



PERFORMANCE WORK STATEMENT (PWS)

**DEPARTMENT OF VETERANS AFFAIRS
VHA, Office of Informatics and Analytics (OIA)
Program Support Operations (PSO)**

Healthcare Delivery Research and Advisory Services

**Date: April 24, 2015
PWS Version Number: 1.2**

Healthcare Delivery Research and Advisory Services

Contents

1.0	BACKGROUND.....	3
2.0	APPLICABLE DOCUMENTS	3
3.0	SCOPE OF WORK.....	4
4.0	PERFORMANCE DETAILS.....	5
4.1	PERFORMANCE PERIOD.....	5
4.2	PLACE OF PERFORMANCE.....	6
4.3	TRAVEL	6
5.0	SPECIFIC TASKS AND DELIVERABLES.....	6
5.1	TASK PROJECT MANAGEMENT	6
5.1.1	PROJECT MANAGEMENT PLAN.....	6
5.1.2	REPORTING REQUIREMENTS	6
5.2	BUSINESS AND TECHNOLOGY MANAGEMENT SERVICES (BASE AND OPTION PERIOD).....	7
5.3	CORE RESEARCH SERVICES (BASE AND OPTION PERIOD).....	8
6.0	GENERAL REQUIREMENTS	9
6.1	POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	9
6.1.1	POSITION/TASK RISK DESIGNATION LEVEL(S)	9
6.2	METHOD AND DISTRIBUTION OF DELIVERABLES	11
6.3	PERFORMANCE METRICS	11
6.4	FACILITY/RESOURCE PROVISIONS.....	12
6.5	GOVERNMENT FURNISHED PROPERTY	12
	ADDENDUM A	13
	ADDENDUM B	18

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA), Office of Informatics and Analytics (OIA), is to provide benefits and services to Veterans of the United States.

In meeting these goals, OIA is dedicated to supporting customers and clients to deliver the best healthcare to Veterans and other beneficiaries. OIA works closely with frontline VA doctors, nurses, other healthcare providers, non-clinical staff and associated IT system professionals to provide the tools they need to get the most out of VA's healthcare system to care for their patients. OIA develops and manages requirements, working closely with VA Office of Information and Technology (OIT) partners to turn requirements into IT solutions. OIA collaborates with colleagues across VA to support vital efforts, including electronic health record (EHR), health IT innovations and the Department's major initiatives.

Research and Advisory services are needed to help VA accomplish its initiatives, build a well-trained and informed workforce, and improve OIA assistance and guidance to programs and projects across VA.

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. 10 U.S.C. § 2224, "Defense Information Assurance Program"
4. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
10. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008

Healthcare Delivery Research and Advisory Services

13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012
16. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
17. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010
18. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012
19. VA Handbook 6500.3, "Certification and Accreditation of VA Information Systems," November 24, 2008
20. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010
21. VA Handbook 6500.6, "Contract Security," March 12, 2010
22. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at <https://www.voa.va.gov/>)
23. 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.
24. Technical Reference Model (TRM) (reference at <https://www.voa.va.gov/>)
25. National Institute Standards and Technology (NIST) Special Publications
26. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
27. VA Directive 6300, Records and Information Management, February 26, 2009
28. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
29. OMB Memorandum, "Transition to IPv6", September 28, 2010

3.0 SCOPE OF WORK

The Contractor shall provide healthcare delivery research and advisory subscription based services. The VHA/OIA requires healthcare delivery research subscription services and a variety of ad hoc data collection reporting requests as described in section 5.2 paragraph "Executive Services #1 and #2", and section 5.3 paragraph 2. The VHA is seeking this support from an unbiased source with no interest in any predetermined outcome or relationships to technology vendors or service providers to ensure that this research is independent and objective and adds real value and confidence to VHA decisions.

The Contractor shall provide in-person peer networking events. The Contractor shall provide unlimited access to Webinars for all subscribers as well as all members of staff.

