PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Veterans Benefits Administration
Administrative Loan Accounting Center

Centralized Administrative Accounting Transaction System (CAATS)
Development Phase III

Date: February 20, 2015
TAC-15-16502
PWS Version Number: 8.1

Contents

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Product Development (PD), Veterans Benefits Administration (VBA), Administrative Loan Accounting Center (ALAC), and National Cemetery Administration (NCA) is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely, and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

The Centralized Administrative Accounting Transaction System (CAATS) is a web-based, automated system that allows for the electronic input and approval of accounting source documents and transactions. It improves internal controls, standardizes accounting entries, produces an electronic audit trail, and maintains separation of duties.

CAATS is designed as a system of modules and sub-modules. There are currently 18 modules in CAATS and five modules in development:

1. Obligations
2. Budget
3. Payments
4. Accounts Receivable
5. Deposits
6. Cost/Revenue- Suspense Transfers
7. Accrual
8. Purchase Card
9. Manila
10. Vocational Rehabilitation and Employment (VRE) Service Group
11. Administrative Accounting Division (AAD) Workload
12. Workload Measurement
13. Loan Guaranty (LGY)
14. Paralympics
15. Benefit Debts
16. Contract Exam
17. Requisition
18. Reports
19. Recertification Accounting and Tracking System (RATS) System Administration – currently in development and planned to be completed by award of this contract
20. RATS Import/Export – currently in development and planned to be completed by award of this contract
21. RATS Workload Management – currently in development and planned to be completed by award of this contract

22. RATS Reconciliation – currently in development and planned to be completed by award of this contract
23. RATS Reports and Documents – currently in development and planned to be completed by award of this contract

All CAATS users are VA personnel at:

1. VBA field stations (Regional Offices)
2. NCA Memorial Service Networks (MSNs) and NCA field stations
3. ALAC in Austin, Texas
4. VBA Finance Center (VBAFC)
5. NCA Finance Department in Stafford, Virginia.

Users have the capability to submit various transactions, which are either approved or returned by designated staff.

CAATS interfaces with several other applications:

1. Daily interface with the Financial Management System (FMS) to keep a running total of balances (including budgetary allowances, open advances, unapplied deposits, open receivables, and open obligation data) throughout the day.
2. Nightly batch process feed to FMS with any approved CAATS transactions. The following morning, CAATS receives back from FMS a file indicating the transactions that have been accepted or rejected.
3. Daily interface with VA's Credit Card System (CCS) to obtain credit card transactions.
4. Multiple interfaces per day with VA's electronic Contract Management System (eCMS). CAATS sends requisitions to eCMS for processing and receives Purchase Orders (POs) processed by eCMS back for obligation in FMS via CAATS. Status updates are also passed back and forth between eCMS and CAATS.
5. Daily Vendor File received from the Financial Service Center (FSC) for the purpose of validating Vendor Identification Codes used on transactions.

CAATS contains a Microsoft Structured Query Language (SQL) Server database to record internal information, such as users, configurations, and access logs, as well as recording data on all events and usage of the CAATS system. The database provides for comprehensive web-based reporting using Microsoft's integrated SQL Reporting Service.

CAATS functionality is based on the Microsoft application development platform. This platform includes the following core technologies:

1. Microsoft .Net Framework 4.0 – All core business and application logic are built using the Microsoft .Net framework.

2. ASP.Net – All user interfaces into the CAATS system are web based and leverage Microsoft's ASP.Net web application platform.
3. Internet Information Services (IIS) – The CAATS web application is hosted on load-balanced Microsoft IIS servers.
4. Microsoft SQL Server 2008 – All CAATS data storage leverages Microsoft's SQL Server database system.
5. SQL Server Reporting Services – SQL Server Reporting Services is leveraged to provide highly available reporting for the CAATS application.
6. Developer Express Web Components – CAATS uses the Developer Express User Interface (UI) components to deliver a rich web UI experience as well as providing operational reporting to end users.
7. NHibernate Object Relational Mapper (ORM) – NHibernate is used for object persistence operations.
8. Microsoft Enterprise Library – Core crosscutting application operations such as logging, error handling, and database connectivity use the Microsoft Enterprise Library.
9. StructureMap – Inversion of Control (IOC) container used to implement the dependency injection pattern in CAATS. The IOC container serves both as a service locator and as a mechanism for coupling concrete class implementations with abstract interfaces at runtime.
10. Team Foundation System (TFS) provides the mechanism to create, assign, prioritize, and monitor tasks and their related software development.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, http://www1.va.gov/vapubs/
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, http://www1.va.gov/vapubs/
10. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008

