

## **STATEMENT OF WORK**

### **Maintenance and Service Agreement Support of Teleform and Rightfax Equipment VHA National Telehealth Training Center, Boston, MA**

#### **A. GENERAL INFORMATION**

1. Title of Project: The Department of Veterans Affairs Veterans Health Administration Maintenance and Service Contract for Store-and-Forward Telehealth Training Center.
2. Scope: The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) seeks to acquire a maintenance service agreement for the existing Teleform and Rightfax equipment used by the Training Center for patient and clinician education.
3. Background: VHA has over 7.8 million enrolled Veterans (with about 5.6 million active users). VA recognizes the need to increase access to patient education and meet the training requirement of our clinicians and health care technicians as well as the more than 200,000 patients that are screened using an imaging pathway.

Telehealth Services is responsible for ensuring our Veteran patients receive the best in patient education and that ongoing training is available to our clinicians that is robust, sustainable and ensures that our clinicians respond to the needs and are ready to meet the challenges of caring for our Veterans in a safe, efficient, and cost-effective manner.

To facilitate this program VA purchased Cardiff Teleform from Digital Documents and RightFax from HBM Information System Developers.

#### **4. Period of Performance**

The Period of Performance shall be for a 12 month base year and two 12 month option years.

#### **5. Schedule:**

Service agreement to commence upon contract award.

#### **B. GENERAL REQUIREMENTS**

##### **Section 1. Maintenance and Service Agreement for Teleform and Rightfax system.**

1. Technical Specifications and Deliverables required for Maintenance and Service Agreement for Teleform and Rightfax Equipment.

- a. Contractor will provide all maintenance and upgrades to software as part of this agreement.
- b. Contractor will provide on-site maintenance and repair during normal working hours 8AM-5PM, Monday - Friday.
- c. All work, repairs and upgrades shall be performed by personnel certified to work on system and shall be covered by vendor for the duration of this agreement.
- d. Contractor will provide support during normal business hours 8AM-5:00PM, Monday - Friday.

### **C. SUPPORT OF TECHNOLOGY REQUIREMENTS**

1. The Contractor shall provide hardware and software maintenance for the Teleform and RightFax equipment as required. All maintenance services shall be completed no later than the three business days.
2. The Contractor shall work with the site engineer or any third-party contractor, if necessary, until encountered hardware/software problems are resolved.
3. Problems that persist for a period of more than three (3) business days, as documented in online trouble call history, shall be augmented by on-site support until the problem has been resolved. If the Contractor is requested to provide on-site support but believes the problem can be most appropriately resolved remotely, the Contractor shall contact the Contracting Officer's Representative (COR) or his/her designee for a decision as to whether or not on-site support is required. The decision of the COR or designee is final.
4. The Offeror shall provide a toll-free number to initiate all trouble calls Monday through Friday from 8AM-5PM.

### **D. PERFORMANCE REQUIREMENTS**

1. The Offeror shall provide internal metrics to the COR as identified in section E of this Statement of Work (SOW).
2. The Offeror shall coordinate directly with the designated COR to receive technical direction and guidance for task performance. The COR performs evaluation of current information systems activities, plans and directs all phases of the work effort and ensures tasks are completed within negotiated time frames.
3. Warranty – All services performed, upgrades implemented, or parts provided shall be

warranted by the contractor for a period of at least 90 calendar days.

#### **E. REPORTING REQUIREMENTS**

The Contractor shall provide the Contracting Officer Representative (COR) with monthly electronic written progress reports, due the second workday following the end of each calendar month throughout the period of performance of the contract.

The progress report will cover all work completed during the preceding month and will present the work to be accomplished during the subsequent month. The report will identify any problems that arose and a statement explaining how the problem was resolved. This report will also identify any problems that have arisen but have not been completely resolved with an explanation.

#### **F. TRAVEL**

Travel expenses shall be the responsibility of the Contractor and shall not be charged to the Government.

#### **G. CONFIDENTIALITY AND NON-DISCLOSURE**

##### **VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY**

##### **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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors' 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 and any of its subcontractors' 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors electronic storage media for restoration in case any electronic equipment or data used by the contractor and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors' 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors are in receipt of a court order or other requests for the above mentioned information, that contractor and any of its subcontractors 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 and any of its subcontractors must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

