

**SPECIFICATION/STATEMENT OF WORK**  
**LEASE OF RADIOLOGY PICTURE ARCHIVE AND COMMUNICATIONS SYSTEM (PACS)**  
**FOR**  
**VISN 1**

**I. Background**

- A. The purpose of this contract is to provide VISN 1 with a comprehensive PACS to include software, hardware, training, and support on an ongoing cost per procedure basis. VISN 1 is comprised of the following locations: VA Boston Healthcare System (Jamaica Plain, West Roxbury, Brockton), Bedford VA Healthcare System, Northampton VA Healthcare System (Leeds and Worcester), West Haven VA Healthcare System, Providence VA Healthcare System, Manchester VA Healthcare System, White River Junction VA Healthcare System and Togus VA Healthcare System.

**II. Objectives**

- A. An overview of this SOW will include the following goals and objectives; VISN 1 has a need to continuously lease a PACS where all images performed or uploaded at a single site are available to all sites within the VA New England Network. The system will have high reliability and multiple redundancies (back up and disaster recovery). The system will have built in or integrated advanced visualization as well as integration with third party dictation systems and other medical devices and software, the system will also provide for a zero-footprint web-based viewing client for referring providers.

**III. Scope, Tasks, or Requirements**

- A. The general scope of the work the contractor will be performing is to supply a comprehensive PACS solution to include all servers, hardware, workstations, monitors, software, on-going upgrades, training, and technical support.
- B. If required the contractor will provide migration services for all existing images in the current legacy PACS. This migration will be performed without significant interruption to day-to-day operations and will be at least 90% complete prior to go-live on the new PACS
- C. The PACS will be configured such that each facility will have at least five years of on-site storage to allow for rapid (< 8sec) display of images. All images from all facilities within the VISN shall reside on a central archive which will in-turn have a mirrored disaster recovery archive located at another facility. The system should also be configured in such a way that software or other upgrades can be performed with no or minimal impact to end users.
- D. Workstations will be provided and maintained in both a standard diagnostic/reading format and in a display or non-diagnostic format. The hardware will be supported and maintained as needed by the contractor and will be refreshed at least every three (3) years or sooner if needed to support software/system changes. There will be additional quantities within the price / cost schedule to allow for future additional workstations as needed.
- E. All servers, RAID, and other “backend” hardware will be supplied and supported by the contractor and will be refreshed and expanded on an on-going basis.
- F. On-going upgrades and hardware refresh will be performed in an expeditious manner with minimal impact to the daily operations of the radiology service. All installed upgrades will

first be FDA approved and vetted in the field for compatibility with the VISN 1 Electronic Medical Record (EMR) and currently interfaced third party vendors.

- G. It is desirable that the contractor shall provide a dedicated field service engineer (FSE) for the VISN to allow for greater understanding of the unique needs and challenges presented by this installation.
- H. On-going Integration Services will be provided to include integration with third party medical devices and software as they are acquired and implemented by the VA.
- I. PACS software will provide for visualization and storage of all common image file formats encountered in the medical environment, to include static and moving image file types.
- J. The diagnostic visualization software will contain a base set of imaging tools to aid in diagnosis to include, but not limited to:
  - a. Multiplanar measurement
  - b. Volumetric measurement
  - c. Bone/vessel subtraction
  - d. Multiplanar reconstruction
  - e. 3D reconstruction
  - f. Image (prior study) linking/synchronization
- K. The PACS will provide advanced image visualization tools for diagnosis and display, these may be provided as a native toolset or as inclusion of a third-party integrated solution. Examples of advanced visualization are:
  - a. Vessel tracking and analysis
  - b. Prosthetics measurement and planning
  - c. Advance cardiac analysis
  - d. Computer Aided Diagnosis
  - e. Multimodality image fusion
- L. The PACS software will provide administrative management tools for image/study correction and maintenance such that when changes are made at the local level those changes are propagated at all levels/instances in the PACS storage environment.
- M. The PACS will provide a web based, zero footprint viewer for referring providers. This viewer should have a robust tool set and a look and feel similar to that of the PACS diagnostic viewer.

## **V. Delivery Schedule**

- A. Upon award the contractor will work with VISN 1 to establish a timeline for installation, migration, and cutover from the legacy PACS,
- B. Within 10 business days of award the government will conduct a post award conference with the awardee and the field representatives

## **VI. Government-Furnished Equipment and Government-Furnished Information**

- A. The VA-VISN 1 will furnish server space, electrical and environmentals as needed to meet the specifications of the vendor provided hardware.
- B. The VA-VISN 1 will provide network infrastructure (speed and access will be governed by OI&T and may be subject to limitations), network security/isolation instructions and structure, IP and naming conventions, and other networking/security assistance and instruction as required for project implementation.