11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. 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
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
19. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
20. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
25. OI&T ProPath Process Methodology (reference https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
26. Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, “Transition to IPv6”, September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006

35. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
36. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
43. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
49. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
51. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007

53. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
54. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
55. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
59. A. Software Engineering Institute, Software Acquisition Capability Maturity Model (SA-CMM) Level 2 procedures and processes
60. ATTACHMENT 1 – RATS SYSTEM DESIGN DOCUMENT (Will be provided with the solicitation)
61. ATTACHMENT 2 – CAATS PHASE III REQUIREMENTS SPECIFICATION DOCUMENT

3.0 SCOPE OF WORK

The Contractor shall provide CAATS development, testing, and release support for the CAATS software including both internal (intranet accessible) and external (internet accessible) system interfaces. The Contractor shall provide integration support to incorporate the previously developed RATS modules into CAATS. The Contractor shall also support the transition to sustainment and provide Project Management Accountability System (PMAS) support.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be 12 months from date of award with one 12-month option period. The Optional Task under PWS Section 5.10 shall not exceed a 12 month period of performance and may be exercised by the Government a single time, at any time, during the Base Period and the Option Period. The Optional Task under PWS Section 5.11 shall have a period of performance of 60 days and may be exercised by the Government a single time, at any time, during the Base Period or the Option Period.

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

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11

Christmas Day	December 25

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

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

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

The CAATS development effort under this TO shall be performed at the Austin Information Technology Center (AITC) located in Austin, Texas. The remainder of the effort (project management and the Project Management Accountability System (PMAS) support) shall be performed at Contractor facilities. The Contractor shall coordinate with the Contracting Officer's Representative (COR) in order to obtain physical and remote access to the AITC.

Normal working hours shall be 8 hours per working day within the range of 7:00 a.m. to 6:00 p.m.

4.3 TRAVEL

The Government anticipates that no travel will be required to perform the tasks required under this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following tasks and provide the cited deliverables. The Contractor shall use only VA approved software in performance of this effort. The list of approved software can be found in the Technical Reference Model (TRM).

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of this TO effort. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc

data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the TO. The Contractor shall update and maintain the VA Project Manager (PM) approved CPMP throughout the period of performance.

Deliverable:

A. Contractor Project Management Plan

5.1.2 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, NCA and VBA Business Owners, Product Owner, and the VA Program Manager.

5.1.3 PROGRESS MEETINGS

The Contractor shall attend, participate in, and support the Government hosted weekly progress meetings at the AITC to update all parties of project progress. In these progress meetings, the Contractor shall be prepared to discuss current iteration progress, participate in the planning of upcoming iterations, and sustainment progress for both the development and testing.

5.1.4 TASK TRACKING SYSTEM

The Contractor shall use the VA task tracking system (currently Team Foundation but there are plans to transition to Rational Tools at a future, but undetermined date) to enter and track newly discovered bugs and to view the status of previously discovered project defects. The Contractor shall support the tracking system transition efforts by working with the Rational Tools Team to move all data to Rational Tools. VA sponsored Rational Tool training classes are required before gaining access to the software suite. The Contractor shall track bugs/defects and maintain a Monthly Defect Report providing, at a minimum; a bug/defect description, planned/current actions taken to date, and current status.

The Contractor shall update the VA task tracking system (Team Foundation/Rational Tools suite) on a weekly basis as required.

Deliverable:

A. Monthly Defect Report

5.1.5 PRODUCT DEVELOPMENT (PD) REPORTING REQUIREMENTS

The Contractor shall deliver Bi-Weekly (every two weeks) PD Status Reports. These reports shall provide accurate, timely, and complete project information supporting PD

reporting Requirements. The Bi-Weekly PD Status Report shall include the following data elements:

a. Project Name and TO Name
b. Overview and description of the TO
c. Overall high level assessment of TO progress
d. All work in-progress and completed during the reporting period
e. Identification of any TO related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
f. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
g. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
h. Work planned for the subsequent four (4) reporting periods, when applicable
i. Current TO schedule overlaid on original TO schedule showing any delays or advancement in schedule
j. Current definition of user requirements / function points overlaid over the original function points and the last reported function points to specifically identify changes in the function points to be delivered since the previous report.
k. Current expenditures overlaid over the original budget showing any deviations in the actual expenditures versus the original budget and versus the current budget for Cost and Time and Materials type contracts. For Firm Fixed Priced efforts provide expenditures based upon your proposed spend plan.
l. Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. After the initial labor baseline is provided, each Bi-Weekly PD Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract.
m. Original schedule of deliverables and the corresponding deliverables made during the current reporting period.

