or remotely, as defined in the specific TO requirements.

Installation and configuration is defined as setting up the MASS solution in a targeted environment or site, installing all required HW and SW and applying all applicable configurations. The Contractor shall also support the MASS Solution for non-production environment installations such as the prototyping, Development, Quality Assurance, Integrated Test, Release/Change Management, etc.

The Contractor shall develop and execute a strategic implementation to include the planning, installation and configuration of each MASS solution increment as defined in each TO. This shall include all technical and operational services necessary to support the planning and implementation of an enterprise MASS deployment such as detailed integrated deployment schedules, site surveys, site specific requirements/architectures, training, shipping receipt/acceptance, integration and set up, thru operational check out and post deployment evaluation/modification and support. The Contractor shall coordinate with the MASS VA Implementation Manager and other planning, site, and service representatives to plan and execute system and component deployments. The contractor shall document the pre and post deployment implementation efforts as required in each TO.

After implementation, the Contractor shall provide sustainment support for all implementations of the MASS COTS application. Specific tasks and requirements will be identified in the individual TOs.

## 5.10 Operations and Maintenance (O&M)

The Contractor shall operate, repair, and maintain systems, applications, and IT environments in support of MASS and/or system components for production environments. This includes but is not limited to, preventive maintenance and scheduled maintenance, activities to retain or restore systems (such as testing, measurements, replacements, and adjustments), and other routine work required to maintain and/or enhance IT systems. Environments requiring O&M tasks may include pre-production, production, test, training, disaster recovery/fail over, hosting, or any other combination of IT accounts. The Contractor may also be required to provide software, platform, telecommunications and storage as a service through a subscription or other means. The Contractor may also be required to recommend best practice for requirements analysis, planning, design, deployment and ongoing operations management and technical support. The Contractor shall also maintain a current and up-to-date library of all operational documentation, logs of operational events, maintenance of operational monitoring and management tools, operational scripts and operational procedures.

Software maintenance includes all activities starting once an initial capability has been developed through the life cycle of that capability.  Software maintenance includes all adaptive, perfective, and defect maintenance.   Adaptive maintenance activities are those required to adapt software and systems to support changing externally initiated changes in requirements.   Examples could include, but are not limited to, regulatory changes, congressional actions, VA mandates, and changes required to maintain interoperability with key systems (internal or external to the VA).  Perfective maintenance activities are those required to increase deployed software and systems efficiency to improve performance and/or lower cost of operation.  Defect maintenance includes those activities required to identify and repair defective coding or systems post production deployment.

### 5.10.1 SYSTEMS ADMINISTRATION

The Contractor shall support IT hardware, operating systems, installation of software, monitoring and adjusting system performance, application of patches, security updates and service packs, repairs and upgrades of IT hardware associated with the MASS project. The Contractor shall monitor system resources such as processor, memory and disk utilization using automated monitoring tools, monitor system logs, create system backups, schedules and tape allocation, establish/maintain access authorizations, perform installations, upgrades or replacements as required. The contractor shall specifically define the timeline for patching systems as defined in VA 6500.

### 5.10.2 DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

The Contractor shall provide services related to any and all methodologies pertaining to disaster recovery and business continuity for the MASS project. The range of recovery services under this functional area covers the spectrum from partial loss of function or data for a brief amount of time to a “worst-case” scenario in which a man-made, natural disaster, or IT failure results in the loss of the entire IT enterprise. Services may be required during any timeframe from initial declaration of a disaster to final recovery of all business processes.

### 5.10.3 CAPACITY/AVAILABILITY PLANNING AND MANAGEMENT

The Contractor shall perform analysis to ensure that IT capacity meets current and future business MASS and VA requirements in a cost-effective manner. The Contractor shall monitor availability and maintenance obligations to sustain IT service-availability to support business in a cost-effective manner.

