DRAFT- PERFORMANCE WORK STATEMENT (PWS)

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Financial Services Center (FSC) is a franchise fund site authorized pursuant to the Government Management Reform Act of 1994 (Public Law 103-356). The Act authorizes designated agencies to provide certain common administrative support services on a reimbursable basis both internally and to Other Government Agencies. In 2006, permanent status was conferred upon the VA Franchise Fund under the "Military Quality of Life and Veterans Affairs Appropriations Act 2006," Public Law 109-114. Consequently, the VA FSC receives no federally appropriated funding, and is required to market VA-FSC services to customers.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement (PWS), the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. 10 U.S.C. § 2224, "Defense Information Assurance Program"
3. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
4. **42 U.S.C. § 2000d "**Title VI of the Civil Rights Act of 1964"
5. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
6. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
7. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012
8. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
9. VA Handbook 6500.6, "Contract Security," March 12, 2010

3.0 SCOPE OF WORK

The Contractor shall provide all necessary personnel, equipment (to include but not limited to, captioning software and laptop, as requested on an as needed basis), and materials to perform the work described in the PWS. The services required include:

1. Oral spoken English into signed English and American Sign Language (ASL),
2. Pidgin Signed English (PSE)
3. Oral with sign or ASL (in reverse) back to oral English
4. Video Remote Interpreting: remotely located professional sign language interpreter to provide real-time interpreting services between hearing impaired individuals and hearing individuals who are located in the same room
5. Remote CART: The audio feed of a meeting or training is transmitted via microphone by the speaker over a phone line to the interpreter in a remote location and is transmitted to a hearing impaired employee's computer through a modem or at a website on the internet provided by the interpreter company.

The Government reserves the right to videotape the signing and use as deemed necessary.

A sample list of onsite interpreting events is listed below and subject to change dependent upon the FSC requirements:

- Staff meetings,
- Commemorative programs,
- Award ceremonies,
- Safety talks,
- On the job training (OJT),
- Committee meetings,
- Discussions on work procedures, policies, or assignments for formal and informal settings,
- Special event programs
- Mid-year performance discussions, annual performance appraisals, disciplinary discussions,
- Basic staff training, classroom training, formal training,
- Interviews,
- All hands meetings, and other ad hoc assignments similar in nature on an as-need basis.

4.0 INTERPRETER QUALIFICATIONS:

The certifications required include:

All interpreters shall have a certification obtained from a recognized certifying organization. Certification for interpreter providers must be obtained from organizations such as the Registry of Interpreters for the Deaf (RID, NIC, NIC Advanced, NIC Master, CI, CT, CI/CT or CSC), the National Association of the Deaf (NAD), or a recognized State agency. Interpreters shall have, at a minimum, a proficiency level of III unless the nature of the assignment requires a higher level. All interpreters shall conduct themselves according to the NAD and/or RID Code of Ethics.

Interpreter(s) shall be dressed in business attire. It is understood that the interpreter(s) shall not act as an agent or employee of the Federal Government or FSC. The interpreter(s) shall not discuss personal business; distribute personal business cards or promotion of personal “cause” while on assignment in order to develop clientele from assignments originating from the Federal Government or FSC. The interpreter(s) shall adhere to the Federal Government’s rules of protocol, ethics, procedures and professionalism while on assignment at FSC. Any professional conduct in question warrants an immediate review at the discretion of the COR and the Contracting Officer.

The COR or designee will contact the Contractor POC primarily via e-mail, and secondarily via telephone or facsimile, with requests for, changes to or cancellations of interpretation services

5.0 SPECIFIC TASK

Contractor shall provide interpreter services for requests received at least 2 days in advance. Business hours are defined as Monday through Friday (08:00AM – 04:30PM), except Federal Holidays. Upon receipt of request, the Contractor shall provide to the COR or designee in writing (email is acceptable) receipt confirmation within one (1) business day of receipt of request. The name of the assigned interpreter(s) shall be provided to the COR or designee in writing (email is acceptable) no later than one (1) business day prior to start of assignment.

If, however, the Government should require interpreter services with less than 2 day notice, the Contractor shall attempt to provide an interpreter if possible. The Government understands that the Contractor may not always be able to comply with short notice request. Inability to fill a short notice

request will not be held adversely towards contractor performance. Contractor's acceptance must be given within two (2) business hours of the time the request was placed during FSC's business days. If the Contractor fails to accept within the time specified, the Government will consider the assignment refused. If the Contractor accepts the request, the agency shall be billed at the hourly rate established. Travel to the FSC Waco location will not be expected. In the event an interpreter is required to travel to Waco for an event travel reimbursement is authorized. The Contractor shall provide the COR or designee the name(s) of the interpreter(s) as soon as possible but no later than two (2) business hours prior to the assignment.