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

Deliverable:

A. Bi-Weekly PD Status Report

5.1.6 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; 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:

A. VA Privacy and Information Security Training Certificates

5.2 CAATS DEVELOPMENT (BASE PERIOD AND OPTION PERIOD)

In the performance of these tasks, the Contractor shall review, validate, update, and refer to the CAATS Architectural Manual Version 5 document and review and refer to the CAATS Training Manual Version 6 document provided by VA throughout the period of performance.

The CAATS development shall be based on an iterative, agile software process resulting in a new production release bi-monthly (every other month). An increment shall include at least two bi-monthly production releases. There shall be at least two modules included in each increment. The modules to be developed are listed below. Five modules shall be developed in the base period and, if exercised by the Government, the Contractor shall develop the remaining five modules in the option period.

The Contractor shall use only VA TRM compliant software in their development. The Contractor shall upgrade, as needed, and maintain the CAATS system, including the integrated RATS modules, to be TRM compliant and Section 508 compliant.

<u>Base Period (Increment 1)</u>

1. Integration of RATS Modules

The Contractor shall integrate the following five RATS modules (also listed in Section 1.0 Background) into the CAATS system.

a. RATS System Administration
b. RATS Import/Export
c. RATS Workload Management
d. RATS Reconciliation
e. RATS Reports and Documents

These five RATS modules have already been developed using the same .NET framework as CAATS and reside on the same server as the CAATS application. The RATS modules do not have any external interfaces and they will not interface with any existing CAATS modules except for authentication and permission type purposes. Refer to Attachment 1 – RATS System Design Document (Will be provided with the solicitation) for additional RATS information.

The Contractor shall integrate the RATS modules into CAATS so that the following are met:

a. There shall be a single point of entry to the CAATS application which contains both the CAATS and RATS modules.
b. CAATS and RATS are currently role-based applications. The user's roles shall determine if the user has access to only the CAATS modules, only the RATS modules, or both the CAATS and RATS modules. Administrators have the ability to give RATS users access to specific RATS modules.
    i. A user group named "VBAFC" (organization) shall be created to allow RATS users to view the RATS module.
    ii. A user profile labeled "RATS Admin" shall be created to allow certain users to view both RATS and CAATS modules.
c. Users that have access to both RATS and CAATS modules shall be able to toggle between RATS modules and CAATS modules.
d. The RATS database shall be combined with the CAATS database, with the RATS and CAATS tables contained in the CAATS database. There will be no comingling of RATS and CAATS data in the tables.
e. When a user needing access to the RATS modules registers in CAATS for the first time, the user will select RATS for the organization. The user's request will be directed to the RATS user administration for the RATS administrator to give appropriate access to the different RATS modules.

After the integration of the RATS modules into CAATS is complete, the Contractor shall run a script that will be provided by VA to upload data from VBAFC's Recertification Access database and populate the new RATS tables/modules within the CAATS database.

2. Requisition Module for Vocational, Rehabilitation, and Employment (VR&E) Service Module

This requisition module for VR&E Service shall be developed using existing requisition module functionality. The requisition module for VR&E shall replace the current manual obligation process and contains Personal Identifiable Information (PII) which is different from the current Requisition module. This module shall consist of the following three sub modules:

a. Purchase request
b. Establish purchase order
c. Modify purchase order

This module will interface with FMS and eCMS.

Base Period (Increment 2)

3. Purchase Card Module for VR&E Module

This purchased card module for VR&E shall be developed using existing purchased card module functionality. The purchased card module for VR&E shall replace the current manual purchase card process and contains PII which is different from the current purchase module.

This module shall include the following six sub modules:

a. Purchase card order
b. Purchase card receiving
c. Purchase card reconciliation
d. Purchase card reconciliation approval
e. Purchase card setup list
f. Purchase card reports

This module will interface with FMS and CCS.

4. Archiving Functionality Module

This module shall add the functionality of archiving data in the system.

5. VBMS Interface for Contract Exams Module

This module shall add the ability of CAATS to accept the Contract Exam file from Veterans Benefits Management System (VBMS). This module will interface with VBMS and FMS.