### 5.10.4 TIERS I, II, III, AND HELP DESK SUPPORT

The Contractor shall deliver the full array of services, staff, and expertise to operate and maintain Service Desk/Help Desk/Call Center functions as specified in individual TOs. This shall include all Tier I, Tier II, and Tier III support up to 24/7/365. This shall include any technical as well as customer help support system.  Service-level requirements, metrics and other specifics shall be defined in each TO.

### 5.10.5 IT SERVICES MANAGEMENT GUIDANCE

The Contractor shall be responsible for recommending and supporting the development and implementation of IT service management plans, practices, infrastructures and systems using industry best practices to minimize negative impact of the MASS project on the IT enterprise. IT services management includes, but is not limited to:

* Application Administration
* Application Architecture
* Application Development
* Asset Management
* Availability Management
* Build Management
* Business (Service) Continuity Management
* Capacity Management
* Change Management
* Configuration Management
* Database Administration
* Desktop Support
* Incident Management
* Network Administration
* Problem Management
* Program Management
* Project Management
* Release Management
* Security Management
* Service Level Management
* Storage Management
* System Administration

The Contractor shall manage organizational Service Level Agreements (SLA) including, but not limited to developing and monitoring SLA metrics, and establishing escalation procedures. The Contractor may be subject to Service Level Agreements (SLAs) and subsequent metrics as specified in the individual TOs. SLAs may include definitions of services, performance measurement, problem management, customer duties, warranties, disaster recovery, and other common elements. The Contractor may assist in the creation of SLAs with both internal and external stakeholders as well as third party vendors.

## 5.11 Training

The Contractor shall identify training requirements, obtain or develop training programs and conduct training for systems, applications and products at any stage of the MASS lifecycle. This includes, but is not limited to newly developed systems, as well as existing deployed systems, current systems, and any updates or changes to migrated systems. The Contractor shall develop training plans, manuals and other training documentation or training aids. Electronic training tools such as video teleconferencing and computer-based training shall be employed to enhance the effectiveness of training materials and courses. The Contractor shall conduct training for personnel to ensure proper operation, maintenance and testing of systems, applications and products. The Contractor shall provide training and knowledge transfer to technicians and other staff with regard to services and associated products delivered under any functional areas described herein. The training allows personnel the ability to operate and maintain the product or process in the future.

In order to meet the objectives of MASS, end user training (throughout each Scheduling center) in tools, process and techniques is a critical component to the success of the initiative. The Contractor shall provide training for VA and associated personnel as identified in individual TOs. Training will also include initial startup training at the Alpha and Beta site(s) where it is implemented (to include development and test centers) and future training for future capabilities. Scheduling application end user training, including training on GUI and application changes shall be provided as part of this contract.

The Contractor shall develop and deliver the detailed training for maximizing employee, supervisor and management adoptionof the new workflow-oriented business model.

The Contractor shall identify and/or provide any additional training required by end-users, technicians, or any other staff for implementation, maintenance and use of deliverables specified in individual TOs.

## 5.12 CONTRACT MANAGEMENT

**5.12.1 GOVERNMENT SUPPORT**

### 5.12.1.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR)

For this contract, a COR shall be designated and shall reside within the OI&T PD MASS Program Office. The COR shall be appointed by the Contracting Officer and duties delegated in an appointment letter. Contract surveillance duties shall be defined and be in accordance with the Quality Assurance Surveillance Plan (QASP).

### 5.12.1.2 COR – TASK ORDERS

For each TO a COR shall be designated and shall reside within the Requiring Activity. The COR shall be appointed by the ordering CO and duties delegated in an appointment letter. The COR is the Requiring Activity’s designated representative. The COR designated for each TO shall provide the Contractor access to all available Government furnished information, facilities, material, equipment, services, among others as required to accomplish each TO. Contract surveillance duties shall be defined and accomplished in accordance with the TO QASP.

