

## **I. BACKGROUND**

The mission of the Department of Veterans Affairs (VA) is to honor America's Veterans by providing exceptional health care that improves their health and well-being. VA will continue to be the benchmark for excellence and value in health care and benefits by providing exemplary services that are both patient centric and evidence based.

Public Law 111-163 Caregivers and Veterans Omnibus Health Services Act of 2010, established the Program of Comprehensive Assistance for Family Caregivers (*limited to eligible post 9/11 Veterans*) and the Program of General Caregiver Support Services (*open to eligible Veterans of all service eras*). These programs are collectively referred to as VA's Caregiver Support Program. The Caregiver Support Program falls under the purview of VHA, Care Management, Chaplain and Social Work Services.

Under Public Law 111-163, VA recognizes three distinct types of Caregivers all eligible for unique VA benefits based upon their Caregiver type: Primary Family Caregivers, Secondary Family Caregivers, and General Caregivers. It is critical that VA Caregiver beneficiaries are properly identified and tracked in VA systems to ensure the appropriate services and supports are rendered at the point of care and that VA staff are supported with effective technology to operationalize delivery of services and benefits.

The Veterans Health Administration (VHA) has launched a series of major initiatives to improve VHA strategy, governance, systems and operations. Congress recently passed The VA Maintaining Internal Systems and Strengthening Integrated Outside Networks (MISSION) Act to enable sweeping change, and VHA is taking a comprehensive approach to meet the MISSION Act requirements to modernize.

On June 6, 2018, John S. McCain III, Daniel K. Akaka, and Samuel R. Johnson VA Maintaining Internal Systems and Strengthening Integrated Outside Networks Act of 2018 or the VA MISSION Act of 2018, Public Law 115-182, was signed into law. Section 161 of this law expands eligibility for VA's Program of Comprehensive Assistance for Family Caregivers to eligible Veterans with a serious injury incurred or aggravated in the line of duty in the active military, naval, or air service before September 11, 2001 in two phases. First, VA must certify to Congress that VA has fully implemented a required information technology system. This law also establishes new benefits for designated primary family caregivers of eligible Veterans under the Program of Comprehensive Assistance for Family Caregivers. The Program of Comprehensive Assistance for Family Caregivers provides certain medical, travel, training, and financial benefits to primary family caregivers. VA is currently working on regulations to define the scope of financial planning services and legal services under 38 U.S.C.

1720G(a)(3)(A)(ii)(IV), as amended by section 161(a)(3) of the VA MISSION Act of 2018, under which VA is required to provide designated primary family caregivers:

- (1) financial planning services relating to the needs of injured Veterans and their caregivers; and
- (2) legal services, including legal advice and consultation, relating to the needs of injured Veterans and their caregivers.

Under the law, these services must be provided through the use of contracts with, or the provision of grants to, public or private entities.

## **II. DEFINITIONS**

- **Client** – The Department of Veterans Affairs (VA), Veterans Health Administration, Office of Patient Services, Care Management and Social Work.
- **CO** – Contracting Officer
- **Contractor** – The entity performing the contract
- **COR** – Contracting Officer's Representative
- **CSC** – VA Caregiver Support Coordinator
- **PM** – VA Program Manager
- **VA** – Department of Veterans Affairs
- **VAMC** - VA Medical Center
- **VHA** – Veterans Health Administration
- **VISN** – VA Integrated Service Network
- **Caregiver** – An individual who provides personal care services to the Veteran.

## **III. APPLICABLE DOCUMENTS**

Documents referenced or germane to this PWS are listed below. The Contractor shall be guided by the information contained in the documents in performance of this PWS.

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
3. 10 U.S.C. § 2224, "Defense Information Assurance Program"
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
6. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule, parts 160 and 164.
7. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (Pub. L. No. 105-220)
8. Caregivers and Veterans Omnibus Health Services Act of 2010 (Pub. L. No. 111-163)
9. VA Caregivers Program, 38 C.F.R. Part 71
10. VA MISSION Act of 2018 (Pub. L. No. 115-182, Sec. 161)
11. 38 U.S.C. 1720G(a)(3)(A)(ii)(IV),

## **IV. PERFORMANCE WORK STATEMENT**

The Contractor shall provide the resources necessary to accomplish the tasks as described in this Performance Work Statement (PWS). The Contractor shall implement and deliver a comprehensive National Family Caregiver Financial and Legal Services for Caregivers of Veterans who are applying for the Program of Comprehensive Assistance for Family Caregivers.