Project-based services:

Healthcare Delivery Research and Advisory Services

The Contractor shall conduct targeted projects based on industry research and best practices as related to digital business/government, information technology strategies, IT operating models, IT workforce, IT sourcing, IT program management, and IT performance management on an as-needed basis.

The contractor shall analyze industry research to formulate specific recommendations related to the development of near-term and long-term strategies and roadmaps.

The Contractor shall conduct information technology, cost, organizational maturity and customer experience benchmarking projects on an as-needed basis. The results of benchmark projects will be used to support executive decision making business case development for key IT initiatives.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be 12 months from date of award with four (4) 12-month option period.

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 (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

Tasks under this PWS shall be performed at Contractor facilities.

4.3 TRAVEL

The Government does not expect travel for this task, unless the successful contractor is not located in the Washington, DC area. If not located in the Washington, DC area, then the Government anticipates 3 trips per year to Washington.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 TASK PROJECT MANAGEMENT

5.1.1 PROJECT MANAGEMENT PLAN

The Contractor shall draft a Project Management Plan (PMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The PMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The PMP 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 PMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved PMP throughout the period of performance.

Deliverable:

- A. Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the Contracting Officer's Representative (COR) with Monthly Progress Reports in electronic form in Microsoft Word and/or Project and/or PowerPoint formats. The report shall include detailed instructions/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 month.

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

Deliverable:

- A. Monthly Progress Report

5.2 BUSINESS AND TECHNOLOGY MANAGEMENT SERVICES

The Contractor shall provide Research and Advisory (R&A) services to VA in both Business and Technology Management.

Technology Management R&A services shall cover the areas of emerging and legacy technologies to determine new ways that technology can be applied to improve support for the VA mission and initiatives. The specific emphasis of Technology Management R&A services shall be on assessing near-term and long-term impacts on communications with Veterans and their families, healthcare access and effectiveness (including access to healthcare analysts), information systems and networks, security, data management and analysis, and technology management processes.

Business Management R&A services shall cover the areas of business intelligence and emerging management practices. Specific emphasis of Business Management R&A services shall be on assessing government organization structure and processes, governance, sourcing and vendor relationships and partnerships, information management and analytics, big data and data mining, security, and application management

The Contractor shall provide one level of Research and Advisory (R&A) services: Executive #1 Services and Executive #2 Services. The Executive Services #1 and #2 includes all Core Research Services as described in Section 5.3.

Executive Services #1: The Contractor shall provide Core Research Services and Executive #1 Services in addition to research and toolkits written exclusively for CIOs on topics surrounding the intersection of business and IT.

Specific Requirements:

The Contractor shall have experience in advising government, civilian, healthcare, as well as commercial Chief Information Officers.

The Contractor shall provide unlimited inquiry to expert IT analysts that are specialists in specific fields.

The Contractor shall provide an executive peer advisor for the Executive, with a minimum of 15 years of experience in IT, at least 2 years of IT Executive experience in the Federal Government or the Commercial sector. The executive peer advisor shall deliver strategic advice and serve as a sounding board for the Executive.

The Contractor shall provide industry-leading events in the U.S. Executive-level memberships require invitation to attend a CIO-focused Symposium, held in the continental U.S.

The Contractor must provide the opportunity for the Executive to engage in at least quarterly exclusive executive roundtables in the Washington, DC area.

Healthcare Delivery Research and Advisory Services

Contractor shall provide an additional opportunity for the Member to attend an event in the continental U.S. delivering a workshop-style experience to exchange ideas with prominent CIOs.

Executive Services #2: The Contractor shall provide Core Research Services, Executive #1 Services and Executive #2 Services in addition to access to subject matter experts (SMEs) and analysts for elucidation on research topics. The Contractor shall provide a forum in Technology/Business Management for ongoing peer-to-peer collaboration and networking with other Government and private sector leaders and managers.

