STATEMENT OF WORK (SOW)
**as of 01/10/2016**

| | |
|---|---|
| **Contract Number:** | *(completed by the CO at time of award)* |
| **Task Order Number:** | *(completed by the CO at time of award if a TO)* |
| **IFCAP Tracking Number:** | **654-17-1-5052-0001** |
| **Follow-on to Contract and Task Order Number:** | Not Applicable |

## 1. Contracting Officer's Representative (COR).

| | |
|---|---|
| Name: | LaRena Schwartz |
| Section: | Human Resources Management Service |
| Address: | 975 Kirman Avenue, Reno, NV 89502-2597 |
| Phone Number: | (775) 829-5649 |
| Fax Number: | (775) 829-5656 |
| E-Mail Address: | LaRena.Schwartz@va.gov |

## 2. Contract Title. Court reporting services.

## 3. Background.

3.1. The VA Sierra Nevada Health Care System (VASNHCS), Reno, Nevada, Human Resources Management Service is interested in contracting with a company to provide court reporting services/transcription for hearings/arbitrations. It is the intent of this document to establish a non-personal performance-based service contract for the VA Medical Center.

3.2. Invoices: Unless another form of payment is agreed upon by the Contracting Parties (i.e., Government Credit Card), invoices received from the Contractor must provide the unique Task Order Number that will be given for each requirement issued under this contract.

3.2.1. Contractor shall be required to invoice through the Tungsten Network (OB10) link at http://ob10.com/us/en/veterans-affairs-us/. Additional information regarding OB10 shall be provided upon award. The contract shall have current registration in the System for Award Management (SAM) for this solicitation; Ural: www.sam.gov.

3.2.2. Payment of invoices are made in arrears, upon certification of invoice. Invoices shall be submitted in accordance with the invoice clauses. Ensure the obligation # and a company invoice # is included on the invoice.

## 4. Scope.

4.1 The place of performance is the VA Sierra Nevada Health Care System, 975 Kirman Avenue, Reno, Nevada. The work will be performed during the business hours of 7:30 a.m. to 4:30 p.m., Monday through Friday. The work schedule is intermittent/on-call/as-needed. Full business days/weeks may be required at times. At other times, one-two full or partial workdays may be required. At other times, no work will be provided. Court reporter must be available at a moment's notice during VASNHCS normal business hours.

4.2. The contractor will not be required to work on any Federal holidays. The ten holidays observed by the Federal Government are: New Year's Day; Martin Luther King, Jr.'s Birthday; President's Day; Memorial Day; Independence Day; Labor Day; Columbus Day; Veterans Day; Thanksgiving Day, and Christmas Day and any other day specifically declared by the President of the United States to be a national holiday. In the event a holiday falls on a week end day (Saturday or Sunday), the normal observance is the connecting weekday.

## 5. Specific Tasks.

5.1. Persons who are selected to perform court reporting services must be a Certified Court Reporter (CCR). The Contractor shall provide all personnel, equipment, tools, materials, supplies, vehicles, certifications, supervision, and all other technologies and technical services to provide Court Reporter services for the VA Medical Center (VAMC) upon request. The services may be required for, but not limited to: Administrative Investigations, Disciplinary Appeals Boards, Equal Employment Opportunity (EEO) hearings or Merit Systems Protection Board (MSPB) hearings, Office of Resolution Management, or Regional Counsel requirements. It will also be used for any other meetings that require legal documentation.

5.2. The Contractor shall provide only qualified certified Court Reporters to perform these services. Only one Court Reporter shall be assigned to each administrative process from its beginning to end. If an unforeseen emergency should occur that would require absence of the assigned Court Reporter, the proposed substitute shall have comparable qualifications to those of the person being replaced. The contractor shall provide a detailed explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any additional information requested by the Contracting Officer (CO).