The scope of this contract encompasses all resources and development of resources, processes, personnel, materials, training, equipment, and technology necessary to provide family caregivers and their families with unlimited access to stateside information, referral, and counseling through a centralized source.

The National Family Caregiver Financial and Legal Services must be available 24 hours per day, 7 days per week, through the Internet, telephone (via 800 number), e-mail, postal, and face to face. The services must be capable of reaching Caregivers of Veterans residing in all VA markets to include Puerto Rico, American Samoa, Guam, etc. as well as both urban and rural areas. All personnel, materials and services to deliver Financial and Legal Services will be provided by the Contractor.

The Contractor shall develop a secure website that allows the Government and CSCs to make referrals containing Caregiver personal identifying information (PII) consisting of name of Caregiver, email address, and phone number for the National Family Caregiver Financial and Legal Services. The Contractor/Subcontractor's firewall and Web services security controls shall meet or exceed VA's minimum requirements. Please reference VA Handbook 6500.6, Contract Security Appendix C. The Contractor will be storing, generating, transmitting and exchanging VA sensitive information and must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide to the COR.

It is estimated that a minimum of 1,000 Caregivers will utilize Financial and Legal Services. It is estimated that 80-90% of service utilization will occur online or telephonic. The Contractor is required to respond to requests for services within 2 business days of receipt of the referral. The contractor must maintain records of all referrals by CSC and track Caregiver completion. Reports on referral numbers and utilization rates per subject will be required monthly. The contractor may be asked to provide 1-2 special reports annually, based on data being currently collected by Contractor.

The Contractor shall maintain the current 800 number and be responsible for all costs associated with the toll-free services including service provider fees, usage charges, and staff.

## **V. PERFORMANCE DETAILS**

### **A. PERFORMANCE PERIOD**

Period of performance is one (1) twelve-month base period from effective date of award with four (4) twelve-month option periods. Base: January 2020 – December 2020. Option year 1: January 2021– December 2021. Option year 2: January 2022 – December 2022. Option year 3: January 2023 – December 2023. Option year 4: January 2024 – December 2024

### **B. PLACE OF PERFORMANCE**

It is anticipated that the work under this Performance Work Statement (PWS) will be performed at the Contractor facilities.

### **C. GOVERNMENT HOLIDAYS:**

There are 10 Federal holidays set by law (USC Title 5 Section 6103). 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 any holiday falls on a Sunday, then Monday shall be observed as a holiday.

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

Martin Luther King's Birthday	Third Monday in January
President's Day	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

**D. TYPE OF CONTRACT:** Firm Fixed-Price contract.

#### **E. CONTRACT AWARD MEETING**

The contractor shall not commence performance on the tasks in this PWS until the Contracting Officer has conducted a kick-off meeting or advised the contractor that a kick-off meeting is waived. A "kick-off" meeting shall occur within (10) business days of the contract award. This meeting introduces the project team and provides an opportunity to discuss the role of each team member in the project work. The Contractor's kick-off meeting presentation should include, at a minimum, assumptions and the plan for successful deployment.

The Contractor shall provide an agenda, in advance, and document meeting minutes after the meeting. The Contractor shall coordinate with the COR to invite relevant stakeholders including the Contracting Officer (CO) and identified VHA Staff.

#### **Deliverables (Non-priced):**

- Kick-Off Meeting Agenda
- Kick-Off Meeting Participation
- Contract Management Approach, Work Plan, and Projected Staffing Report
- Contract Work Breakdown Structure and Dictionary
- Contract Kick-Off Meeting Minutes

#### **F. TRAVEL**

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings throughout the PoP. Contractor management will be required to travel to VA headquarters location at 810 Vermont Ave NW, Washington, DC 201420 for an initial kick-off meeting. Thereafter, meetings shall be held via telephone conference call or a web based online conferencing service. Travel within a 50-mile radius from the Contractor's facility is considered local and will not be reimbursed.