Option Period One (Increment 3)

6. New Payment Module for Dignified Burial and Other Veterans' Benefits Module

This module shall allow for the payment of a casket or urn reimbursement for burial of eligible Veterans for Dignified Burial and Other Veterans' Benefits in accordance with public law 112-260. This module is for NCA only. This module will interface with FMS.

7. Paralympics Phase III Module

This module shall add the ability for the Paralympics Veterans and the US Olympic Committee coaches to access CAATS to update and verify training data for payment. This module will interface with FMS.

8. RATS Minor Enhancements

This module shall deliver minor enhancements to the RATS modules. It is anticipated that the following enhancements will be needed.

a. RATS Workload Management module
    i. Update user displays to convey aging of records through color coding
    ii. Modify log displays for personalization based on user preferences for sorting
    iii. Add one Assignment email notification
    iv. Update two letter templates
    v. Add the ability to search records marked for purge
b. RATS Reports and Documents module
    i. Add ad hoc reporting functionality
    ii. Add/modify three reports

Option Period One (Increment 4)

9. Processing and Enhancement Module

This module shall allow the user to submit processing and/or enhancement requests electronically to the CAATS Administrators. This module will interface with FMS.

10. Help Functionality Module

This module shall add help functionality for the user to be able to find information needed inside the system.

The Contractor shall transition the current CAATS source code from Team Foundation to the Technical Reference Model (TRM) compliant Rational Tools suite. VA will provide access to the Rational Tools Suite. The Contractor shall take required Rational tool training before VA will provide access to the tool suite. The Contractor shall provide a bi-weekly report, listing the updated status of the transition.

Each month, the Contractor shall meet with the stakeholders (to include the COR as required) to determine what modules will be included in the next bi-monthly releases. The Contractor and VA testing team determine their available workload on a weekly basis, while the VA stakeholders prioritize which tasks are most important to produce with the available workload. The Contractor shall enter and monitor all tasks needed to develop and test the bi-monthly iterations in a task tracking system (Team Foundation/Rational Tools suite) and the Contractor shall meet all timeline dates.

The Contractor shall develop the requirements specifications and design based on the requirements provided by VA (refer to Attachment 2 - CAATS Phase III Requirements Specification Document). The Contractor shall document the requirement specifications in the Requirements Specification Document and the design in a System Design Document in accordance with ProPath. The Contractor shall develop the Source Code/build in accordance with the requirements provided by VA and the Requirements Specification Documents. The Contractor shall conduct testing (unit, functional, system,

and performance) of software throughout the development lifecycle. The Contractor shall develop a Master Test Plan in accordance with ProPath describing all aspects of the CAATS Phase III testing. Using the Requirements Specification Document and System Design Document, the Contractor shall develop Test Cases/Test Scripts as part of the Master Test Plan. The Contractor shall develop the CAATS Composite Requirements Traceability Matrix in accordance with the ProPath template. The Contractor shall update the Acceptance Criteria Plan to include what the customer will accept for each increment. As changes occur during the software development lifecycle, the Contractor shall update the Requirements Specification Document, System Design Document, Test Cases/Test Scripts, CAATS Composite Requirements Traceability Matrix, and the Acceptance Criteria Plan to keep them current.

The Contractor shall update the CAATS Architectural Manual with requirements provided by VA in accordance with ProPath and PMAS.

The Contractor shall coordinate all activities for CAATS Phase III development with the COR and the Contractor currently performing CAATS Sustainment work on a separate task order to avoid any potential conflicts.

Deliverables:

A. Requirements Specification Documents
B. System Design Documents
C. Master Test Plan
D. CAATS Composite Requirements Traceability Matrix
E. Updated Acceptance Criteria Plan
F. Updated CAATS Architectural Manual

5.3 CAATS TESTING (BASE PERIOD AND OPTION PERIOD)

5.3.1 SOFTWARE TESTING

The Contractor shall be involved with all phases of CAATS testing, including extensive functional, performance and unit testing of (new modules) releases as well as Supplemental (changes to existing modules) releases (built using automated test frameworks in .NET), to ensure quality and test from all perspectives, including user, security, and performance. The Contractor shall provide test reports performed on all unit tests. The Contractor shall ensure a high percentage of code coverage from a unit testing perspective, generating and analyzing reports that measure and report on code coverage. These measures ensure that testing procedures are an integrated and automated part of the system development effort. VA will provide the Contractor a list of defects based on VA regression testing of existing modules that shall need to be corrected. The Contractor shall comply with VA mandated Software Testing Requirements as defined in ProPath for VA user acceptance testing.