5.3. The Contractor must provide competent, efficient Court Reporters who are experienced and have the necessary training and education in Court Reporting with adequate and appropriate court reporting equipment, in order to produce accurate, timely, appropriately bound and indexed transcribed testimony from witnesses in these processes. Court Reporters must have at least one year experience in court reporting and have the necessary training and education required in Court Reporting along with adequate and appropriate court reporting equipment, in order to produce accurate, timely, appropriately bound and indexed transcribed testimony from witnesses in these processes. The Court Reporter must hold the certification as a National Court Reports Association (NCRA) Registered Professional Reporter (RPR), or equivalent (determination of equivalency at the discretion of VAMC). Appropriate credentials must be provided within one (1) week upon request. The Court Reporter shall be punctual and present at all proceedings, demonstrate a professional demeanor, and provide all the necessary equipment to perform their duties and accomplish the deliverables described below. VAMC will provide seating and a work surface for the Court Report to perform their duties. The court reporter shall read portions of transcript during the proceedings at the request of the board or other presiding body, and ask speakers to clarify inaudible statements. Proceedings may occur over multiple days and the services of the Court Reporter may be needed for varying lengths of time each day. Court Reporters who have experience with the Administrative Investigation Board (AIB) process, Equal Opportunity Hearing, Human Resources Management Merit System Protection Board (MSPB) or arbitration hearings are preferred in the performance of this contract.

5.4. The Contractor shall assume full responsibility for the protection of its personnel furnishing services under this contract, in accordance with the personnel policy of the Contractor. To carry out this responsibility, the contractor shall provide the following for these personnel:

- Worker's compensation
- Professional liability insurance NOTE: A copy of liability insurance on an individual must be presented to the CO prior that person being assigned to this facility.
- Health examinations
- Income tax withholding, and
- Social security payments

5.5. The parties agree that such personnel shall not be considered VA employees for any purpose and shall be considered employees of the contractor. Note: To be in compliance with Homeland Security standards, each Court Reporter assigned to work at this Medical Center shall be subject to the same rules and regulations as all contracted employees. Parking is allowed only in those areas not designated for patient use. All traffic laws and parking rules on the grounds are strictly enforced. Failure to follow these laws and regulations may result in a citation being issued that will have to be resolved through the Federal Court system. Prior to reporting to work, the contracted employee will need to contact the designated COR who will take him/her to the on-site PIV Officer. This Officer will issue a temporary ID badge to the contracted employee, who in turn, will properly display the badge while working at the Medical Center. Upon completion of the assignment, the employee will return the badge to the PIV Officer.

5.6. The contractor shall ensure that all assigned court reporters perform all work in a professional business-like manner and in accordance with the best standards of the reporting profession and the contractor.

5.7. Removing Employees for Misconduct or Security Reasons: The Government, may, at its sole discretion, direct the contractor to remove their employee from the Medical Center or CBOC facilities for misconduct or for security

reasons. Removal does not relieve the Contractor the responsibility to continue providing the services required under this contract. The CO will provide the contractor with a written explanation to support any request to remove an employee.

5.8. In any instance where the contractor has knowledge that any actual or potential situation may delay or threaten to delay the timely performance of this contract, the contractor shall immediately notify the COR and the CO. This notice shall include all relevant information and corrective actions that are being taken. The Government reserves the right to hold the contractor fully accountable for problems incurred as a result of such delays, including denial of delivery time extensions, if such notification is not provided.

5.9. If, after notice of a proposed hearing, the Contractor's employee does not appear at the time and place specified for the hearing, the contractor shall be responsible for finding another equally qualified individual for the hearing. The Contractor may be responsible for the reimbursement to the VA Medical Center for any expenses over and above that which would have been incurred if the Contractor had performed in accordance with this Performance Work Statement. The Government may deduct such expenses from any other sums due or that may become due the Contractor.

5.10. The term "Administrative Investigation" (AI) refers to a systematic process for determining facts and documenting evidence about matters of significant interest to VA. AIs are conducted to collect and analyze evidence to determine what actually happened and why it happened, so that individual and systemic deficiencies can be identified and effectively corrected. These investigations are governed by VA Directive 0700, Administrative Investigations and VA Handbook 0700, Administrative Investigations. These investigations are established by the Medical Center Director as the convening authority. Administrative Investigation Boards are not scheduled in advance; therefore, short notice will be provided for the need of transcription services. Once scheduled, the schedule may change or even be cancelled at anytime up until the time scheduled because of unforeseen events that may arise.