## **VII. Security**

- A. The PACS will conform with all current VA required network and patient information security. It will be the contractor's responsibility to stay abreast of all current and future changes to this requirement.
- B.
- C. The Contractor is required to assure all personnel working on or remotely servicing the PACS meet VA security requirements and have been vetted through the appropriate channels. Please refer to VA Directive 6500, Cyber Security Program. The publication is located at [https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1)
- D.
- E. Remote connectivity and active system monitoring will conform to VA requirements and will be the responsibility of the contractor to monitor and maintain.

## **VIII. Place of Performance**

- A. This work will be performed at a Government site, specifically at the VAMC facilities within the VA New England Healthcare Network (VISN 1)

## **IX. Period of Performance**

- A. The period of performance for this requirement is a one (1) year base with the option to extend the term of the contract for an additional nine (9) years. The exercise of the options is subject to the availability of funds and will be exercised utilizing FAR Clause 52.217-9, Option to Extend the Term of the Contract. .
- B. Work will be performed 365/24/7 with the goal of providing 99.99% up-time with minimal impact to normal hours of operation (M-F 0700-2200 hrs.)

## **X. Contractor's Responsibility**

- A. Contractor will provide qualified support personnel with familiarity and knowledge of VA network and security requirements.
- B. The Contractor will be responsible for all software and hardware updates and upgrades during the performance period of this contract.
- C. The contractor is responsible for keeping equipment in good working order and shall provide all maintenance, repairs, and upgrades to the equipment as required keeping it in optimal condition.
- D. The Contractor will provide services in accordance with ethical, professional and technical standards of the health care industry.

## **XI. Services Not Covered**

- A. Any work other than as specified in the contract shall be identified as a non-priced task, and if determined by the Contracting Officer to be within the overall scope of the contract, work shall be added by a modification to the contract.
- B. Any work requested that is identified as outside the scope of the contract shall be addressed by the facility as a separate procurement.

## **XII. Federal Holidays Observed By The VA**

New Year's Day	1 January	Labor Day	1st Mon. in Sept
M L King's Birthday	3rd Mon. in Jan	Columbus Day	2nd Mon. in Oct
President's Day	3rd Mon. in Feb	Veterans Day	11 November
Memorial Day	Last Mon. in May	Thanksgiving Day	4th Thurs. in Nov
Independence Day	4 <sup>th</sup> of July	Christmas Day	25 December

1. Also included would be any other day specifically declared by the President of the United States to be a National Holiday.
2. When a *holiday* falls on a Sunday, the following Monday shall be observed as a legal holiday by U.S. Government agencies. When a holiday falls on a Saturday, the preceding Friday shall be observed as a legal holiday.

## **XIII. Identification, Parking, Smoking, and VA Regulations:**

- A. The Contractor's FSEs shall wear visible identification at all times while on the premises of the VAMC. It is the responsibility of the contractor to obtain and pay for parking as may or may not be required. The VAMC does not guarantee on-site parking. The VAMC will not invalidate or make reimbursement for parking violations or charges for the Contractor under any conditions. Smoking is prohibited inside any buildings at the VAMC and only in designated areas on campus. Possession of weapons is prohibited. Enclosed containers, including tool kits, shall be subject to search. Violations of VA regulations may result in citation answerable in the United States (Federal) District Court, not a local district, state, or municipal court.

## **XIV. Orientation For Contractor Employees**

- A. Contractor will attend an orientation meeting as arranged by the Contracting Officer's Representative (COR) on-line or other written training may be substituted at the discretion of the COR.. The VA will schedule this meeting and it will include discussion of the following topics: (VA will provide information to the contractor regarding these topics and will document the meeting)
  1. Fire and Safety
  2. Infection control
  3. Disaster procedures
  4. Other
- B. The Contractor will be responsible to ensure that Contractor employees coming to the work site will receive the information required above.
- C. The Contractor will be responsible to ensure Contractor employees providing work on this contract are fully trained and completely competent to perform the required work.

## **XV. Contractor Personnel Security Requirements:**

All contractor employees who require access to the Department of Veterans Affairs' Contractors computer systems or have access to sensitive information shall be the subject of a background investigation. The contractor is encouraged to have its employee immediately download the background investigation packet

from [http://www.osp.va.gov/Security\\_and\\_Investigations\\_Center\\_FF.asp](http://www.osp.va.gov/Security_and_Investigations_Center_FF.asp) upon notification of contract award. A contractor's employee shall not commence working at VA under contract until the Contracting Officer receives notification from the VA Office of Security and Law Enforcement that the contract employee's application was received complete. A favorable adjudication from the VA Office of Security and Law Enforcement must be received in order for a contractor employee to continue contract performance. This requirement is applicable to all subcontractor personnel.