In general, two (2) interpreters shall be required for assignments lasting more than two (2) hours; requiring detailed or technical interpreting or captioning; or involving general audiences that last more than one (1.5) hours.

Contractor and its interpreter(s) shall keep all assignments. Canceled assignments are not tolerated except for true emergencies. If the scheduled interpreter(s) cancels an assignment, the Contractor shall provide a substitute interpreter(s) and notify the COR or designee within 24-hours. If the Contractor is not able to provide an interpreter(s), the contractor shall notify the COR or designee. If the Contractor interpreter does not meet qualifications or fails to appear at the event location within twenty (20) minutes of the scheduled assignment start time, the assignment shall be cancelled. The Government shall not incur any charges associated with such cancellations. Interpreters must arrive in time to be at the designated assignment at the determined start time. The Interpreter must allow sufficient lead time prior to the assignment start time to enter the secured grounds, park, be assigned an access badge and be escorted to the assignment location within the facility (approximately 10-15 minutes).

Government may cancel the services no less than 3 days before the scheduled appointment without penalty or charges assessed. If the Contractor is notified of a cancellation less than 3 days prior to the scheduled assignment but, before interpreter(s) arrival on site, the Contractor may invoice for a two (2) hours maximum. If upon arrival to the assignment and service is no longer required or the assignment ends early, the interpreter(s) shall notify the COR or designee. If the interpreter(s) cannot reach the COR or designee and the original scheduled time expires or the 2-hour minimum passed (whichever occurs first), the interpreter may leave and the Contractor may invoice for a two (2) hour minimum. The 2-hour minimum does not apply if the assignment was scheduled for less than 2 hours or if the interpreter leaves prior to notifying the COR (or designee) or before the times stated above.

Assignments lasting more than two (2) hours shall be invoiced in quarter (¼) hour increments for the actual duration of the assignment, not the estimated duration requested by the COR or designee when coordinating and scheduling the request.

The assignment is considered complete when the later of the following occurs:

1.) Conclusion of event equals or exceeds the estimated duration specified when scheduling the request

2.) The COR or designee releases the interpreter(s).

For any assignment over 6 hours in duration and lunch breaks are offered during the assignment(s) for Deaf and/or Hearing impaired employee(s), the same time for lunch breaks apply to the interpreter(s) and shall be included within the assignment(s) as paid time. Otherwise time taken for meals shall not be billed. Other breaks are billable.

6.0 PERFORMANCE DETAILS

1. PERFORMANCE PERIOD

The period of performance shall be one year base and four (4) one year option periods

PERIOD	DATE
Base	TBD
Option Period One	TBD
Option Period Two	TBD
Option Period Three	TBD
Option Period Four	TBD

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

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

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

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

Inclement weather, Emergency or Unscheduled Closure: Interpreters will not report to an assignment if the federal government is closed due to inclement weather, emergency or in the event of an unscheduled closure. No cancellation fee or charges shall be assessed. The contractor will not bill the government for interpreter service hours when the government is closed due to inclement weather or emergency. Delay and closure information status can be found at http://www.fsc.va.gov/fsc/index.asp. In addition the Contractor point of contact (POC) may call the number for Center wide information at (512) xxx-xxxx or toll free at 1-866-xxx-xxxx for delay or closure status.

2. PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA FSC located at 7600 Metropolis Drive, Building 5 Austin TX 78744. On rare occasions, translation services shall be required at VA FSC Waco, located at 4800 Memorial Drive, Building 92, Waco, TX 76712, or at another location as determined by the Government. The COR will give explicit instructions as to where and when the services will be required. Services will need to be performed in offices, training rooms, auditoriums and conference rooms. **Travel reimbursement is not authorized for FSC locations in the Metro Austin Area.**

3. Invoices

Contractor shall provide monthly invoices by email to the COR for review and concurrence before submitting the invoice for reimbursement. The invoice shall detail the dates and times the services were performed, and total value. Once the invoice is approved it will be approved for submission via TBD.