**5.12.5 CONTRACTOR SUPPORT**

### 5.12.5.1 CONTRACTOR PROGRAM MANAGEMENT

The Contractor shall provide a Program Manager who shall serve as the manager of the contract and shall be the Contractor’s single point­ of contact for the VA COR. The Program Manager shall be responsible for formulating and enforcing work standards, assigning schedules, and reviewing work discrepancies, communicating policies, purposes, and goals of the organization to the assigned Contractor personnel for all projects. The Program Manager shall manage all TO performance. The Contractor shall be available to meet with the Government virtually or at the Government facilities within 24 hours’ notice, depending on the issue to be addressed, without added cost to the Government. This Contractor function shall handle MASS programmatic issues, facilitate information exchange, and enhance management coordination.

The Contractor shall provide the following Program Management activities and services.

1. Timely and sustained response to program issues and problems that occur during the execution of the contract as identified by the VA MASS Program Office

2. Conduct Project Progress Reviews (PPR)

3. Provide Monthly Contract Status Report

4. Perform risk management activities

### 5.12.5.2 POINTS OF CONTACT

The Contractor shall provide a list of Contractor points-of-contact to the COR no later than ten calendar days after the effective date of the Notice to Proceed. The list shall include names, telephone numbers, facsimile numbers, and areas of responsibility for the Contract, addresses, and e-mail addresses. When a key point-of-contact is replaced, the Contractor shall notify the COR no later than five workdays afterward.

### 5.12.5.3 WORK CONTROL

All program requirements to include deliverables, contract actions and data interchange shall be conducted in a digital environment using electronic and web-based applications. At minimum, such data shall be compatible with the Microsoft Office 2003® family of products, and Microsoft Windows XP® network protocols. The Government will designate a standard naming convention for all electronic submissions within 60 days after contract award. Electronic methods for the interchange of data/documents (to include deliverables and invoices) shall be required for the duration this contract.

## 5.13 GOVERNMENT RIGHTS

The Government shall have full and unrestricted rights, in accordance with copyright laws and regulations, to use and reproduce for its own use, all documentation and software provided under this contract. The Contractor shall provide the VA MASS user community with online access to, including the rights to download, search and copy in order to create derivative works, all user manuals and software reference documentation.

### 5.13.1 TECHNOLOGY INSERTION

As new technologies are developed and used by the commercial industry or the Government, VA and/or Contractor may identify these technologies, and propose necessary additions, modifications, upgrades, enhancements, and improvements to the current Contract scope. The Contractor shall translate the technology insertion recommendation into a formal Engineering Change Proposal (ECP) as directed by the CO.

All inserted products shall comply with VA Acceptance testing defined in this MASS IDIQ PWS.

The Contractor shall inform VA in advance of any known, or potential changes, in cost of ownership pursuant to technology refreshments, insertions, or other changes to the MASS. The Cost of Ownership change shall be quantified and communicated to VA at the earliest possible date.

**6.0 GENERAL REQUIREMENTS**

The deliverables defined below are required for the base contract and each TO and shall be provided in accordance with paragraph 5.12.5.3 (Work Control). The base contract report shall be a rollup of each TO and shall be delivered to the CO and the COR. Each individual TO report shall be delivered to the COTR/COR for that TO. Any differences between the requirements for the overall basic contract report versus the TO report are noted below. Each deliverable is required by the 15th day of each month.

**6.1 MONTHLY CONTRACT STATUS REPORT**

The Contractor shall prepare and submit a Status Report in Microsoft Office Excel format not less than once a month. VA may request reports more frequently, as needed. This report shall convey the status of all TOs awarded as of contract inception as well as cumulative contract performance. A standard format shall be utilized for submission of the below required information. This report is required at the basic contract level and shall be a rollup/summary of each TO. In addition, the Contractor shall provide a monthly individual TO report. The TO report shall be unique to that TO only.