**a. Position Sensitivity** - The position sensitivity has been designated as low risk.

**b. Background Investigation** - The level of background investigation commensurate with the required level of access is National Agency Check with Written Inquiries (NACI).

**c. Contractor Responsibilities**

1. The contractor shall bear the expense of obtaining background investigations. If the Office of Personnel Management (OPM) conducts the investigation, the contractor shall reimburse VA within 30 days. If timely payment is not made within 30 days from date of bill for collection, then VA shall deduct the cost incurred from the contractors 1<sup>st</sup> month's invoice(s) for services rendered.

2. It is imperative for the contractor to provide, at the request of VA, a listing of contractor personnel performing services under the contract in order for the background investigation process to commence. This list will include name (first, middle, last) social security number; date of birth; city, state, and country of birth.

3. The contractor or their employees shall submit a complete background investigation packet. Additional guidance and information in completing the required forms, and examples of the forms, can be found at [http://www1.va.gov/VABackground\\_Investigations/page.cfm?pg=2](http://www1.va.gov/VABackground_Investigations/page.cfm?pg=2).

7. All contractor employees and subcontractors are required to complete VA's Privacy training annually. All Contractor employees and subcontractors requiring access to VA computer network are required to complete Cyber Security training courses annually either on-line or hard copy. Documented proof must be provided to the Contracting Officer.

8. The contractor will notify the COR immediately when their employee(s) no longer require access to VA computer systems.

**d. Government Responsibilities**

1. The contracting officer will request the contractor employee's background investigation by the Office of Security and Law Enforcement.

2. The Office of Security and Law Enforcement will notify the contractor with instructions for the contractor's employees, coordinate the background investigations, and notify the contracting officer and contractor of the results of the investigations.

3. The VA facility will pay for requested investigations in advance. A bill for collection will be sent to the contractor to reimburse the VA facility. The contractor will reimburse the VA facility within 30 days. If timely payment is not made within 30 days from date of bill for collection, then VA shall deduct the cost incurred from the contractors 1<sup>st</sup> month's invoice(s) for services rendered.

4. The current fees associated with background investigations are \$210.00 each for low level investigation, \$850.00 each for medium level investigation, and \$2,900.00 each for high level investigation.

## **XVI. Security Training**

Due to the increased emphasis on privacy and information security, the following special contract requirements are established and hereby made part of the contract entered into with the Department of Veterans Affairs.

a. Privacy Training: Contractor and their sub-contractors assigned work under the contract are required to receive annual training on patient privacy as established by HIPAA statutes. Training must meet VHA's and the Department of Health and Human Services Standards (HSS) for Privacy of Individually-identifiable health information. Contractor shall provide documented proof to the contracting officer that all employees assigned work and/or having access to protected health information have received annual training. Proof of training is to be forwarded to the COR. Training can be obtained through <http://www.insidelms.va.gov/index.shtm>. An account must be set up in order to access the training site by visiting <https://www.tms.va.gov/plateau/user/login.jsp> page and contacting the local LMS Administrator or contacting the VA TMS Help Desk by phone at 1-866-496-0463 or via e-mail at [vatmshelp@va.gov](mailto:vatmshelp@va.gov). For contractors and sub-contractors who do not have access to VHA computer systems, this requirement is met by receiving VHA National Privacy Training, other VHA approved privacy training or contract furnished training that meets the requirements of the HHS standards.

b. Rules of Behavior for Automated Information Systems: Contractor personnel having access to VA Information Systems are required to read and sign a Rules of Behavior statement which outlines rules of behavior related to VA Automated Information Systems. The COR will provide, through the facility Information Security Officer (ISO), the Rules of Behavior to the contractor for the respective facility.

c. VA Information Security Awareness Training: Each contractor assigned work under the contract is required to receive and document completion of VA training on Information Security. Training can be obtained through <http://www.insidetms.va.gov/index.shtm>. An account must be set up in order to access the training site by visiting <https://www.tms.va.gov/plateau/user/login.jsp> page and contacting the local LMS Administrator or contacting the VA TMS Help Desk by phone at 1-866-496-0463 or via e-mail at [vatmshelp@va.gov](mailto:vatmshelp@va.gov). Contractor shall provide documented proof to the COR that all contractor employees servicing a VA contract have received annual training.

## **XVII. Access to VA Information and VA Information Systems**

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.

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.

## **XVIII. 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 COR.

## **XIX. 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/subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or 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, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

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 3 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.

## **XX. Security Incident Investigation**

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

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

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

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

## **XXI. 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.

## **XXII. 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.

### **XXIII. 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 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.