5.10.1. EEO Hearings and MSPB and/or arbitration hearings are similar processes and are established by a judge or other government source. EEO Hearings may be scheduled a few weeks in advance; MSPB hearings may be scheduled several weeks to a month or more in advance. These hearings may also have to be rescheduled or cancelled because of unforeseen events.

5.10.2. The number of witnesses can only be estimated in advance of the start of the process, and may change during the course of the investigation or activity.

5.11. Transcription Format:

5.11.1. The Court Reporter shall index each individual transcript and include behind each bound testimony a tabbed index stating "WORD INDEX." The evidence and information gathered during the course of the investigation shall be organized in an appropriately indexed investigative file that includes a numerical or alphabetical list of each time a symbol, number or word was used and the page number and line number.

5.11.2. The transcribed testimony product must be accurate, double-spaced, printed, and bound in a satisfactory manner, according to accepted standards for court reporting, which at a minimum includes one original and one copy of each witnesses' testimony. All are to be securely fastened with metal prongs (not plastic binding). Line numbers must be listed in the left margin and the page number in the bottom right corner of each page. The court reporter shall include their signed, dated, and officially sealed certificate as the last page of the testimony.

5.11.3. An "ACKNOWLEDGEMENT" sheet shall be included as the last page of each testimony to include a certification statement at the top that the testimony is accurate to include blanks for a date to be filled in and a signature block for each. The second half of this acknowledgement sheet shall include a place for corrections, i.e., Page No. ____, Line No. ____, and a blank to write in the corrections.

5.11.4. Visible Black Character.

5.11.4.a. A Visible Black Character is defined strike-able and visible characters and includes any printed letter, number, symbol, and/or punctuation mark excluding any or all formatting (e.g., bold, underline, italics, table structure, formatting codes). All visible black characters can be seen with the naked eye as a mark, regardless of whether viewed electronically or on a printed page.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | C | D | e | f | G | H | I | j | k | l | m | n | o | p | q | r | s | t | u | v | w | X | y | z |

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | < | > | ? | ÷ | ± | | | | |
| ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ‘ | , | . | / | “ | | | | |

5.11.4.b. Visual Black Character (VBC) Line or ASCII no Spaces Line. A VBC Line is defined as the total number of characters you can see with the naked eye, divided by 65. It includes any character contained within a header or footer. Spaces, carriage returns, and hidden format instructions, such as bold, underline, text boxes, printer configurations, spell check, etc., which are not counted in the total character count. A VBC Line is calculated by counting all visual characters and simply dividing the total number of characters by 65 to arrive at the number of defined lines.

5.11.5. All documents shall by typed using black ink on white good quality paper. Paper shall be 8 ½ by 11 inches with ruled margin of 1.5” at the left side and ruled margin of 0.5” at the right side, and a ruled margin of 1” at the top and bottom . A number indicating each line of the document upon each page, i.e., 1 to 25 inclusive, shall be printed at the left side of the left marginal line of the original and copies of the transcript.

5.11.6. Typing shall be 10 letters to the inch, 25 lines to the page, exclusive of pager number, with 2 single spaces between lines. Whenever testimony is continuous, requiring more than 1 line, the typing shall begin as close as possible to the left ruled marginal line. Words shall be properly hyphenated when necessary.

5.11.7. In the original and each copy of the transcript, outside the ruled margin, the cover page and each subsequent page of the transcript (including the Certificate and Acknowledgement) shall show the name, address, and phone number of court reporting service centered at the bottom and the page number of the transcript in the bottom right corner.

5.11.8. The paging of the transcript shall be in a single series by consecutive numbers regardless of the number of days consumed in the investigation, hearing, etc.

5.11.9. The original transcript and (1) copy shall be authenticated by the Official Reporter by a certificate page in the following form, which shall be included before the Acknowledgement:

CERTIFICATE

Certificate of Reporter:

Name of Hearing/Type of Proceeding:

Docket Number:

Place of Hearing:

Date of Hearing:

I, (name of transcriber), do hereby certify that said witness (name of witness), whose testimony appears herein, was duly sworn, that said transcript is a true record of the testimony given by said witness. I further certify that I am neither attorney, nor counsel for, nor related to or employed by, any of the parties in which this action is taken and further that I am not a relative or employee of any attorney or counsel employed by the parties hereto or financially interested in the action.