Travel shall be processed in accordance with the Federal Travel Regulations (FTR) and requires advance approval by the COR utilizing the VA-provided Contractor Travel Request form at ATTACHMENT XXXX.

## **VI. SPECIFIC TASKS AND DELIVERABLES**

The Contractor shall perform the following tasks:

### **A. CONTRACTOR PROJECT MANAGEMENT PLAN**

The Contractor shall include a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP should display the schedule, milestones, risks and resource support in both a narrative and graphic format. The CPMP shall also state how the Contractor plans to coordinate and execute planned, routine, and special data collection reporting requests. The initial baseline CPMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance.

#### **Deliverable (Non-Priced):**

Contractor Project Management Plan

### **B. REPORTING REQUIREMENTS**

After execution of contract, the Contractor will submit an outline of monthly data to be provided for approval by COR and PM. These reports will include progress reports that contain explanations for each required data element to ensure that data is accurate and consistent. The PM and/or COR shall approve an outline from the Contractor of the content to be presented each month. The same format shall be followed during subsequent option years.

The progress reports will be due by the 5<sup>th</sup> of every month and will include activity performed from the previous month. The progress reports shall include all work completed during the reporting period, a summary of data collected from all previous monthly reports, and work planned for the subsequent reporting period. The report shall also identify any complaints that arose and a description of how they were resolved. If complaints have not been completely resolved, the Contractor shall provide an explanation and the actions that will be taken to resolve the complaints. The Contractor shall notify the, COR, CO, and PM in writing, within 24 hours, if concerns arise that may adversely impact the performance of the PWS.

The Contractor shall provide weekly and monthly progress reports in an electronic format that will be agreed upon at kick-off meeting. The due date of the progress reports will be determined after award of the contract that will be most beneficial to the VA. The progress reports shall include a statistics log, which will include the following information for the National Family Caregiver Training Program:

- Total Number of Referrals (including a breakdown of Referrals by individual CSCs and their VAMC location)
  - Reported weekly by individual CSC
  - Aggregate reported monthly

- Number of Caregivers who have begun to receive services broken down by:
  - Telephone
  - Web-Based
  - In person
  - Spanish
  - English
  - Reported monthly
- Total Number of phone calls (including a breakdown of English calls, Spanish calls)
  - Reported monthly
- Utilization trends of the different services provided broken down by:
  - Financial
    - Subject matter
    - Referrals to outside organizations
  - Legal
    - Subject matter
    - Referrals to outside organizations
  - Unique users
  - Repeat users
  - Reported Monthly
- Persistence/consistency of use and completion rates broken down by:
  - State
  - VAMC location

**Monthly Progress Reports** shall reflect data as of the last day of the preceding Month. The Monthly Progress Report will be due on or before the 10<sup>th</sup> day of the month following the reported 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 CPMP and report any deviations. It is expected that the Contractor shall maintain communication with VA accordingly so that any arising issues are transparent to both parties to prevent escalation of outstanding issues.

Deliverables (Non-priced)

Weekly Report

Monthly Progress Report

Total Number of Referrals

ETC

A satisfaction survey will be conducted within two weeks of service completion to capture Caregiver satisfaction with the services provided. The data collection methods and the survey tool must be approved by the VA PM or COR. Surveys must be routed to the Office of Management and Budget (OMB) for approval. The VA may elect to provide the Contractor with a survey tool which has already been approved by OMB for this purpose. The Contractor shall translate into Spanish any correspondence related to the survey as well as the survey.

## C. DEVELOPMENT REQUIREMENTS

The Contractor shall provide call center services necessary to manage and operate a 24/7 financial and legal services program for family caregivers and Veterans . Call centers shall be located in the Continental United States and should include recruiting, hiring, training, and managing a professional staff. The Contractor shall provide expert consultation and education on a wide array of topics, the establishment of business applications, interpreter and translation services, back up operations and surge handling, developing the technological infrastructure necessary to operate a call center, and refreshing technology used to maintain a state-of-the-art system. The Contractor is to follow the guidance provided in VA 6102 Handbook which can be found at <http://vawww.va.gov/vhapublications/searchresults.cfm> and the VA Web Best Practices Guide found at [www.section508.va.gov/docs/VASWebBestPracticesGuide.pdf](http://www.section508.va.gov/docs/VASWebBestPracticesGuide.pdf) which will provide specific direction for the establishment, management, and maintenance of all VA websites as well as all external websites that represent the VA.