A. For Each TO, indicate/discuss:

1. TO summary

2. Performance metrics

3. TO schedule

4. PMAS Compliancy (as applicable)

5. Critical items for Government review

6. Accomplishments

7. Significant open issues, risk and mitigation action

8. Summary of issues closed

9. Meetings completed

10. Projected meetings

11. Subcontractor performance – discuss 1st tier Subcontractors and Contractor performance

12. Projected activities for next reporting period

13. Explanation if the reporting period is over one month

14. Receiving report submitted

15. Milestone payment schedule

16. Automated bill of materials in data base format

17. A summary of the top risks and the mitigation activities underway

B. General and Cumulative Performance. Indicate the following:

1. Any general meetings that occurred with Government representatives during the reporting period

2. Total dollars awarded to date (ceiling)

3. Total dollars invoiced to date, by fiscal year, and since contract award

C. Performance Metrics

1. Schedule Performance to Plan

**Deliverables:**

1. Monthly Contract Status Report

**6.2 STATUS OF GFE REPORT**

This report is required at the base contract and shall be a rollup/summary of each TO. The overall base contract report shall show the detail for each TO with a summary column for the entire program. In addition, the Contractor shall provide a monthly individual TO report. The TO report shall be unique to that TO only. This report shall include:

1. TO Number

2. Project Name

3. Type of Equipment

4. Tracking Number

5. Location

6. Value

7. Total Number of Pieces

8. Total Value of Equipment

9. Anticipated Transfer Date to Government

10. Anticipated Transfer Location

11. The Government Furnished Equipment Report

**Deliverable:**

1. GFE Report

**6.3 PERSONNEL CONTRACTOR MANPOWER REPORT**

This report is required at the base contract and shall be a rollup/summary of each TO. The Contractor shall provide a Personnel Report (MS Excel), on a monthly basis listing all personnel working at a VA facility or accessing VA networks under each TO. As personnel changes occur, a revised report is required only for the individual TO affected for Background Investigations. The overall basic contract report should only be updated on the monthly basis. The overall basic contract report shall show the detail for each TO with a summary column for the entire program. The individual TO report will be unique to that TO. The information required is as follows:

1. TO Number

2. Name

3. Clearance level and/or Status

4. Company name

5. Prime/Subcontractor

6. Labor Category

7. Facility location

8. Tour of Duty Schedules (e.g. Monday through Friday, 9:00 am to 5:00 pm)

9. Project supporting

10. Contractor Rules of Behavior

11. VA Cyber Security Awareness and Rules of Behavior Training

12. Annual VA Privacy Training

13. The Personnel Contractor Manpower Report as set forth in Section D, Attachment 012(basic) and 013 (task order), shall be submitted monthly via the VA TAC website or the CO.

**Deliverable:**

1. Personnel Contractor Manpower Report

**6.4 SMALL BUSINESS PARTICIPATION REPORT**

This report is required at the base contract and shall be a rollup/summary of each TO. In accordance with Small Business Participation Requirements (reference section C, clause C.6.6), The Contractor shall submit the Small Business Participation Report on a quarterly basis to the CO.

**Deliverable:**

1. Small Business Participation Report

**6.5 MEETINGS AND REVIEWS**

For successful management and contract surveillance, the following meetings and reviews are required.

### 6.5.1 POST AWARD CONFERENCE

The Government intends to convene a Post-Award Conference within 40 days after contract award to review the PWS, business policies, and procedures, and introduce personnel. The CO shall notify the Contractor of a specific date, location and agenda within seven days after contract award.

### 6.5.2 TASK ORDER KICKOFF MEETINGS

As required by the designated COR, and CO, a kickoff meeting may be held on the TO level after award. Dates, locations, and agenda shall be specified at least five (5) calendar days prior to the meeting.

### 6.5.3 PROJECT PROGRESS REVIEWS

The Contractor shall conduct Project Management Reviews (PMRs) at the overall MASS Project/IDIQ Contract level on a quarterly basis at a facility or via virtual means as mutually agreed upon. The Contractor shall construct a PMR briefing and perform PMRs to provide the VA PM insight to cost, schedule, performance, and status of progress of all executed tasks to include the status of progress, deliverables, and project quality performance. The Contractor shall capture problems or risks and risk mitigation strategies, risk owners, and expected completion.