_____ _____

Name and Signature of Court Reporter Date

_____

Name of Company

5.11.10. Retention of Notes and Transcripts: The Contractor agrees that all recordings, stenographic notes, or their equivalent, taken in connection with the services rendered under this contract, and typed plate made therefrom, shall be filed and held by the contractor, subject to authority and control of the Department of Veterans Affairs for a period of one year.

5.12. Should the Contractor cause the Government to re-hear any case or hearing or other proceeding, the Contractor shall provide the reporting services at that re-hearing at no cost to the Government. In addition, the Contractor shall be

liable for all Government expenses, claimant expenses and attorneys fees incidental to the re-hearing. Although not a comprehensive list of examples, causes for re-hearings may include:

- Loss of original recordings, transcripts or photocopies.
- Failure of the contractor's court reporter/stenographer to appear, and a substitute cannot be obtained in sufficient time.
- Receipt of products by the Government in such poor condition as to be unusable.
- Attempted use of electronic recording equipment which does not conform to the requirements noted herein.
- Failure of the Contractor to deliver transcripts (original and 1 copy) within three (3) business days after a hearing.

## 6. Performance Monitoring

The Government will evaluate the contractor's performance under this contract using the method of surveillance specified below. All surveillance observations will be recorded by the government. When an observation indicates defective performance, the COR will provide the Contractor with a copy of the record of the observation.

The government shall reduce contractor invoices by 15% in the event the contractor's level of performance falls below 90% of the expected performances as outlined in this PWS. Confirmation of these delinquent performances will be made known to the contractor immediately upon discovery.

| Para No. | Performance Objective | Standard | Acceptable Quality Level |
|---|---|---|---|
| 4.1-5.9, 5.12 | Full Representative at all scheduled hearings | A trained and experienced transcriptionist with past experience in AIB's, EEO Hearings, and MSPB Hearings is prompt and present for all scheduled hearings with functioning recording equipment | Not late to more than 1 hearing per year. All direct and indirect costs associated with re-hearings will be reimbursed to the Government. |
| 9.d. | Timely Delivery | Transcribed paper copies (no digital, e-mailed, etc.) of reports are delivered as stated in paragraph 9.d. | Less than 1% of the reports are late. |
| 5.11 | Error-Free Deliverables | Hearing recordings, transcriptions and photocopies accurately reflect that which transpired at the hearing, the individual testimonies are appropriately bound in a sturdy plastic folder, clear front cover, with metal prongs, include an acknowledgement/errata sheet inserted at the front, and a word index behind the testimony. | Less than 1% of recordings, transcriptions and photocopies must be returned for correction by the Contractor. All corrections are made and re-delivered to the COR within five (5) days of notification of the need for correction. |

The COR will assure Contractor quality with inspection from the VA Sierra Nevada Health Care System Employee and Labor Relations Human Resources Specialist(s) who are the facility advisors for each specific case.

## 7. Security Requirements

Contractor Security Requirements (Handbook 6500.6):

*Program Directors and Facility Directors, through the ISO,* are responsible for: Reviewing proposed SOWs to ensure that the resulting contracts and service providers sufficiently define information security responsibilities, provide a means to respond to information security problems, and include a right to terminate the contract if it can be shown that the contractor does not abide by the information security terms of the contract; Assisting the COTR and CO in verifying and validating that appropriate security measures are implemented and functioning as intended in accordance with the contract or agreement provisions; Monitoring compliance with the security awareness and training requirements for each employee and contractor;

*Local Privacy Officers (PO)* are the agency officials assigned responsibility for managing the risks and business impacts of privacy laws and policies and they assist the ISO with the development and implementation of an information protection infrastructure for VA data. The VA POs assist by: Coordinating with COTRs and ISOs, as

appropriate, to ensure that all privacy breaches involving VA sensitive information are reported to the VA-National Security Operations Center (VA-NSOC) within one hour of receipt of breach notification from the contractor;