The Contractor shall provide individualized money management, financial counseling, financial planning, and referral services when applicable, to family caregivers and Veterans. The Contractor will not give specific financial investment advice in specific investment/funding opportunities. Services are specifically for personal finances and not business finances.

The services available for the National Family Caregiver Financial Services must include at a minimum the following:

**a. Debt Management – Regular**

- Help caregiver prepare for Veteran discharge
- Creating a personal budget/financial plan to reduce, eliminate, and avoid debt and to achieve solvency and stability.
- Teaching family caregivers and their families' money management techniques.
- Temporary assistant
- Understanding tier structure

**b. Debt Management – Intensive**

- **90 day program**
- **No money to be exchanged during this program**

**c. Credit Management**

- Credit Management: understanding credit, finance charges, interest rates, and the implications of only paying the minimum amount each month.
- Credit: Educating family caregivers and their families on the importance of maintaining excellent credit histories and ratings. Teaching family caregivers and their families how to establish, monitor, and protect their credit.
- Negotiating with Creditors
- Dealing with collection agents and delinquencies
- Improving credit scores
- 

**d. Financial Planning and Literacy**

- Complex financial planning
- Investment issues and opportunities
- Managing income changes or increased expenses
- Retirement planning – long term care planning
- Paying bills and managing check accounts

- VA and social security benefits
- Planning for college expenses and addressing student loans
- Evaluating and building understanding of health, life, rental insurance needs
- Mortgage loans and refinancing
- Identity theft. Teaching family caregivers and their families how to detect, deter, and avoid identity theft.
- 
- 
- 

e. Extensive Financial Coaching

- 90-day telephonic coaching program to assist in developing and implementing an action plan.
- 
- Referrals to community resources
- Self-paced education courses with online community

The services available for the National Family Caregiver Legal Services must include at a minimum the following:

- Thirty-minute consultation via telephone or in person
- Referrals to community resources for individual representation
- Estate planning
- Advanced care planning
- Wills
- Trusts
- Designating Power of Attorney
- Appointing a guardian
- Identity theft
- Referrals to community resources for individual representations
- Educational programs on areas of state and subject specific laws

Additional family caregiver and family assistance will be provided as identified by the VA.

## D. IMPLEMENTATION REQUIREMENTS

### **Requirement 1.** Call Center Operations and Information Technology (IT) services

1.1 **Call Center Objective.** To encompass all resources and development of resources, processes, personnel, materials, training, equipment, and technology necessary to provide family caregivers and their families with unlimited access (via 24-hour, toll free telephone and online/Internet) to stateside information, referral, and counseling services available through a centralized source.

1.1.1 **Call Center Minimum Requirements.** The Contractor shall provide staffing, processes, procedures, and the technological infrastructure necessary to operate a 24/7 toll free call center. All call centers must be physically located in the Continental United States.

1.1.1.1 The call center consultants answering the telephones shall have a minimum of a XXXXXXXX



1.1.1.2 The Contractor will ensure that a single number can be used by family caregivers and their families from any location world wide to access the call center. The Contractor's technical infrastructure provides back up call center capability instantaneously and shall include redundant back up call centers with trained and experienced personnel and technical support capable of supporting toll free stateside and international call from family caregivers and their families. There is a minimum of two call centers for this requirement.

1.1.1.3 The Contractor shall provide on a monthly basis call center statistics, including but not limited to number of total incoming calls, total calls answered, number of calls answered within 30 seconds, number of calls abandoned, number of calls placed on hold in total duration of more than 5 minutes, number of call backs completed.

1.1.1.4 The Contractor's technical infrastructure supports translation/interpretation. Contractor telephone integration shall include a process and capability to use interpreter/translators for telephone calls. Translation services will be offered on an immediate/on-demand basis to individuals calling the call center. Translation services will also be available for legal documents within 3 business days.