Specific Requirements:

The Contractor executive peer advisor shall meet onsite with the Member quarterly.

The Contractor shall provide the ability to extend Executive level services to an assigned Senior Executive level staff member. The purpose of this Alternate is to support research continuity for Executives and to foster professional development for the Alternate.

Service	Number of Licenses to be Provided
Executive Service #1	9
Executive Service #2	1

Deliverables:

- A. Account Access to Executive Service #1 (9 licenses)
- B. Account Access to Executive Service #2 (1 license)

Optional Deliverables to be included in the base year and all option years

- C. Account Access to Executive Service #1 (1 additional license)

5.3 CORE RESEARCH SERVICES

VHA/OIA requires unlimited access to basic IT research to provide foundational knowledge for core staff. Research must include immediate insight into current trends and new developments in the IT industry. The Contractor shall make accessible to VA a Core Research service that includes access to a Contractor-provided, robust, online, research library database of no fewer than 6,000 current documents (to include new IT research documents and toolkits) that provides insight into the entire spectrum of IT Healthcare delivery products, services, processes, metrics, and roles/functions. The database shall include research into current and evolving IT Healthcare delivery trends in the areas including: cloud computing, mobility, security, infrastructure, operations, portfolio management, applications, and telecommunications. The database shall also include research addressing current Government and healthcare trends in these areas.

Healthcare Delivery Research and Advisory Services

Access to the online research library database shall also include the ability for VA to make unlimited inquiries via telephone or written request to a Contractor analyst who will provide responses to those inquiries through 30-minute inquiry, as well as responses to VA requests for document reviews, contract/RFP/RFI reviews, white papers, and business case justifications regarding the leading products or services pertinent to IT Healthcare delivery in such areas as customer relationship management, change control management, enterprise resource planning, and supply chain management software. VHA/OIA requires access to monthly audio commentaries on current IT topics. Contractor shall provide on-line peer networking including Federal peers, and Contractor Subject Matter Experts only (no IT vendors). The Contractor shall provide industry-leading events in the U.S. in role-focused conferences.

Additional Requirements:

The Contractor shall provide a Research Process Description that documents the process used by the Contractor to ensure that research results provided in the Contractor research library database reflect unbiased and independent methods of investigation and inference. Access shall consist of the following:

Service	Number of Licenses to be Provided
Core Research:	7

Deliverables:

- A. Account Access to Core Research Services (7 licenses)
- B. Research Process Description

Optional Deliverables to be included in the base year and all option years

- C. Account Access to Core Research Services (1 Additional license)
- D. Account Access to Core Research Services (1 Additional license)

6.0 GENERAL REQUIREMENTS

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

6.1.1 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

Healthcare Delivery Research and Advisory Services

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

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

	Position Sensitivity and Background Investigation Requirements		
<u>Task Number</u>	<u>Low/NACI</u>	<u>Moderate/MBI</u>	<u>High/BI</u>
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 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).

6.3 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 Products completed, reviewed, delivered in timely manner Notifies customer in advance of potential problems	Satisfactory or higher
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

Healthcare Delivery Research and Advisory Services

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.

6.4 FACILITY/RESOURCE PROVISIONS

Not applicable.

6.5 GOVERNMENT FURNISHED PROPERTY

Not applicable.

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 and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: <http://www.section508.gov> and <http://www.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:

- § 1194.21 Software applications and operating systems
- § 1194.22 Web-based intranet and internet information and applications
- § 1194.23 Telecommunications products
- § 1194.24 Video and multimedia products

Healthcare Delivery Research and Advisory Services

- § 1194.25 Self contained, closed products
- § 1194.26 Desktop and portable computers
- § 1194.31 Functional Performance Criteria
- § 1194.41 Information, Documentation, and Support

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

A4.0 Physical Security & Safety Requirements:

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

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

A5.0 Confidentiality and Non-Disclosure

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

The Contractor may have access 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.