The Contractor shall execute program governance to provide quality oversight and controls of program, architectural, and technical aspects of the full SDLC of the MASS project.

The Contractor shall conduct the first PMR at the end of the first three month period following contract award and shall conduct subsequent PMRs every three months thereafter. The Contractor shall coordinate date, time, and support for the PMR, as required. The Contractor shall provide a Draft PMR Agenda for VA PM approval at least five business days prior to the PMR. The Contractor shall document meeting minutes and distribute to attendees within two business days following the PMR. Any other required management reviews will be documented at the task order level.

During each PMR, the Contractor shall present material that addresses:

1. Status of current technological substitutions and additions

2. Status of configuration and risk management activities

3. Status of TOs, to include but not limited to, received and processed dates (listed by Requiring Activity), scheduled delivery date, and shipped date and period of performance for services

4. Actions under warranty and maintenance

5. Significant trends (quantities by CLINs, component reliability safety issues, problems, and recommended solutions)

6. Minutes from the previous PMR

7. Activities determined to be of importance to VA, such as unanticipated problems, and high visibility issues identified by VA;

8. Status of significant program events

9. Customer feedback

10. VA organizations contacted and initiatives with each; and

11. Reasons for delinquent TOs

12. A report on current risks and risk mitigation activities

**Deliverables**:

1. Contract Quarterly Project Management Review Brief
2. Contract PMR Agenda and Minutes

### 6.5.4 ORGANIZATIONAL CHART

The Contractor shall include in each review, a current organizational chart that includes the names and telephone numbers of all key Contractor personnel, and any key personnel changes highlighted. The Contractor shall prepare and coordinate with the COR, an agenda for all PPRs at least five workdays before a scheduled PPR. The Contractor shall provide the briefing charts to the COR electronically at least three workdays prior to the day of the PPR. The Contractor shall prepare and coordinate minutes of the PPRs with COR no later than five workdays after the PPR. Coordination shall be done through electronic mail. Upon COR approval, the Contractor shall, have no more than five workdays to distribute electronic copy of the minutes to COR and CO.

**Deliverable:**

1. Organizational Chart

### 6.5.5 PRIMAVERA

The MASS Program uses Primavera as its program and project planning, scheduling and resource tracking program and project management information system. The Contractor shall use Primavera to plan, execute, monitor, and control its resources and TOs. Contractor’s staff members shall become resources in Primavera, participate in developing and defining activities used in Primavera, and complete Primavera Progress Reporter worksheets on a weekly basis. The Contractor shall work with the MASS PMO Planner to develop and have approved Work Breakdown Structures (WBS) in Primavera. The Contractor shall provide initial recommended WBS structures and activities for infrastructure development and COTS scheduling application integration. The Contractor shall make weekly recommended updates to WBS structures and activities for infrastructure development and COTS scheduling application integration. The Contractor shall make daily updates to the MASS PMO Primavera Planner on MASS program activities assigned to Contractor resources. The Contractor shall complete weekly Primavera timesheets for Contractor resources.

**Deliverables:**

A. Primavera Progress Reporter Worksheets

B. Work Breakdown Structures in Primavera – initial and weekly updates

C. MASS PMO Primavera Planner Daily Updates

D. Weekly Primavera Timesheets

### 6.5.6 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 the following: 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 BI-Weekly PD Status 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”.

**Deliverable:**

1. VA Privacy and Information Security Training Certificates

### 6.5.7 PRODUCT DATA

The Contractor shall review, develop and/or submit Product Data that shall be identified in individual TOs as deliverables. Product Data may define configuration items, associated processes and procedures, and other items throughout the applicable life cycle. Various types of Product Data, including engineering drawings, specifications, software configuration documentation, interface control documentation, quality assurance provisions, and/or commercial item descriptions may be required. The Contractor may be required to apply Computer-Aided Design (CAD), and Computer Automated Engineering (CAE) methods/systems to support concurrent design integration with manufacturing and logistics considerations. Product Data may include, but is not limited to:

* Complete design disclosure
* Form, fit and function requirements
* Performance specifications

**7.0 DELIVERABLES**

**7.1 Products**

All products shall be delivered to the Government locations and accepted by authorized Government personnel as specified in the individual TO. Inspection and acceptance criteria shall be specifically identified in each TO. The COR shall be notified of any discrepancies found during acceptance inspection upon identification.