## **1.2 Website Platform**

### **1.2.1 Website Platform Interfacing Requirements.**

1.2.1.1 The Contractor shall maintain the non-proprietary interface integrating its services into the Caregiver Financial and Legal Services website.

1.2.1.2 The Contractor shall provide a single-entry point into services with a secure login capability. The Government requires access, but not ownership, to the vendor's program. The Government shall maintain ownership of all data and content in front of the login, and all of the data behind the login contained within the vendor's system.

1.2.1.3 The Caregiver Financial and Legal Services website shall comply with Section 508 of the U.S. Rehabilitation Act for website, voice and data services. Content shall be available in both English and Spanish. At a minimum, compliance includes TDD/TTY, IVRs/Automated Attendants, voice mail systems, websites, and information systems.

1.2.1.4 The Contractor shall provide Caregiver Financial and Legal Services on a continuous basis. The Contractor shall provide these services by utilizing the following support methodology principles:

- Ensure physical and logical security for all hosted computer resources.
- Provide all necessary power and environmental controls to operate and maintain the equipment.
- Plan and implement 24x7x365 backup and recovery.

1.3 Disaster Continuity of Services. The Government requires that Caregiver Financial and Legal Services are available 24/7 despite any natural or man-made disasters. In the event of a disaster, the Caregiver Financial and Legal Services telephone number will serve as the primary information source for family caregivers and their families.

## **Requirement 2. Financial Counseling**

**2.0 Financial Counseling Objective.** To provide private, confidential, financial counseling to family caregivers and their families.....Eligible participants may receive up to XX financial counseling sessions per person per issue at no cost to the participant.....

**2.0.1 Confidentiality**

2.0.1.1 All employees, contractors, and subcontractors will have access to client information will subject to VA privacy requirements.....

**2.1 Financial Counseling Requirements**

**Requirement 3. Legal Services**

**3.0 Legal Services Objective**

**3.0.1 Confidentiality**

**3.1 Legal Services Requirements**

**3.1.1 Certification**

**3.1.2 Training**

**Requirement 4: 2Training and Confidentiality.**

The Contractor shall develop, maintain, and conduct a training program and methodology to ensure all staff will be current on issues related to Veterans and caregiving needs to include but not limited to:

- Scope of Practice
- Training on military and Veteran culture and sensitivity
- VA approved training and guidance on each service component to include: Army, Air Force, Marines, Navy, Coast Guard, National Guards and Reserve componentsVA approved suicide prevention and crisis hotline interventions. This will include training on processes and procedures to support the warm handoff of family caregivers and their families.

The Contractor shall design and implement a method for regularly updating personnel on current/emerging issues pertaining to Veteran and family caregiver life.

All required training must be completed successfully prior to being referred or working with a family caregiver and training must be renewed on an annual basis.

The Contractor shall annually certify and also be able to demonstrate at any time to VA Program Office or the contracting officer, in writing, that all Contractor staff assigned to this contract have comprehensive and current knowledge of the overall military and veteran culture and all requirements of this contract.

In cases of extreme financial hardship, threat of deprivation, or other similar circumstances, financial network providers ensure that family caregivers and their families are referred to the appropriate Veteran resources.....

All personnel working on this contract shall participate annually in VHA approved training on HIPAA and the protection of Protected Personal Information (PII) and Protected Health Information (PHI). Personnel must receive this training prior to the initiation of Caregiver training. All Contractors must comply with VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY guidance and adhere to VA Handbook 6500.6 included as attachment A. Contractors will provide a certificate of completion.

The Contractor shall submit the status of VA Privacy and Information Security Awareness training for all individuals engaged on each task in the form of a Security Training Personnel Report. The status reporting shall identify; a single Contractor Security Point of Contact (POC), the names of all personnel engaged on each task, their initial training date for VA Privacy and Information Security training, and their next required training date during the base and each option period. The Contractor shall submit VA Privacy and Information Security training certificates in accordance with Section nine (9), Training, from Appendix C of the VA Handbook 6500.6, "Contract Security".

All Personnel working on this contract shall participate annually in VHA approved training on suicide prevention....

