PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Technology Transfer Program (TTP)

TTP Database Knowledge Management Software System

Date: August 5, 2013
Solicitation VA118A-13-P-0356
PWS Version Number: 3.1

Contents

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Technology Transfer Program (TTP) is to serve the American public by translating the results of worthy discoveries made by employees of VA into practice. The TTP mission is to commercialize invention by VA employees for the benefit of Veterans and the public. TTP requires a system that educates inventors concerning their rights and obligations, rigorously evaluates all inventions, obtains patents, and assists in the commercialization of new products. The TTP also requires consistent policies that govern the necessary relationships between investigator (i.e., inventor), academic partners, local VA medical centers, industry, and the Department of Commerce. The TTP requires close collaboration between Office of Research and Development (ORD) and the VA Office of General Counsel (OGC).

VA TTP seeks to acquire a Knowledge Management Software System that permits for the creation and organization of records related to technology transfer activities and stores invention disclosures, intellectual property, contractual agreements and special projects documents into one system. The Contractor shall perform Information Technology (IT) services such as data conversion from TTP's existing database into the new Knowledge Management Software System, if applicable. The Knowledge Management Software System shall also include reporting and querying tools, and web-based portal access for VA staff to utilize the system.

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, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
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. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
9. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”

13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. 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
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
16. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012
17. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
18. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010
19. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012
20. VA Handbook 6500.3, "Certification and Accreditation of VA Information Systems," November 24, 2008
21. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010
22. VA Handbook 6500.6, "Contract Security," March 12, 2010
23. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
24. OIT ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OIT ProPath takes precedence over other processes or methodologies.
25.
26. National Institute Standards and Technology (NIST) Special Publications
27. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
28. VA Directive 6300, Records and Information Management, February 26, 2009
29. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
30. OMB Memorandum, "Transition to IPv6", September 28, 2010

3.0 SCOPE OF WORK

TTP seeks a Commercial Off-The-Shelf (COTS) Knowledge Management Software System and IT services that provide for the effective management of intellectual property and technology transfer activities. The Contractor shall provide installation, configuration, maintenance, and training of the Knowledge Management Software System. The Contractor shall also perform any necessary data conversion from the existing Knowledge Sharing System database, if applicable.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be 16 months from the date of award, which includes 12 months of maintenance support. This requirement also includes four 12 month option periods for maintenance support.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are ten 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

Data conversion and configuration of the software shall be performed via the VA Virtual Private Network (VPN) or Citrix access to the VA server at the Contractor facilities. Installation shall be conducted in VA facility, Research and Development Computing Center (RDCC), located at 103 South Gay Street (room 400), Baltimore, MD. Training shall be conducted in VA facility located at 131 M Street NE, Washington, DC. If access to VA facilities is required, escorts will be required and provided.

4.3 TRAVEL

There are three estimated trips in support of the program related meetings for this effort. Meetings are estimated to last one day at the following locations:

1. RDCC, 103 South Gay Street (Room 400), Baltimore, MD

2. 131 M Street NE, Washington, DC

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that documents the Contractor's approach, timeline, and tools. 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.

Deliverables:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the Contracting Officer's Representative (COR) with Weekly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions and explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding week.

The Weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations. The Contractor shall communicate with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

Deliverables:

A. Weekly Progress Reports

5.2 KNOWLEDGE MANAGEMENT SOFTWARE SYSTEM ("System")

The Contractor's COTS Knowledge Management Software system shall provide TTP with the ability to automate the creation, retrieval, and organization of activities and documents and reports related to all business practices in the technology transfer program into one system. This will include records and documents created and maintained by TTP and the management of intellectual property activities, patent prosecution activities, licensing, royalty invoicing and monitoring, transactional agreement activities, marketing activities, and special consulting projects. The system shall permit multiple users (up to 50 concurrent users) to create new records, track activities, retrieve, and upload documents, generate templates and forms, and generate reports in multiple formats (such as: MS Word, PDF, Excel). All software that is part of the Knowledge Management Software System Solution shall include perpetual licenses that allow Government to use the licensed software indefinitely.

The Contractor's COTS Knowledge Management Software System shall provide the capabilities listed below.