*Program or Project Managers and Information Systems Owners who are requesting or managing a contract or service* must determine whether contractors or third party servicers require information access (documents or electronic) in the accomplishment of the VA mission. Specifically, these individuals are responsible for:

- Identifying information security and privacy requirements during the requirements analysis based on a specific analysis of availability, integrity, and confidentiality and the technical requirements of the contract;
- Participating in the review and completion of Appendix A, *Checklist for Information Security in the Initiation Phase of Acquisitions*;
- Ensuring appropriate security language is included in applicable contracts so that the Statement of Work (SOW) accurately reflects the requirements of the contract;
- Ensuring appropriate background investigations are initiated and verified on all contractors under their supervision through the VA Security and Investigations Center (SIC);
- Ensuring that all hardware and software purchases conform to VA's requirements;
- Ensuring that all system development efforts comply with the best practices, technical standards, and product standards of VA;
- Determining the contractor's "need to know" before access is granted. Access to any VA information or information system must not be authorized for a person who does not have a need for access to the system in the normal performance of that individual's official duties;
- Ensuring that periodic reviews of the project are conducted to ascertain whether information security has been maintained at the appropriate level and compliance with the information security program continued after award. All instances of noncompliance must be reported to the CO or designated representative, for necessary action;
- Ensuring users (including contractors) under their supervision or oversight complete all security and privacy training requirements;
- Ensuring users (including contractors) under their supervision or oversight review and sign the appropriate Rules of Behavior on an annual basis;
- Notifying system managers and ISO to revoke access privileges immediately when a user under their supervision or oversight (including contractors) no longer requires access privileges or fails to comply with this policy;
- Authorizing remote access privileges for contractors, if required, and reviewing remote access user security agreements on a regular basis to verify the continuing need for access and the appropriate level of privileges; and
- Conducting closeout activities, including the return of all VA sensitive information and information resources provided to the contractor during the life of the contract at the expiration or completion of the contract. See VA Handbook 6500, Appendix D.

**COs and COTRs** are responsible for:

- Supporting the PM and ISO during the requirements analysis phase by conducting market research and providing procurement planning assistance as needed, including requirement specifics that address impact levels, security controls, and requirements in the acquisition, its plan, and its process;
- Participating in the review and completion of Appendix A, *Checklist for Information Security in the Initiation Phase of Acquisitions*;
- Reviewing incoming SOWs to ensure that information security has been addressed in the acquisition's requirements and deliverables and if not, coordinating with the requestor to ensure compliance with the VA Information Security Program;
- Ensuring that information security interests are represented and included as an evaluation factor during the evaluation period and as a performance measure during the life of the contract;
- Ensuring that the VAAR security clause and appropriate security language is included in contracts, if required;
- Ensuring that contractors sign the *Contractor Rules of Behavior* (Appendix D) on an annual basis;
- Maintaining the original or copy of the *Contractor Rules of Behavior* for the life of the contract;
- Ensuring contracts for services include appropriate background investigation requirements;
- Ensuring that the PDAT is used to appropriately designate in the Statement of Work or other written description of the assignment, the proper risk or sensitivity level for the contract employees;
- Ensuring that appropriate service providers and contractors who have negotiated agreements with VA, that involve VA sensitive information (but whose systems do not require C&A) complete an initial CSCA and one annually on the due date of their contract renewal;

- Ensuring that the CSCA is submitted to the ISO;
- Ensuring and documenting that contractors complete the required security and privacy awareness training initially and then annually thereafter;
- Ensuring that contractors know when and how to report security and privacy incidents;
- Monitoring the contract and the contractor to ensure that the contract's security and privacy requirements and responsibilities are being implemented; and
- In coordination with the facility PO, ensuring that contracts for services involving access to or disclosure of, protected health information have appropriate business associate agreements.

VA Information and Information System Security/Privacy Language:

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.

Access to VA Information and VA Information Systems

a. A contractor/subcontrator 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.

VA Information Custodial Language:

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and*

*Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.
d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.
k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.
l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

Security Incident Investigation:

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

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

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

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA

and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

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. However, it is the policy of VA to forgo collection of liquidated damages in the event the contractor provides payment of actual damages in an amount determined to be adequate by the agency.
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.