**7.2 Data**

The preliminary and final deliverables and all associated working papers, application source code, and other material deemed relevant by the Government which has been generated by the Contractor in performance are the exclusive property of the Government or as specified in the individual TO. Request for deviation shall be approved by the CO. Data rights for all final deliverables and working papers shall be in accordance with the individual TO.

**8.0 SECURITY**

**8.1 Systems Security**

The Contractor shall comply with all the physical and data security policies of the ordering activity.

**8.2 Personnel Security**

The Contractor shall comply with all personnel security requirements included in this contract and any unique organization security requirements described in each TO.

**8.2.1 Position Risk Level and Contractor Personnel Security Requirements**

1. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access will be determined at the TO level. It is anticipated there may be requirements at the Low, Moderate, and High levels for this contract. The levels of access are:

| **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** | **Minimum 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. |

Contractor Responsibilities:

a. 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.

b. The Contractor shall bear the expense of obtaining background investigations.

c. For a Low Risk designation the following forms are required: 1.OF-306 and either 2. DVA Memorandum – Electronic Fingerprints or FD-258 Fingerprint card. For Moderate or High Risk the following forms are required: 1. VA Form 0710 and either 2. DVA Memorandum – Electronic Fingerprints or FD-258 Fingerprint card. These should be submitted to the CO or COTR after award has been made.

d. Within 3 days after award, the Contractor shall provide a staff roster to the CO and COTR to enable the initiation of the Electronics Questionnaire for Investigations Processes (e-QIP) to begin their background investigations.

e. The Contractor personnel will receive an email notification from the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85 or SF85P). 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).

f. The Contractor is to sign the signature page and send to the COTR and CO for electronic submission to the Security and Investigations Center (SIC).

g. 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.

h. If the background investigation is not completed prior to the start date of the contract, the Contractor employee may work on the contract once the investigation has been initiated and sent to the OPM. 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 databases of either the OPM or the Defense Industrial Security Clearance Organization (DISCO).

i. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration in working under the contract.

j. Failure to comply with the Contractor personnel investigative requirements may result in termination of the contract for default.

**8.2.2 Security Requirements**

The following security requirement must be addressed regarding Contractor-supplied computer equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. (i.e. any device capable of processing or storing digital data) for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include:  a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) Equipment will meet all sanitization requirements and procedures before disposal as per VA policy (hard drives will not be returned). The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

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

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

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

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

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

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

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

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

10. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is to be determined at the TO level.

**8.3 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).

**8.4** **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 | 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.

**8.5 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.

**ADDENDUM A**

**A1.0 Cyber and Information Security Requirements for VA IT Services**

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.  The Contractor’s firewall and web server shall meet or exceed VA minimum requirements for security.  All VA data shall be protected behind an approved firewall.  Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible.  The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE).  Security Requirements include:  a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal.  The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, “Contract Security,” March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, “Contract Security” shall also be included in every related agreement, contract or order.  The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at [https://www.tms.va.gov](https://www.tms.va.gov/). If you do not have a TMS profile, go to <https://www.tms.va.gov> and click on the “Create New User” link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

**A2.0 VA Enterprise Architecture Compliance**

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP).  VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

**A2.1 VA Internet and Intranet Standards:**

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor’s work includes managing, maintaining, establishing and presenting information on VA’s Internet/Intranet Service Sites.  This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): <http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2>

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): <http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2>

**A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements  (Section 508)**

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees.  Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