I. The Knowledge Management Software System shall be configured to contain the following functionality:

1. The ability to create, manage, and organize data records and documents relating TTP technology transfer activities including:

    a. Intellectual Property activities; such as invention disclosures, determinations of rights, patents, patent applications, and trademarks;
    b. Funded agreements such as Cooperative Research and Development Agreements (CRADAs);
    c. Non-funded transactional agreements and contracts such as material transfer agreements, confidentiality agreements, Cooperative Technology Administration Agreement (CTAA), Inter- Institutional Agreements (IIA), or consulting activities;
    d. Patent prosecution activities including capturing office actions, statutory deadlines, and pre-and post-prosecution expenses;
    e. Expenses and payments related to funded agreements, contracts, patent prosecution, maintenance fees, and outside patent firm expenses;
    f. Tracking of licenses and royalties including the receipt of funds and distribution of royalties to organizations and individuals.
    g. Marketing activity in general and those related to a specific agreements or invention disclosure;
    h. Special projects such as contracts

2. The Knowledge Management Software System shall allow for management of information within modules and the integration of information across modules related to TTP activities (inventions, Intellectual Property, patents agreements, special projects). The System shall allow users to enter and view key information found within the module on one screen (home screen) :

    a. Invention Module: including the inventors, invention description and, law firm and affiliate contact information, affiliate contact information, materials, and related inventions.

b. Intellectual Property Module: including patents and patent applications numbers, filing dates, deadlines for future activities, trademark filing information and materials, inventors, and law firm and affiliate contact.
c. Agreements Module: Type of Agreement, associated contracts, Non-profit, collaborator, and principal investigator of any kind.
d. Licensing Module: Patent and patent applications associated with license, related licenses, inventions, inventor, and affiliate and licensor contact information.
e. Royalty Module: Patent and patent applications associated with license, related licenses, and patents, inventors, and affiliate and licensor contact information.

f. Any home screen Modules shall offer the ability to enter and display the following:
    i. Assign case number automatically according to Administrator established numbering scheme;
    ii. Title;
    iii. TTP staff responsible for activity;
    iv. Track of important dates and milestones related to technology transfer activities;
    v. Status of case;
    vi. Indicate funding associated with agreements, licenses and patent activities;
    vii. Contact information;
    viii. Function or roles to contacts associated with activity;
    ix. Functions or roles to the different organizations, such as companies, other VA or Federal Agencies, and academic affiliates; and
    x. Notes.

3. The Knowledge Management Software System shall offer the ability to visualize and organize Contact information of individuals and organizations that are involved in the Technology Transfer activities.

4. Query Functionality: the ability for a user to build and store queries.
    a. An intuitive query tool to build complex (nested Boolean logic and table join) queries that can be saved, emailed, printed, or exported to other databases.
5. Index and Search Functionality: The System shall have capability to index all terms in all records, including text readable attached files, and provide the ability to perform global key word search, field specific search and the use of Boolean logic to facilitate searching through the use of multiple criteria across different fields and activity modules.
6. Functionality to index text-based documents and optical character recognition for image-encoded documents to support full text searching.

7. Financial Reporting Tools: allowing automated and custom reports to be generated on demand by users. This function shall include the ability to store and re-use custom reports.
8. Administrative Functions: Data Merge, Manage Users, Manage Permissions, Manage Surveys:
   a. The ability for administrators to delete standard fields.
   b. The ability for administrators to reorder fields within a page/section.
   c. The administrators to change the label (name) of fields and sections.
   d. The ability for the administrator to configure reporting years and dates and financial (fiscal) years and dates.
   e. The ability for the administrators to reassign automatically populated data fields such as reassignment of staff responsible for TTP activity
   f. Allowing administrator to designate user to submit agreements online.
   g. Any administrator modifications including field additions, modifications, and deletions to be carried through to reporting and search tools native to the System, including the following functionality:
      i. Each field added shall be searchable globally and through the system's query builder and available to establish query criteria against it and return the field in a report.
9. System shall provide an ability to view and manage workflow by projects and staff including:
   a. Tracking of daily tasks, status and action items.
   b. Ability to view in process or completed tasks
10. System shall provide an ability to hold data for verification before release to the public domain of the Knowledge Management Software System.
11. Marketing Automation: System shall include features allowing users to automate marketing through the use of user defined templates that pull data from multiple fields.
12. Financial Management Tool: System shall include the capability for designated users to manage financial activities such as receipt of funds, expenses, and revenues. The system shall include the capability to generate and save templates such as invoices, documents and forms, and automatically populated by data from a selected record.
13. Document Template Tool: to generate documents, forms, automatically populated by data from selected records for different categories of TTP activities and agreements.
14. Lightweight Directory Access Protocol (LDAP) Integration: The system shall integrate with VA's implementation of Microsoft's Active Directory.
15. The ability for users to create both automated ("trigger") user defined alert emails and ad hoc (manually created) alert emails.
16. Functionality to recognize email from designated users in order to programmatically update appropriate records in the Knowledge Management Software System.
17. Document management, including tracking document revisions, the ability to attach a single document to several records, the ability to tag, categorize, and