Healthcare Delivery Research and Advisory Services

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.

Healthcare Delivery Research and Advisory Services

- 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.

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.

Notes to the Contracting Officer

(This section to be removed from PWS before solicitation)

TYPE OF CONTRACT(S)

- Firm Fixed Price
- Cost Reimbursement
- Labor-Hour
- Time-and-Materials
- Other _____

SCHEDULE FOR DELIVERABLES

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

Task	Deliverable ID	Deliverable Description
5.1.1	A	Project Management Plan Due thirty (30) days after contract award. Inspection: Destination Acceptance: Destination
5.1.2	A	Monthly Progress Report Due the fifteenth (15) day of each month reporting on the previous month. Inspection: Destination Acceptance: Destination
5.2	A	Account Access to Executive Service #1 (9 licenses) Due within five business days after contract award. Inspection: Destination Acceptance: Destination
5.2	B	Account Access to Executive Service #2 (1 licenses) Due within five business days after contract award. Inspection: Destination Acceptance: Destination
5.2	Optional C	Account Access to Executive Service #1 (1 additional license) Due within five business days after contract award. Inspection: Destination Acceptance: Destination
5.3	A	Account Access to Core Research Services (7 licenses) Due within five business days after contract award. Inspection: Destination Acceptance: Destination

Healthcare Delivery Research and Advisory Services

Task	Deliverable ID	Deliverable Description
5.3	B	Research Process Description Due fifteen (15) days after contract award. Inspection: Destination Acceptance: Destination
5.3	Optional C	Account Access to Core Research Services (1 additional license) Due within five business days after contract award. Inspection: Destination Acceptance: Destination
5.3	Optional D	Account Access to Core Research Services (1 additional license) Due within five business days after contract award. Inspection: Destination Acceptance: Destination

INSPECTION and ACCEPTANCE / Free on board (FOB) for Shipped Deliverables

N/A

Special Shipping Instructions:

N/A

POINTS OF CONTACT

VA Program Manager:

Name: Charles Hume
Address: 810 Vermont Ave., NW, Washington, DC 20420
Voice: (202) 461-5834
Email: charles.hume@va.gov

Contracting Officer's Representative:

Name: Denise Zibura
Address: 113 Holland Ave., Albany, NY 12208
Voice: 518-449-0605
Email: denise.zibura2@va.gov

Contracting Officer:

Name:
Address:
Voice:
Email:

ADDITIONAL ITEMS

Healthcare Delivery Research and Advisory Services

GOVERNMENT RESPONSIBILITIES

The following needs to be provided by the CO to the Contractor:

1. The Security Investigations Center will require the following forms from the Contractor or to the Contractor's personnel:
 - a. N/A

SPECIAL INSTRUCTIONS/REMARKS

This contract is for subscription access to a database (e.g. Gartner, LexisNexis, etc.). Access to the subscription, which is inclusive of ad hoc research of the subscriber database, is the only deliverable.

SPECIAL CLAUSES, ETC. TO BE INCLUDED IN THE SOLICITATION

- Transition clause required?
(Insert FAR clause, Continuity of Services, FAR 52.237-3)
 - Intellectual Property/Technical Data Rights Clause required?
 - OCI Clause required?
 - Government Furnished Material/Equipment: CO should add a special clause to the contract citing the Title of the material/equipment, Identifier (Serial Number), Quantity, Purpose, and Date required by Contractor.
 - Other _____
 - Other _____
-

FOR TAC USE ONLY---SECURITY RELATED GUIDANCE

- Addendum B Security Requirement guidance to CO within Addendum B, Section B9 Training, Para. a) Sub Para. d,

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.]*

SECURITY CHECKLIST REQUIREMENTS--

- Yes No Question 4: Contracting Officials need to work with the Program Manager or (procurement requestor), COR, PO, and ISO to (IF YES):