**Section 508 – Electronic and Information 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: <http://www.section508.gov> and <http://www.section508.gov/acquisition-regulations>. A printed copy of the standards will be supplied upon request.  The Contractor shall comply with the technical standards as marked:

\_x\_§ 1194.21 Software applications and operating systems

\_x\_§ 1194.22 Web-based intranet and internet information and applications

\_x\_§ 1194.23 Telecommunications products

\_x\_§ 1194.24 Video and multimedia products

\_x\_§ 1194.25 Self contained, closed products

\_x\_§ 1194.26 Desktop and portable computers

\_x\_§ 1194.31 Functional Performance Criteria

\_x\_§ 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

**A4.0 Physical Security & Safety Requirements:**

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property.  Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed.  It is the responsibility of the Contractor to park in the appropriate designated parking areas.  VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

**A5.0 Confidentiality and Non-Disclosure**

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access toProtected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”).  Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA.  These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA.  Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38.  Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information.  Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities.  Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract.  Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature.  If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract*,*the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information.  Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives.  The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements.  All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none.  The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
17. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed.  In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

**ADDENDUM B**

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

**B1 GENERAL**

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

**B2 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS**

* 1. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
  2. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
  3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.
  4. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.
  5. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor’s employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

**B3 VA INFORMATION CUSTODIAL LANGUAGE**

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor’s information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA’s sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Destruction of sensitive paper document must be accomplished by following VA Directive 6371.Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.
4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
9. The Contractor/Subcontractor’s firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.
10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.
11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.
12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

**B4 INFORMATION SYSTEM DESIGN AND DEVELOPMENT**

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.
2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.
3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.
4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.
6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
7. The Contractor/Subcontractor agrees to:
   1. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:
      1. The Systems of Records (SOR); and
      2. The design, development, or operation work that the Contractor/Subcontractor is to perform;
   2. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and
   3. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR
8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.
   1. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.
   2. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
   3. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.
10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.
11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.
12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

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

* 1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor’s security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.
  2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.
  3. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor’s systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.
  4. The Contractor/Subcontractor’s system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.
  5. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.
  6. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.
  7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.
  8. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1. Vendor must accept the system without the drive;
2. VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
3. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
4. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
5. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
6. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
7. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

**B6 SECURITY INCIDENT INVESTIGATION**

* 1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.
  2. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.
  3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.
  4. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

**B7 LIQUIDATED DAMAGES FOR DATA BREACH**

* 1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.
  2. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.
  3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
     1. Nature of the event (loss, theft, unauthorized access);
     2. Description of the event, including:
     3. date of occurrence;
     4. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
     5. Number of individuals affected or potentially affected;
     6. Names of individuals or groups affected or potentially affected;
     7. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
     8. Amount of time the data has been out of VA control;
     9. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
     10. Known misuses of data containing sensitive personal information, if any;
     11. Assessment of the potential harm to the affected individuals;
     12. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
     13. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
  4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
     1. Notification;
     2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
     3. Data breach analysis;
     4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
     5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
     6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

**B8 SECURITY CONTROLS COMPLIANCE TESTING**

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

**B9 TRAINING**

1. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
   * 1. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
     2. Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
     3. Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;
     4. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
     5. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access
2. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

**ADDENDUM C**

This addendum contains system level technical specifications for the Medical Appointment Scheduling System (MASS). Due to the nature of the data and information traversing the MASS solution as well as availability requirements, this solution is expected to be assigned the security classification of FISMA High. The vendor solution shall meet the following technical requirements.

### C1 Fundamental Design Requirements

* Solution design shall support dual stack IPv4.
* 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 solution shall be designed and configured such that components related to the system (not DR components) which transfer data within the system during it’s normal operations (e.g. web server communicates with database backend, e.g. user authentication and user workstation to server data transfers are performed by one component and then data is transferred to separate database server) must be designed/configured such that the traffic between servers remains on the same local area network.

### C2 Continuous Availability

Downtime: Any time in which a service is not available to end users. Furthermore, any redundant components that fail while the application remains in service are not counted as downtime.