store meta-data about documents, using documents from file structures external to the System, including those residing on different servers.

18. System shall provide a web-based interface that provides full functionality including read, write, editing and reporting activities for all data records
19. Web-based interface that permits designated users to browse their related records (inventions, patents, and agreements) based on administrator-defined permissions as well as submit online invention disclosures.
20. A graphical reporting capability natively in the software without the installation or purchase of additional software to create reports.
21. The ability to add user defined fields as needed. Fields shall of the following types:
    a. Text fields of pre-defined length (based upon the vendor's architecture)
    b. Text areas of unlimited characters(based upon the vendor's architecture)
    c. Dropdown menu
    d. Multi-select list (controlled vocabulary, with administrator ability to define)
    e. Radio buttons
22. System shall have a reporting capabilities that contains template reports and which permits the generation of ad hoc, storable, reports based upon the following TTP office activities:
    a. Intellectual Property activities-filing decision, patent family information, patent status, patent number, license information, inventor by name, organization, organizational function (patent lead).
    b. Investigator Activity- to include the status of invention disclosures, patents, agreements, other special projects, and royalties for an inventor.
    c. Activities by organization- to include inventions, agreements, patents, payments, royalties, contact information, and the ability to report the organizational function (academic affiliate, company collaborator, NPC, VA division, law firm, marketing firm or other).
    d. Docket report by staff- showing staff work activities
    e. Activities by Organization type and function/role.
    f. Special Projects - activities status and contacts.
    g. Activities over a given time period.
    h. Activities by type.
    i. Activities by users TTP specialist or OCG contact.
    j. Ability to report funding associated with agreements, licenses, patent costs and royalties.
    k. Ability to report marketing activities.
23. System shall provide the ability to export reports as either an Excel spreadsheet or PDF format.

II. Knowledge Management Software System shall support the following Operating Environment:

1. The COTS Software shall be based on a Structured Query Language (SQL) database such as MySQL, Microsoft SQL Server, or Oracle Relational Database Management System (RDBMS).
2. All interfaces to the Software shall be through web browsers. The supported browsers shall include Firefox, Google Chrome and Microsoft Internet Explorer.
3. Web browser interface shall be created with commercially available development tools.
4. Software shall operate in either a Microsoft Windows or Linux environment.
5. Software shall be supported in a virtualized environment using VMware.
6. Software shall be 508 compliant.

The Contractor shall provide VA with detailed Application Program Interface (API) Documentation for the Knowledge Management Software System. The API Documentation shall describe the software components interface and the data structure of the Knowledge Management Software System.

Deliverable:

A. Application Program Interface - Draft

5.3 SYSTEM CONFIGURATION

The Contractor shall install and configure the COTS Knowledge Management Software System in both a production environment and test environment accessible to VA. VA will continue to test and verify the system under the test environment to ensure the configuration of the Knowledge Management Software System meets the PWS requirements. Upon successful testing of the system and with VA approval, the Contractor shall migrate the Knowledge Management Software System into the production environment.

The Contractor shall configure the COTS Knowledge Management Software System based on discussions with VA staff regarding TTP’s business practices.