The Contractor shall conduct extensive performance testing of the CAATS system 45 days before the end of the base period and 45 days before the end of each option period, if exercised. The testing shall gather and collect statistics during normal

operations and under high usage load (e.g., toward month end between 10am – 5pm EST). Based on the test results, performance adjustments shall be applied to the system. The following metrics shall be collected:

Production Site Metrics

1. Total page views
2. Peak page views
3. Average page response time
4. Average page response time at peak

Load Test Metrics

1. Average request/page per second
2. Maximum requests/page per second
3. Average response time
4. Total page views

The Contractor shall deliver the performance test results. The results shall also identify enhancements that CAATS requires to scale for the current and future user base.

The Contractor shall report all test results including any defects identified during testing to the product owner and to the VA CAATS PM in the Initial Operating Capability (IOC)/Pre-Production Test Results document. After the product owner and the VA CAATS PM review of defects, the Contractor shall correct the reported defects. The Defect Remediation process is defined below in Sections 5.3.2 and 5.3.3. The Contractor shall correct the defects and re-test the source code to ensure corrections are successful, and update the IOC/Pre-Production Test Results. The Contractor shall provide successfully tested, Release Source Code as a result of the correction of the defects.

Deliverables:

A. Release Source Code
B. Unit Test Reports
C. Performance Testing Results
D. IOC/Pre-Production Test Results

5.3.2 DEFECT EVALUATION SUPPORT

The Contractor shall remediate reported software defects for all CAATS system software as well as CAATS Major and Supplemental releases to include feedback received from VA business regression testing. The Contractor shall evaluate software defects that are documented in the CAATS task tracking system (Team Foundation/Rational Tools suite). The Contractor shall duplicate the problem and perform an analysis to determine the severity of the problem. The Contractor shall develop a Debug Resolution Report to identify the defects to be addressed in each software patch and a brief synopsis of the defect evaluation and analysis. In addition,

the Contractor shall develop a Software Design Document for each maintenance release that defines how the applicable defects will be repaired.

Deliverables:

A. Debug Resolution Report
B. Software Design Document

5.3.3 SOFTWARE DEFECT REPAIR SUPPORT

The Contractor shall provide defect repair support for the CAATS system software as well as CAATS Major and Supplemental releases to include feedback received from VA business regression testing. The Contractor shall remediate software defects contained in the existing VA task tracking system (Team Foundation/ Rational Tools suite) based on the release plan which can involve changes to code or modifications to software logic, database schemas, and metadata, as necessary, in accordance with ProPath policies and procedures. The Contractor shall provide the source code affecting the defect repair based on the information delineated in the software design document. This source code shall be made available for VA testing.

Deliverable:

A. Source Code

5.4 ASSESSMENT AND AUTHORIZATION (A&A) SUPPORT (BASE PERIOD AND OPTION PERIOD)

The Contractor shall coordinate with the CAATS management team to plan for A&A. This shall include gathering information to be included in the documentation needed for A&A and coordination (and in some instances preparation) with the management team to ensure that all necessary project documentation is prepared, accurate, complete, and approved. The Contractor shall support CAATS with security management, to include maintenance and application of the Security Plan, input in the development of Security Assessment Reports and Security Risk Assessments, reviewing software application requirements to assure that the necessary security elements are identified, and posting of all required security documentation in the VA Security Management and Reporting Tool (SMART). Such documentation includes:

1. System Security Plan
2. Risk Assessment
3. Privacy Impact Assessment (if applicable)
4. Disaster Recovery Plan
5. Contingency Plan
6. Incident Response Plan
7. Configuration Management Plan
8. Security Configuration Checklist
9. System Interconnection Agreements (if applicable)
10. Signatory Authority

This documentation, when packaged, will be referred to as the information systems "Pre-Approval Package". It is also referred to, in general terms, as the Security Plan. The Contractor shall coordinate with the VA Certification Program Management Office (CPMO) to transmit documents and coordinate between the CPMO and the CAATS team to provide responses to any questions that the CPMO may have. The Contractor shall maintain routine contact with the A&A officials during the certification process.