**Deliverables:**

- A. Security Training Personnel Report
- B. VA Privacy and Information Security Training Certificates

**Requirement 5. Outreach and Marketing.**

**5.0 Outreach Objective:** Strategic outreach materials and plans will raise awareness further brand family caregiver financial and legal services for eligible populations. Educational, informational, and promotional materials provide Clients with in-depth information and resources that support Client management.

**5.0.1 Outreach Tool kit:** The Contractor shall develop or update a variety of outreach tool kit materials including but not limited to brochures, posters, e-billboards, website graphics, fact sheets, presentations, social media content, and other outreach materials as needed. All products developed for the tool kit shall be readily available in color, black and white, and web versions that can be customized for use by VA Central Office, VAMCs, Vet Centers, Community-Based Outpatient Clinics, etc. ALL EIT/media products shall be 508 compliant in accordance with Federal 508 standards, which can be found at: [www.Section508.gov](http://www.Section508.gov). The Contractor shall translate to Spanish a limited number of communication products such as brochures, flyers, and posters. Finally, the Contractor shall include a set of instructions to optimize for local or commercial printing for various staff at VA medical centers.

The Contractor shall review and update outreach materials and plans to maintain relevance and accuracy.

The Contractor will warehouse, provide inventory management and distribution services for all outreach materials.

The Contractor shall replenish inventory upon request by VA.

Any outreach material that will be disbursed to the public will need approval by VA. Costs for outreach must be approved in writing by COR

4. Transition Plan

**E. GOVERNMENT FURNISHED EQUIPMENT**

The Contractor will provide resumes and/or curriculum vitae of key personnel to the COR and PM prior to confirmed offer to potential personnel. Documentation includes but not limited to resume, certification, education, credentials, etc.

Government will not be providing government furnished equipment

**F. SCHEDULE OF DELIVERABLES**

Deliverable	Description	Due Date
<i>Deliverable 1:</i>	<i>Management Plan to include at a minimum the following information in both a narrative and graphic format: Approach Timeline Tools Personnel resumes and/or curriculum vitae for key personnel on the contract Schedule Milestones Identify risks &amp; plans to mitigate Plan for Data Collection and Reports – Routine and Special Requests</i>	Submitted with offer
<i>Deliverable 2:</i>	<i>Progress Report every month with the following information:</i>	Monthly
<i>Deliverable 3:</i>		
<i>Deliverable 6:</i>		
<i>Deliverable 7:</i>		
<i>Deliverable 8:</i>		
<i>Deliverable 9:</i>		
<i>Deliverable 9:</i>		

Areas I did not see in the PWS:

## 1. Labor categories

### **TASK AREAS AND LABOR CATEGORIES**

Contractor personnel shall have the level of experience necessary to accomplish the requirements of this PWS. In addition, contractor personnel shall be acceptable to the Government in terms of personal and professional conduct, and in technical knowledge. Furthermore, contractor personnel are expected to be proficient in using office automation equipment and software and have sufficient written and verbal communication skills to support VA program offices, their customers and any other VA organizations. Should any contractor personnel be determined to be unacceptable in terms of technical competency or unacceptable conduct or behavior while on-site working on contract activities, the Contractor shall immediately remove and replace the unacceptable on-site personnel at no additional cost to the Government. Contractor personnel are to serve in a support role; therefore, final decisions regarding inherently governmental functions will always be made by Government personnel.

**2.1.1 Certification.** All financial counselors will have a minimum of a Bachelor's degree and shall maintain a national certification through Association for Financial Counseling and Planning Education (AFCPE), Certified Financial Planner (CFP), Chartered Financial Consultant (ChFC), or with the National Foundation for Credit Counseling (NFCC). Minimum of 3 years' experience with financial counseling/planning.

**2.1.2 Licensure.** All Attorneys will have a minimum of a Juris Doctor (J.D.) degree from a law school accredited by the American Bar Association (ABA) and shall be admitted to the State Bar in the jurisdiction of practice. Furthermore, all Attorneys must have at minimum 5 years' experience with the legal services described in this PWS.

**2.1.3 Call Center Staff.** All staff will have a minimum of a high school diploma or equivalent, be at least 18 years old, pass a background check, and trained in military, Veteran, and caregiver specific issues.