The Contractor shall provide VA with the following documents:

1) System Design Document (SDD) detailing system requirements, operating environment, system and subsystem architecture, files and database design, input formats and output layouts.

2) System Installation / Configuration Guide detailing the steps required to install, configure and setup the operating system, Knowledge Management Software System, and supporting database.

3) System Configuration Report documenting the settings actually used to install, configure and setup the operating system, Knowledge Management Software, and supporting database.

4) Administrative Guide detailing administrative tasks of maintaining the Knowledge Management Software System and database to include any periodic and data maintenance activities.

Deliverables:

A. System Design Document - Draft
B. System Configuration Guide - Draft
C. System Configuration Report - Draft
D. Administrative Guide - Final

5.4 DATA CONVERSION

The Contractor shall convert records and import data including documents from TTP's existing knowledge sharing system, TechTracS, into new Knowledge Management Software System within following award of the contract, if applicable.

5.5 DATA REVIEW

Contractor shall provide the services related to VA's current data as listed below.

I. *Data Audit*: The Contractor shall audit and review current VA's Knowledge Sharing System TechTracS for missing key client data that is required for the application to function correctly, missing essential client data as defined by VA, and duplicate data. The Contractor shall perform data audit to correct errors prior to data being uploaded into the new Knowledge Management Software System. The Contractor shall provide a Data Audit Report to identify duplicate, missing and erroneous data.

For the purpose of this PWS:

1. *Key data is defined as critical data required for the system to function correctly*
2. *Essential data is defined by VA according to the VA TTP business rule*

II. *Data Cleaning*: Based on the Data Audit process and VA's responses to the Audit documentation, the Contractor shall ensure that all data in the existing database is mapped to appropriate data fields. The Contractor shall correct any mismatched data by entering missing client data into the database, identify duplicate data, and merge or delete such duplicate data as directed by VA. The

Contractor shall provide a listing of records that identify missing key data information.

III. *Trial Data Upload*: The Contractor shall upload all of cleaned client data as result of Data Cleaning into the Knowledge Management Software System under a testing environment for VA's review, and approval of that data has been uploaded correctly and successfully without any error.

IV. *Final Data Upload:* After a successful trial data upload and acceptance testing, the Contractor shall perform a final data upload to the production environment of all cleaned data. The acceptance testing will be performed by VA.

Deliverables:

A. Data Audit Report

5.6 TRAINING

The Contractor shall conduct onsite instruction training for up to thirty (30) users in VA facility located at 131 M Street NE, Washington, DC. The Contractor shall provide the user with knowledge, procedures, and processes to operate and maintain the new Knowledge Management Software System.

The Contractor shall conduct the training session after completion of system implementation to the production environment, but prior to the post implementation for Knowledge Management Software System.

The Contractor shall provide both hard and electronic copies of Training Materials to include training schedule and training objectives, and curriculum.

The Contractor shall provide both hard and electronic copies of the User Guide detailing actual use of software. The User Guide shall clearly outline methods for creating and saving customized queries and reports by the user.

Upon implementation of Knowledge Management Software System, and completion of training, the Contractor shall provide at least one additional web-based training session per contract year to train new users or provide training on any system updates.

Deliverables:

A. Training Materials
B. User Guide

5.7 KNOWLEDGE MANAGEMENT SOFTWARE SYSTEM POST IMPLEMENTATION

Upon completion of data conversion, data review, and implementation of the Knowledge Management Software System to the production environment, and training, VA will perform testing to ensure the implementation meets the requirement as stated in this PWS.

The Contractor shall perform post implementation configuration adjustments and error corrections on the Knowledge Management Software System as directed by VA. VA will provide the Contractor with information pertaining to any required post implementation adjustment and error correction requirement.

Upon completion of Post Implementation of Knowledge Management Software System, the Contractor shall provide VA with updated API, SDD, System Configuration Guide, System Configuration Report, and User Guide to reflect any changes made during Post Implementation.