Total Application Uptime: Total time in measurement period minus scheduled downtime

Scheduled Downtime: Scheduled downtime is any change in which is identified and planned.

Unscheduled Downtime: Any time the service is unavailable due to unplanned events. This includes the following:

1. MASS Releases that exceed their scheduled downtime deployment window.

2. System Recovery due to failed installation process.

3. Failure of a component that renders one or more services unavailable

4. Application unavailability due to improper redundancy configuration.

5. Any Degraded business service performance due to an inability of the system to meet stated service level requirements for any business service designated as a Key Performance Indicator.

Availability Calculation:

Availability Percentage= [(Total Application Uptime-Unscheduled Downtime)/Total Scheduled Uptime]\*100%

MASS will be a critical component to the delivery of Veteran care. MASS shall deliver a target level 99 % availability with a target goal of 99.9% to end user experience. The vendor solution architecture must support application level high-availability above the hypervisor with a design that mitigates single points of failure from the system. Should this solution be externally hosted, the entire solution shall demonstrate 99.9% availability rating. For VA Internal hosting, the Enterprise Operations data centers provide a fully redundant, highly available IAAS solution that provides a standard Disaster Recovery Service utilizing storage replication. It is desired that this application be continuously available across two data centers that can be located up to 1500 miles apart.

At a minimum, the architectural design shall provide a 99.9% availability solution at the local level. The design shall eliminate single points of failure within the MASS infrastructure.

### C3 Disaster Recovery

The MASS solution shall comply with VA Enterprise Disaster Recovery Service Tiers and Technology Solutions Standards:

http://trm.oit.va.gov/files/VA\_Enterprise\_Disaster\_Recovery\_Service\_and\_Technology\_Standards.pdf

### C4 Integration with ESB SOA Architecture

The MASS Solution shall integrate the VA provided ESB and utilize VISTA Messaging to the maximum extent possible Network Requirements.

### C5 Storage Requirements

The MASS solution shall comply with the storage requirements within attachment “MASS Storage Requirements”.



### C6 Enterprise Monitoring

The MASS solution shall provide native/out of the box integration with the VA Enterprise Monitoring Suite. The tools that are currently in use by VA for Enterprise Monitoring are:

* Aternity Desktop Performance Monitoring (www.aternity.com) – agents deployed on the end user desktop monitoring the application transactions and the desktop performance.
* Bluestripe FactFinder ([www.bluestripe.com](http://www.bluestripe.com)) - operations view across a system to reveal hidden communications/hidden items that you don’t know are occurring which include essential infrastructure elements (for example: DNS, authentication services, etc.).
* www.appdynamics.com – provides on premise monitoring at the application and database layers and provides SAAS monitoring.
* http://arcturustech.com – heap tuning plus application and database monitoring similar to Appdynamics and CA APM
* www.xpolog.com – log management and analysis. This is specifically focused on application layer analysis as opposed to Splunk which has its roots in Security and Network logs.
* And a very large suite of products from CA including
  + CA Spectrum and eHealth
  + CA Application Delivery Analysis (formerly NetQoS, provides an application transaction view of network performance and health)
  + CA Service Operations Insight

Should components for this application of the MASS solution be hosted in a private, external environment, the Contractor shall provide an Application Performance Management suite that has the capability of interfacing with the enterprise management solution.

### C7 Identity and Access Management (IAM)

COTS product(s), software configuration and customization, and/or new software development must be compliant with the VA Enterprise Technical Architecture (ETA), specifically for compliance and integration with Identity and Access Management (IAM) requirements and IAM enterprise design and integration patterns. All Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145) and VA IAM enterprise identity management requirements. All 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 PIV and CAC.  Specific Identity and Access Management Personal Identity Verification (PIV) requirements as set forth in Office of Management and Budget (OMB) Memoranda M-04-04 <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>, M-05-24 <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>, and 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.

GFI: <http://www.techstrategies.oit.va.gov/docs_design_patterns.asp>