Training:

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;

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

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

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

b. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

Contractor Security Investigation Requirements: Contractor will not have access to any VA application or computer programs.

Contractor Security Requirements (Handbook 6500.6)

## 8. Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI).

All services will be provided at the VA Medical Center in a conference room setting.

## 9. Other Pertinent Information or Special Considerations.

### a. Identification of Possible Follow-on Work.

The contractor shall provide the reviews and quality checks necessary to ensure that the reporting, recording, transcripts and photocopying conform to acceptable government standards. No transcripts shall be forwarded to the government until the quality checks reveal full format conformance and freedom from error.

The Contractor shall closely monitor its performance in meeting the requirements for timely delivery of hearing transcripts. The Contractor shall advise the COR in advance, by **specific case number only** (no names, SSNs or any other personal identification data) when timely delivery cannot be made, and estimated time when correction of delivery will be made.

### b. Identification of Potential Conflicts of Interest (COI).

Conflict of Interest: The contractor shall not assign any person who is an employee of the United States Government to work under this contract if that employment would appear to cause a conflict of interest.

### c. Identification of Non-Disclosure Requirements.

The Contractor will be responsible for ensuring compliance by its employees with the security regulations of the Veteran's Administration where work is performed under this Contract. A Business Associate's Agreement (BAA) will be entered into by both parties. Contracted employees will have to complete VA's Cyber Security and Privacy Act Training annually, and sign the VA's Rules of Behavior document.

Note: All work associated with this contract shall be performed in the United States of America. Because this contract is funded with American appropriated tax dollars, all persons working under this contract shall be American Citizens. There shall be no exception to this requirement.

The information obtained in the performance of this contract is considered to be confidential and must not be revealed to anyone who is not authorized to know. Portions of information disclosed during the performance of this contract are protected by the provisions of the Privacy Act of 1974; therefore, all personnel assigned to this Contract are required to take proper precautions to protect the information from disclosure.

Commitment to Protect Sensitive Information. The Contractor and its employees shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with provisions of 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records) and any other pertinent laws and regulations governing the confidentiality of sensitive information.

d. Packaging, Packing and Shipping Instructions.

Contractor will ship the transcribed testimonies/copies to the VA Sierra Nevada Health Care System Human Resources Management Service by overnight delivery.

e. Inspection and Acceptance Criteria.

The AIB team leader, team, or other designated VA staff member will evaluate the quality and timeliness of the product and services and notify the COR and the Chief, Human Resources Management Service or other convening authority – i.e., EEO Manager, Human Resources Specialist (Employee/Labor Relations), or other so designated official of the acceptability of the product and services. However, only an appointed Contracting Officer Representative (COR) is authorized to monitor contract performance and only a Warranted CO is authorized to make changes to the contract by way of written contract modifications.

## 10. Risk Control

Addressed in paragraph 5.4.

## 11. Place of Performance.

VA Sierra Nevada Health Care System, 975 Kirman Avenue, Reno, Nevada.

## 12. Period of Performance.

The period of performance for Court Reporting services shall be for one base and four option years. Court reporting requirements shall occur intermittently through each fiscal year; the requirement may be an urgency of need with only one day in advance notice. However, the VAMC shall strive to inform the Contractor at least thirty (30) days in advance. It must be noted here that the Government does not automatically extend contracts beyond their initial period of performance period. Option periods are always subject to the availability of funds, Contractor's Performance, Continued Need and FAR Clause 52.217-9, Option to Extend the Term of the Contract.

## 13. Delivery Schedule.

The delivery schedule format is as follows:

| SOW Task# | Deliverable Title | Format | Number | Calendar Days After CO Start |
|---|---|---|---|---|
| 1 | Timely Delivery | Transcribed paper copies (no digital, e-mailed, etc.) of reports are delivered as stated in paragraph 9.d. | Standard Distribution* | Draft - 15<br>Final - 30 |
| 2 | Monthly Invoice (as needed) | Contractor-Determined Format | One in OB-10 | Monthly, on 5th Workday |

* Standard Distribution: 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be Emailed.