#### 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 COR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.
- b. The contractor and any of its subcontractors shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or 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 and any of its subcontractors are 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 and any of its subcontractors agree 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 and any of its subcontractors are 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 and any of its subcontractors are 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 2 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 2 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 and any of its subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA'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 and any of its subcontractors' 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 and any of its subcontractors 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 and any of its subcontractors' procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor and any of its subcontractors 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 and any of its subcontractors must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The government reserves the right to conduct such an assessment using government personnel or another contractor and any of its subcontractors. The contractor and any of its subcontractors 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 and any of its subcontractors-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 and any of its subcontractors or any person acting on behalf of the contractor and any of its subcontractors, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors and any of its subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor and any of its subcontractors 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 and any of its subcontractors shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor and any of its subcontractors have access.
- b. To the extent known by the contractor and any of its subcontractors, the contractor and any of its subcontractors' 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 and any of its subcontractors consider 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 and any of its subcontractors 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 and any of its subcontractors 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 and any of its subcontractors process or maintain under this contract.
- b. The contractor and any of its subcontractors 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.
- b. The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or

termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

## **H. CONTRACTING AND ADMINISTRATION AUTHORITY**

The Contracting Officer is the only person authorized to approve changes or modify any of the requirements under this contract on behalf of the Government. In the event the Contractor affects any change(s) at the direction of any person other than the Contracting Officer that change shall be considered to have been made without authority and no adjustment in price shall be made in the contract to cover any increase in charges incurred as a result thereof. The Offeror shall submit all requests for modification of this contract and any inquiries pertaining to the administration of the contract to the Contracting Officer.

Contact for Technical Questions:

Mr. Junius Lewis  
Telehealth Program Analyst  
Department of Veterans Affairs  
Office of Care Coordination  
810 Vermont Avenue, NW  
Washington, DC 20420  
Telephone Number: (202) 461-6760  
E-mail: [junius.lewis@va.gov](mailto:junius.lewis@va.gov)

## **I. ELECTRONIC AND INFORMATION TECHNOLOGY STANDARDS**

### **INTERNET/INTRANET**

The contractor shall comply with Department of Veterans Affairs (VA) Directive 6102 and VA Handbook 6102 (Internet/Intranet Services).

VA Directive 6102 sets forth policies and responsibilities for the planning, design, maintenance support, and any other functions related to the administration of a VA Internet/Intranet Service Site or related service (hereinafter referred to as Internet). This directive applies to all organizational elements in the Department. This policy applies to all individuals designing and/or maintaining VA Internet Service Sites; including but not limited to full time and part time employees, contractors, interns, and volunteers. This policy applies to all VA Internet/Intranet domains and servers that utilize VA resources. This includes but is not limited to va.gov and other extensions such as, “.com, .edu, .mil, .net, .org,” and personal Internet service pages managed from

individual workstations.

VA Handbook 6102 establishes Department-wide procedures for managing, maintaining, establishing, and presenting VA Internet/Intranet Service Sites or related services (hereafter referred to as "Internet"). The handbook implements the policies contained in VA Directive 6102, Internet/Intranet Services. This includes, but is not limited to, File Transfer Protocol (FTP), Hypertext Markup Language (HTML), Simple Mail Transfer Protocol (SMTP), Web pages, Active Server Pages (ASP), e-mail forums, and list servers.

VA Directive 6102 and VA Handbook 6102 are available at:

Internet/Intranet Services Directive 6102

[http://www.va.gov/pubs/directives/Information-Resources-Management-\(IRM\)/6102d.doc](http://www.va.gov/pubs/directives/Information-Resources-Management-(IRM)/6102d.doc)

Internet/Intranet Services Handbook 6102

[http://www.va.gov/pubs/handbooks/Information-Resources-Management-\(IRM\)/6102h.doc](http://www.va.gov/pubs/handbooks/Information-Resources-Management-(IRM)/6102h.doc)

Internet/Intranet Services Handbook 6102 Change 1 – updates VA's cookie use policy, Section 508 guidelines, guidance on posting of Hot Topics, approved warning notices, and minor editorial errors.

[http://www.va.gov/pubs/handbooks/Information-Resources-Management-\(IRM\)/61021h.doc](http://www.va.gov/pubs/handbooks/Information-Resources-Management-(IRM)/61021h.doc)

In addition, any technologies that enable a Network Delivered Application (NDA) to access or modify resources of the local machine that are outside of the browser's "sand box" are strictly prohibited. Specifically, this prohibition includes signed-applets or any ActiveX controls delivered through a browser's session. ActiveX is expressly forbidden within the VA while .NET is allowed only when granted a waiver by the VA CIO \*PRIOR\* to use.

JavaScript is the preferred language standard for developing relatively simple interactions (i.e., forms validation, interactive menus, etc.) and Applets (J2SE APIs and Java Language) for complex network delivered applications.

## SECTION 508

The contractor shall comply with Section 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.

In December 2000, the Architectural and Transportation Barriers Compliance Board (Access Board), pursuant to Section 508(2) (A) of the Rehabilitation Act Amendments of 1998, established Information Technology accessibility standards for the Federal Government. Section 508(a)(1) requires that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), they

shall ensure that the EIT allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. The Section 508 requirement also applies to members of the public seeking information or services from a Federal department or agency.

Section 508 text is available at:

<http://www.opm.gov/HTML/508-textOfLaw.htm>

<http://www.section508.gov/index.cfm?FuseAction=Content&ID=14>