5.5 IMPLEMENTATION/DEPLOYMENT SUPPORT (BASE PERIOD AND OPTION PERIOD)

The Contractor shall develop a detailed Implementation Plan for the release that shall include a schedule listing all the tasks that must be performed in order to ensure a smooth implementation of the release. The Contractor shall describe the Section 508 compliance including the methodology used to conduct the 508 testing and the remediation plan that was executed, if applicable, in the Section 508 Compliance Self-Certification. The Contractor shall create the build for implementation in accordance with the ProPath product build process and shall provide support to the AITC in the deployment of the iteration. The build shall contain the Build Instructions for the release. The Contractor shall summarize the features and contents of the build in a Version Description Document in accordance with ProPath.

Deliverables:

A. Implementation Plan
B. Section 508 Compliance Self-Certification
C. Build Instructions
D. Version Description Document

5.6 SOFTWARE RELEASE (BASE PERIOD AND OPTION PERIOD)

The Contractor shall utilize established VA processes to implement fully tested releases to the CAATS training and production environments. Prior to the deployment of the release, the Contractor shall prepare the Deployment Plan and Product Operations Manual in accordance with ProPath. The Contractor shall prepare the Customer Acceptance Form and submit it to VA for VA to obtain the necessary signatures. The Contractor shall create the Data and Code Change Orders used in the change management process for implementing the release into the training and production environments. The Data and Code Change Orders shall contain deployment instructions needed for AITC system administrators to update the CAATS training and production environments. The Contractor shall adhere to the release schedule prepared by the CAATS product owner. If the release changes user functionality, the Contractor shall update applicable technical documents such as the Installation Guides and Architecture Manuals to reflect the modified operation. As part of the Installation Guide, the Contractor shall prepare a Backout/Rollback Plan that describes how to re-install the previous release in the event the implementation is not successful. The

Contractor shall also prepare a Product Operations Manual that includes information needed to maintain and trouble shoot the release.

Deliverables:

A. Deployment Plan
B. Product Operations Manual
C. Customer Acceptance Form
D. Data and Code Change Orders
E. Installation Guide

5.7 30 DAY PRODUCTION PERIOD (BASE PERIOD AND OPTION PERIOD)

The Contractor shall support each software module up to 30 days after it is released into the production environment. Once deployed, if a defect is found within the 30 day period, the Contractor shall develop a debug resolution report and resolve the defect. If no defects are discovered within the deployed module, it will be accepted by VA as an approved module and will be ready to transition to sustainment.

5.8 CAATS TRANSITION TO SUSTAINMENT ACTIVITIES (BASE PERIOD AND OPTION PERIOD)

VA plans to transition the CAATS system from OI&T Product Development to OI&T Product Support (sustainment) after each CAATS module is released to the production environment. The Contractor shall support transition activities between CAATS and OI&T sustainment organizations including the development of the Transition to Product Support Services Plan and Operational Acceptance Plan (OAP) in accordance with ProPath.

Deliverables:

A. Transition to Product Support Services Plan
B. Operational Acceptance Plan

5.9 CAATS SUPPORT

5.9.1 CAATS PMAS SUPPORT (BASE PERIOD AND OPTION PERIOD)

VA instituted PMAS, a strategic management process to plan and manage VA IT initiatives. In order to comply with the oversight requirements of PMAS, OI&T programs and projects must maintain and regularly report on their progress and status. This reporting must include not only technical progress but contractual and financial status as well. It is critical that OI&T PMs maintain current and accurate programmatic and financial views of their Programs/Projects, ensuring that enterprise goals and direction are properly aligned. The Contractor shall provide support services to assist the PM in collection, reporting, and monitoring of PMAS information for OI&T to include preparing the required PMAS artifacts in accordance with the ProPath Process Maps as identified in the Document Library section at the following link https://www.voa.va.gov/ to the Virtual Office of Acquisition Website.

The Contractor shall plan and report on PMAS data requirements and submissions. This shall include development of a methodology, and applying that methodology to both routine and ad hoc data requests.

1. Methodology

The Contractor shall coordinate with the CAATS stakeholders to create and document a methodology for meeting PMAS requirements. This methodology shall address timelines, process, procedures, templates, data element definitions, roles, and responsibilities for PMAS data management. Following PM/COR approval of the proposed methodology, the Contractor shall apply the methodology to capture, maintain, track, and report PMAS data related to the specific requirement.

2. Routine PMAS Reporting

The Contractor shall perform data capture, validation, and analysis on a routine, recurring basis, in accordance with the COR approved PMAS Data Collection Methodology. Once data is compiled, validated, and formatted, the Contractor shall log and store the official submission to create an audit trail.