Deliverables:

A. Application Program Interface - Final
B. System Design Document - Final
C. System Configuration Guide - Final
D. System Configuration Report – Final
E. User Guide - Final

5.8 MAINTENANCE SUPPORT

Upon implementation of Knowledge Management Software System, and completion of training, the Contractor shall provide helpdesk and maintenance support for the Knowledge Management Software System via phone and email for 12-months during the base year and, if exercised, the four 12-month option periods. The support shall cover regular business hours and include regular software updates based upon Contractor publicly published update schedule. The maintenance support shall be initiated prior to Post Implementation of Knowledge Management Software System.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. The purpose of the Enterprise Architecture (EA) is to inform and guide the decisions of the enterprise, especially as they pertain to Information Technology (IT) investments. The Technical

Reference Model (One-VA TRM) is one component within the overall EA that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. Moreover, the One-VA TRM, which includes the Standards Profile and Product List, collectively serve as a technology roadmap and as a tool for supporting Office of Information & Technology (OIT).

Adherence to the One-VA TRM is essential to improving the technical environment within VA. All OIT Staff and contractors shall comply with the One-VA TRM. This includes COTS products and/or technical industry standards that are currently implemented or being considered for use by VA programs, projects and business groups. Products that fall into this category must be evaluated, assessed and rendered a decision to meet and satisfy TRM compliance.

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

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. However, the migration from Windows XP to Windows 7 is not yet complete within all of VA. As a result, compatibility with and support on Windows XP, Internet Explorer 7 and Microsoft Office 2007 are also required until April 2014 when Microsoft's extended support for Windows XP ends. Applications delivered to the VA and intended to be deployed to Windows XP or 7 workstation shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a VA trusted 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 has been configured using the Federal Desktop Core Configuration (FDCC) and 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 OIT 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 OIT-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 Security Suitability Program,” Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate	**Moderate Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
	records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

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

	Position Sensitivity and Background Investigation Requirements		
Task Number	Low/NACI	Moderate/MBI	High/BI
5.1	☒	□	□
5.2	☒	□	□
5.3	☒	□	□
5.4	☒	□	□
5.5	☒	□	□
5.6	☒	□	□
5.7	☒	□	□
5.8	☒	□	□
5.9	☒	□	□

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. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
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 termination of the contract for default.

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The following shall apply to all document deliverables:

a) Deliver electronically via email, or by other electronic means (e.g., compact disk) if the document is too large to enter the VA's email system.
b) Shall be in Microsoft Word or Adobe Postscript Data Format (PDF).
c) Shall be free of spelling, punctuation, syntactical, grammatical errors, and other errors.
d) Provide definitions for acronyms and abbreviations.
e) Concepts and issues shall be introduced and explained.
f) When submitting updates, change bars shall be used to highlight modifications or enhancements.
g) Security shall be maintained when submitting deliverables.

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***
1. Technical Needs	***Shows understanding of requirements*** ***Efficient and effective in meeting requirements*** ***Meets technical needs and mission requirements*** ***Offers quality services/products***	***Satisfactory or higher***
2. Project Milestones and Schedule	***Quick response capability within 24 hours of contact*** ***Products completed, reviewed, delivered in timely manner*** ***Notifies customer 24 hours in advance of potential problems***	***Satisfactory or higher***

	Successful installation and configuration of Knowledge Management Software System	
3. Project Staffing	***Currency of expertise*** ***Personnel possess necessary knowledge, skills and abilities to perform tasks***	***Satisfactory or higher***
4. Value Added	***Provided valuable service to Government*** ***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 in accordance with VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

6.6 GOVERNMENT FURNISHED PROPERTY/INFORMATION

The Government will provide the Contractor data included in the previously purchased software for conversion and configuration into the new database system.

ADDENDUM A

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

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

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

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. 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 are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:
The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

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

A4.0 Physical Security & Safety Requirements:

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

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

ADDENDUM B

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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, 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 Contractor 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 Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The Contractor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**,** based upon the severity of the incident.

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

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

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

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 Contractor at the end of lease, for trade-in, or other purposes. The options are:

1) Contractor 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 Contractor 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:

5) Nature of the event (loss, theft, unauthorized access);
6) 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;

7) Number of individuals affected or potentially affected;

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

9) 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;

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

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

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

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

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

15) 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. Within 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) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
2) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
3) Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;
4) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
5) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

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 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.