Healthcare Delivery Research and Advisory Services

- i. Include the appropriate risk designation of the Contractors based on the PDAT determination. *(Contractor Personnel Security Requirements are covered in Section 6.1 of this PWS)*
- ii. Incorporate the security clause (Appendix B) into the contract involved and the appropriate security/privacy language outlined in Appendix C into the solicitation. *(Include Addendum B in PWS)*
- iii. Determine if protected health information is disclosed or accessed and if a BAA is required. *(CO to Provide BAA Assistance (Using Nov 2008 version of BAA (approved by OGC) and coordinate with BAA Manager)*

Yes No Question 5: Incorporate the clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract and initiate planning for the certification and accreditation of the Contractor system(s). Contracting Officials need to work with the COR and ISO to (IF YES):

- Determine the security impact of the IT system as High, Moderate, or Low per 6500 Handbook, *Information Security Program. (Covered in Contractor Personnel Security Requirements Section 6.1)*
- Ensure Contractor understanding of the IT security requirements for certification and accreditation (authorization) (C&A) of the Contractor system. See VA Handbook 6500.3, *Certification and Accreditation. (CO to notify COR of this responsibility in letter to COR)*
- Ensure that the proper VA Management Official is appointed by the Certification Program Office to formally authorize operation of the system in accordance with VA Handbook 6500 and 6500.3. *(CO to notify COR of this responsibility in letter to COR)*
- Enforce Contractor performance (timely submission of deliverables, compliance with personnel screening requirements, maintenance of secure system configurations and participation in annual IT Federal Information Security Management Act (FISMA) assessments to ensure compliance with FISMA requirements). *(CO to notify COR of this responsibility in letter to COR)*
- Ensure yearly FISMA assessments are completed and uploaded into SMART. *(CO to notify COR of this responsibility in letter to COR)*

Yes No Question 6: Incorporate the security clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract. Contracting Officials need to work with the COR and the ISO to (IF YES):

- Ensure Contractor understands and implements the IT security requirements for system interconnection documents required per the Memorandum of Understanding or Interconnection Agreement (MOU-ISA). The standard operating procedure (SOP) and a template for a MOU-ISA are located on the Information Protection Risk Management (IPRM) Portal and can be provided

Healthcare Delivery Research and Advisory Services

to the Contractor. *(CO to notify COR of this responsibility in letter to COR and supply MOU-ISA template)*

- Ensure Contractor understands their participation in IT security requirements for C&A of the VA system to which they connect *(CO to notify COR of this responsibility in letter to COR)*
- Enforce Contractor performance (timely submission of deliverables, compliance with personnel screening requirements, and appropriate termination activity as appropriate). *(CO to notify COR of this responsibility in letter to COR)*

IF NO:

- Include a statement in PWS, immediately following the Security Clause Section that *“The C&A Requirements do not apply and that a Security Accreditation Package is not required”*.

Yes No Question 7: Incorporate the security clause and the appropriate security language from Appendices B and C into the solicitation and contract. The COR needs to (IF YES):

- Ensure that a Contractor Security Control Assessment (CSCA) is completed within 30 days of contract approval and yearly on the renewal date of the contract. *(CO to notify COR of this responsibility in letter to COR and to supply CSCA Document-Self Assessment Questionnaire for Contract Service Providers)*
- Ensure that the CSCA is sent to the ISO and the OCS Certification Program Office for review to ensure that appropriate security controls are being implemented in service contracts. *(CO to notify COR of this responsibility in letter to COR)*
- Ensure a copy of the CSCA is maintained in the Security Management and Reporting Tool (SMART) database. COR will provide a copy of the completed CSCA to ISO for uploading into SMART database. *(CO to notify COR of this responsibility in letter to COR)*

Contractor Rules of Behavior-Appendix D in Handbook 6500.6 – *(CO to add to solicitation, CO to ensure Contractor signs document)*