3. Ad Hoc PMAS Reporting

For ad hoc data requests (i.e., data calls), the Contractor shall coordinate with the PM, and other contractor and Government teammates to collect, validate, compile, and analyze data. Once data is compiled, validated, and formatted, the Contractor shall log and store the official submission in the CAATS SharePoint site to create an audit trail.

5.9.1.1 TECHNICAL DOCUMENTATION SUPPORT

The Contractor shall provide support to the CAATS leadership in planning and managing technical documentation aspects of the CAATS Phase III project in design, development, testing, and delivery of a software solution that meets CAATS Phase III requirements as defined in the Requirements Specification Document.

The Contractor shall update the documentation provided in Draft form for PMAS Milestone 1 reviews for subsequent increments, with input, review, and acceptance by the VA PM and VBA Product Owner. This documentation includes the following:

1. Updated Project Management Plan
2. Updated Project Schedule
3. Updated Risk Plan
4. Updated Risk Log/Risk Register
5. Updated Change Control Plan
6. Updated Requirements Specification Document
7. Updated System Design Document
8. Updated Operational Acceptance Plan
9. Updated Outcome Statement
10. Updated Acceptance Criteria Plan

The Contractor shall update the following artifacts to Final form in support of the PMAS Milestone 2 review for each increment, which includes:

1. Updated Requirements Specification Document
2. Updated Acceptance Criteria Plan
3. Updated System Design Document
4. Updated Installation Guide
5. Updated Project Management Plan
6. Updated Project Schedule
7. Updated Risk Plan
8. Updated Risk Log/Risk Register
9. Updated Change Control Plan
10. Updated Outcome Statement
11. Updated Operations and Maintenance Plan
12. Updated Operational Acceptance Plan

The Contractor shall also produce new PMAS-required Milestone 2 Review documentation, with the input of the CAATS Development team, which are composed of the following:

1. IOC/Pre-Production Test Results
2. Implementation Plan
3. Customer Acceptance Form
4. Master Test Plan (inclusive of Test Cases and Test Scripts, Test Case Traceability, Assurance Review Checklist, Test Results, Test Defect Log, Test Execution Log, and Test Evaluation Summary)
5. Disaster Recovery Plan
6. Backout/Rollback Plan
7. CAATS Composite Requirements Traceability Matrix
8. Version Description Document
9. Product Operation Manual
10. Section 508 Compliance Self-Certification
11. Deployment Plan

The Contractor shall create the documentation required to obtain the Authority to Operate in accordance with the Assessment and Authorization Process in ProPath, and as described in Section 5.4 A&A Support. These artifacts are required to move the project from Active Development State into Active Implementation State.

At the end of the increment delivery and acceptance of the Milestone 2 review, the Contractor shall load the required documentation to the CAATS SharePoint.

5.9.2 QUERY SUPPORT

The CAATS team periodically receives data calls from outside stakeholders. To answer these data calls, reports need to be generated to gather data from the CAATS system. The Contractor shall develop and run queries to pull data from the CAATS system as

needed to answer the reporting requests. The estimated number of queries is approximately 10 during each period of performance. As an example, the Under Secretary for Benefits (USB) may need information on contracted medical exams. Therefore, the Contractor would develop a query to pull the data that is needed for the report to USB. Once the query has been developed, it is available for use for the rest of the period of performance.

5.10 POLICY AND LEGISLATIVE MANDATES (OPTIONAL TASK - BASE PERIOD AND OPTION PERIOD)

VA may exercise this optional task upon written notification from the CO. This task may be utilized to obtain tasks as prescribed below. The Contractor shall provide VA with a written proposal detailing the requirements, resources and price proposal utilizing the labor categories and rates as set forth in the Schedule of Deliverables. VA will perform an analysis to determine if the technical approach and price proposed are reasonable. The price for each optional task requirement shall be negotiated on a FFP basis prior to each exercise of the optional task. The Contractor shall not proceed with the work effort until a written modification is received from the CO.

This task will be used for activities as they are identified. Any such activities related to new policy or legislative mandates approved by VA will be performed under this task. Examples of previous policy and/or legislative mandates that may impact CAATS are 1) Major updates to the purchase card reconciliation process 2) Revisions to VA's Form 1358 process. Support to this task will be executed in parallel to operational requirements, and may be high priority with external stakeholder collaboration required. If exercised, the Contractor shall make any systems modifications that may result from new policy and/or legislative changes and shall provide all the services and deliverables identified in Sections 5.2 through 5.7, inclusive of all subparagraphs.