**2.1.4 IT Staff.** All staff at minimum will have a bachelors degree in information technology or computer science and shall have experience in fields to include software engineer, web development, IT consulting, IT vendor manager, geospatial profession, data modeler, and other areas as identified by the COR or PM.

## 2. Key Personnel

Skilled experienced professional and/or technical personnel are essential for successful contractor accomplishment of the work to be performed under this effort. These are defined as individuals crucial to the successful performance of the orders issued and the programs being supported by those orders and are those persons identified as key personnel in accordance with solicitation requirements. The Contractor agrees that the key personnel shall not be removed, diverted, or replaced from work without prior notification of the CO. Requirements that reflect the seniority and/or expertise levels of these labor categories, if any, will be specified at the order level. All Key Personnel, excluding the Principal (whose years of experience and degree requirements are already defined), should have a BA/BS degree and at

least 3 years of experience relevant to the labor category requirements. Note: Requirements that reflect the seniority and/or expertise levels of these labor categories, if any, will be specified at the order level.

**A. Senior Program Manager (Program Office Support)**

Functional Responsibilities: Experience includes engagement experience in project scope and approach, ability to focus on project delivery and business and technical integration, oversight of key business and process enablers, provide strategic direction, vision, and leadership. A Senior Program Manager works with the Project Director and other senior staff to drive business strategy and planning changes at the executive levels. A Senior Program Manager is proficient in managing the project team and daily operations of project development, project delivery and oversight of key business enablers on projects to achieve the project objectives and goals. This position is responsible for communications with project stakeholders, project and management of multiple projects across a Health Care Delivery system.

Minimum Experience: minimum of ten (10) years of large integrated health care system consulting experience. Four (4) years of this experience shall be directly related to HRO implementation in a healthcare setting. Five (5) years of this experience shall be related to change management.

**Security Requirements**

C&A requirements do not apply, and a Security Accreditation Package is not required.

**VA Handbook 6500.6, Contract Security  
APPENDIX C**

**VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR  
INCLUSION INTO CONTRACTS, AS APPROPRIATE**

**1. 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.

**2. 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.

### **3. VA INFORMATION CUSTODIAL LANGUAGE**

a. 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 the 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).

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the 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.

c. 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 the 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.

d. 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 the 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.

e. 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.

f. 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.

g. If a VHA contract is terminated for cause, the associated 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.

h. 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.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

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

k. 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.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an 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 COTR.

#### **4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT**

a. 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 COTR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

b. The contractor/subcontractor shall certify to the COTR 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 the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c. 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.

d. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

e. 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.

f. 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.

g. The contractor/subcontractor agrees to:

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

**(a) The Systems of Records (SOR); and**

**(b) The design, development, or operation work that the contractor/subcontractor is to perform;**

**(1) 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**

**(2) 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.**

**h. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.**

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

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

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

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

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

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

**l. 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.**

**5. 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 COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's 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 VA's POA&M management process. The contractor/subcontractor must use VA's 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, 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 COTR. 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 VA's 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 the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

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

- (1) Vendor must accept the system without the drive;
- (2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- (3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- (4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;
  - (a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
  - (b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting

technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved 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.

## **6. 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 COTR 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.

## **7. LIQUIDATED DAMAGES FOR DATA BREACH**

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

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

**fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.**

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

- (1) Nature of the event (loss, theft, unauthorized access);**
- (2) Description of the event, including:**
  - (a) date of occurrence;**
  - (b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;**
  - (3) Number of individuals affected or potentially affected;**
  - (4) Names of individuals or groups affected or potentially affected;**
  - (5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;**
  - (6) Amount of time the data has been out of VA control;**
  - (7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);**
  - (8) Known misuses of data containing sensitive personal information, if any;**
  - (9) Assessment of the potential harm to the affected individuals;**
  - (10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and**
  - (11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.**

**d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the 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.**

## **8. SECURITY CONTROLS COMPLIANCE TESTING**

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

## **9. 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 E relating to access to VA information and information systems;**

**(2) Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training;**

**(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and**

**(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]**

**b. The contractor shall provide to the contracting officer and/or the COTR 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.**