4. SCHEDULE OF DELIVERABLES

Task	Deliverable Description
	Interpreter Services Contact with COR or Designee at each visit Inspection: random Acceptance: At task completion

a. GENERAL REQUIREMENTS

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

The VA-FSC is a secure facility located in Austin, Texas. Individuals providing interpreter services will not be processed for Government PIV Badges because they will not receive access to VA Networks. The VA-FSC facility has secure access control; therefore, the interpreter will need to clear security and receive a visitor's badge. The interpreter will receive an escorted visitor's badge from security and will be escorted by a VA FSC employee while in the facility. Upon arrival of the interpreter to the VA-FSC facility, entry control security guards will request photo identification and direct the instructor to the visitor parking. If the Interpreter becomes a regular interpreter for the FSC they can choose to provide their personal information to the FSC Security Staff for a local background investigation to receive unescorted access.

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

5. CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the facility to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.

b. The Contractor shall bear the expense of obtaining local background investigations.

c. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

d. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

1.2 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

Performance Objective	Required Service	Acceptable Performance Levels	Impact
On-Time Deliverables	The contractor shall be responsible for delivering a series of deliverables in accordance with the schedule outlined in this task order.	95% on-time delivery (unless Government causes delay)	Contractor failure to meet this performance standard may result in negative feedback in the contractor's performance evaluation. For every 1% below the 95% standard, the contractor will be deducted 10% off the deliverable cost.
Project Staffing	Contractor personnel shall possess necessary knowledge, skills and abilities to perform all required tasks. Interpreters shall be provided as outlined in stated in PWS.	98% of the time	Contractor failure to meet this performance standard may result in negative feedback in the contractor's performance evaluation. The CO may authenticate certification and education requirements in Section 6.6. The CO has the right to refuse contractor staff based upon false credentials anytime during the performance of the contract. For every 1% below this 98%

			standard, the contractor shall provide a remediation plan.
Timely Conflict Resolution	The contractor shall notify the Government of any problems, disputes, or other conflict involving or affecting performance within one (1) business day.	98% of conflicts are acknowledged within one (1) business day (Unless Government causes delay)	Contractor failure to meet this performance standard may result in negative feedback in the contractor's performance evaluation. For every 1% below this 98% standard, the contractor shall provide a remediation plan.

Surveillance: The COR will evaluate the performance objectives through periodic inspections during each service month.

Standard: The contractor shall perform all work required in a satisfactory manner in accordance with the appropriate PWS paragraph.

Procedures: The Government will inspect all performance objectives a ensure contractor compliance with the appropriate paragraphs of the PWS. The contractor will record the monthly results of inspection, noting the date and time of inspection. If inspection indicates unacceptable performance, the PM will be notified of the deficiencies for correction. The contractor shall be given an appropriate amount of time after notification to correct the unacceptable performance; the COR may approve additional time if the COR considers additional time appropriate. If deficiencies are not corrected within the required time frame the COR shall notify the CO.

The contractor shall notify the Government of any problems, disputes, or other conflict involving or affecting performance within one (1) business day.

The Government reserves the right to alter or change the surveillance methods at its own discretion.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

FACILITY/RESOURCE PROVISIONS

All procedural guides, reference materials, and program documentation for the project and other Government applications will be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the Contracting Officer Representative (COR) as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B

1.3 GOVERNMENT FURNISHED PROPERTY

Not Applicable

1.4 GOVERNMENT RESPONSIBILITIES

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

1. The Security Investigations Center will require the following forms from the Contractor or to the Contractor's personnel:
    a. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
    b. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
    c. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award. (DVA Memorandum – Electronic Fingerprints is filled out by the VA Facility that took the electronic fingerprints)
    d. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). (The SF85 does not need to be uploaded because OPM is going paperless and the contractor will complete this questionnaire online when the e-QIP link is sent.) (DVA Memorandum – Electronic Fingerprints is filled out by the VA Facility that took the electronic fingerprints) (Please be advised that the contractor will need all the necessary information easily accessible as the website will time out and they can lose the information they inputted if they take too long to fill it in.)The Contractor personnel shall submit all required information related to their background

investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).

e. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.

f. The SIC will then upload the e-QIP signature pages to e-QIP and release the case file to OPM for investigation.

g. The SIC will notify the COR, CO, and Contractor after adjudicating the results of the background investigations received from OMB.

(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 5 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 10 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 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/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 COR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or contractor/ subcontractor-owned equipment or software on 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 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.

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 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-days' 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 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.

(End of Clause)