5.11 TRANSITION SUPPORT (OPTIONAL TASK – BASE PERIOD OR OPTION PERIOD)

The Contractor shall provide a Transition Plan for 30 days of outgoing transition to transition work from the current TO to a follow-on contract/TO or Government entity. This transition may be to a Government entity or to another Contractor or to the incumbent Contractor under a new TO. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this TO to the successor. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition plan shall include:

1. Coordination of Government and incoming representatives for each task area.
2. Roster of key points of contact with email address and telephone numbers.
3. Transition timeline with key milestones.

4. Inventory, review, evaluation, and transition of provided VA-furnished property, to include all
    a. Hardware/software
    b. Data/databases
5. Inventory and transition of historical data (e.g., memos, letters, correspondence, regulations, reports, documents, transition agreement documents, software licensing agreements, hardware maintenance agreement, memorandums of agreement/understanding, and inter-service agreements)
6. Procedural manuals/guidelines
7. Operating instructions
8. Data and workflow process
9. Application scheduling process
10. Templates used in day-to-day operations
11. Orientation to introduce incumbent Contractor team, programs, and users to the incoming team, explaining tools, methodologies, and business processes
12. Procedures to introduce Government personnel, programs, and users to the Contractor team's tools, methodologies, and business processes
13. Transition checklist
14. Signed turnover agreements

Deliverable:

A. Transition Plan

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security

Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Assertion authentication at a minimum must include Security Assertion Markup Language (SAML) token authentication and authentication/account binding based on trusted headers. Specific Identity and Access Management PIV requirements are set forth in 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), 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. For applications, software, or hardware that cannot support PIV authentication, a Risk Based Decision must be approved by the Deputy Assistant Secretary for Information Security.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A 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, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 (http://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2%200_2013.pdf).

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

The Contractor shall 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. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

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

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/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 / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/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 / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

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

	Position Sensitivity and Background Investigation Requirements		
Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☐	☒	☐
5.2	☐	☒	☐
5.3	☐	☒	☐
5.4	☐	☒	☐
5.5	☐	☒	☐
5.6	☐	☒	☐
5.7	☐	☒	☐
5.8	☐	☒	☐

5.9	☐	☒	☐
5.10	☐	☒	☐
5.11	☐	☒	☐

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

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. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints

2) For Tier 2/Moderate or Tier 4/High Risk designation:
   a) OF-306
   b) VA Form 0710
   c) DVA Memorandum – Electronic Fingerprints

f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
h. 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.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 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).

6.4 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
A. 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
B. 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
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher

D. 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.

6.5 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 (additional requirements of the contract consolidated into an addendum for easy reference) refer to

ADDENDUM A – Additional VA Requirements, Consolidated and ADDENDUM B - VA Information And Information System Security/Privacy Language.

6.6 GOVERNMENT FURNISHED PROPERTY

The Government will provide office space, telephone service, desktop computers, and system access when authorized Contractor staff work at a Government location as required in order to accomplish the development 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.

The Government will provide access to the current version of VA approved software including the following CAATS specific items in support of this effort:

1. Visual Studio 2013 Ultimate
2. SQL Server 2008 R2 Developer Edition
3. Resharper (8.2) and newer as allowed by subscription
4. Developer Express DXperience ASP.Net Edition (13.2) and newer as allowed by subscription
5. UltraEdit Text Editor
6. Microsoft Team Foundation Server 2010
7. CAATS Architecture Manual
8. Design Document (existing functionality)
9. Development Lifecycle Document
10. Rational Tools Suite

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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. 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.

A3.1. 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

A3.2. Equivalent Facilitation

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

A3.3. Compatibility with Assistive Technology

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

A3.4. Representation of Conformance

In order to be considered eligible for award, offerors must submit the Government Product Accessibility Template (GPAT) to verify Section 508 conformance of their products and/or services. The GPAT will be incorporated into the resulting contract.

A3.5. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include a final/updated GPAT and final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government

reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

Deliverable:

A. Updated GPAT
B. Final Section 508 Compliance Test Results

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 to Protected 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:

a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
b. Controlled access to system and security software and documentation.
c. Recording, monitoring, and control of passwords and privileges.
d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
e. 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.
f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
h. Contractor does not require access to classified data.

8. 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.
9. 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.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” dated October 5, 2009; Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” dated January 24, 2007; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, FEMP designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall

provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at www.femp.energy.gov/procurement. The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S.

services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the 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*. 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:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (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.

a. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

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

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within five days.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS,

and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires 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.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA 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.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law

enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

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

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) 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 any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.