

**Performance Work Statement (PWS)
for
Annual Court Reporter Services for NFSGVHCS**

SECTION 1 GENERAL

1.1. 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.

1.2. PERIOD OF PERFORMANCE.

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.

1.3. BACKGROUND INFORMATION.

1.3.1. The government to establish a non-personal performance-based service contract for the VA Medical Center.

1.3.2. Invoices: Invoices received from the Contractor shall provide the unique Purchase Order Number that will be given for each requirement issued under this contract. 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.

1.3.3. The chart below represents best-known estimates for the total number of exams performed per year.

Procedure	Quantity per year
Administrative Investigations	13-15 per year
EEO Hearings	4-6 per year
MSPB Hearings	3-5 per year
Other	3-5 per year

NOTE: The estimated quantities are based on annual historic data based on prior year needs. Actual quantities may be more or less of these estimated amounts.

1.3.4. The terms “Administrative Investigation” (AI) and “Fact Finding” refer 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 any time up until the time scheduled because of unforeseen events that may arise.

1.3.5. 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.

1.3.6. 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.

1.4. PERSONNEL

1.4.1. 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).

1.4.2. The Contractor shall 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 shall 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 shall 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 shall 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.

1.4.3 OATHS AND NOTARY SERVICES - The Reporter shall be competent to administer oaths. Depositions shall be transcribed by a duly authorized notary. No separate fee is to be charged for notary services, administering oath, or affixing seal.

1.4.4. 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 shall be presented to the CO prior that person being assigned to this facility.
- Health examinations
- Income tax withholding, and
- Social security payments

1.4.5. 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 located in building 9. 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.

1.4.6. 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.

1.4.7. 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.

1.4.8. 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.

1.4.8.1. 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.

1.4.8.2. 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.

1.4.9. **Place of Performance:** Most services will be provided at the VA Medical Center in a conference room setting. Only on a rare occasion, will it be necessary for an investigation or hearing be held at another location as determined by the Government. Malcom Randall VAMC areas of responsibility spans the cities of Gainesville, Tallahassee, Jacksonville, Lake City, St. Augustine, Palatka and other cities within the vicinity of Gainesville, Florida. The location for services to be performed will be communicated by the Contract Officer's Representative. **All services shall be rendered with in-person appearance only. Media, electronic or telephonic services will not be accepted under this agreement.**

The Government reserves the right to add any additional CBOC's to the contract as they become available. During the life of this contract, there may be a need or an occasion that may arise that will require the services of the Court Reporter to be at another location other than these mentioned. If so, the COR will give explicit instructions as to where and when the needed services will be required.

PRIMARY DUTIES OF THE COURT REPORTER INCLUDE:

- Attend events that require transcripts
- Record spoken dialogue with specialized equipment, such as covered microphones
- Report gestures and actions
- Review notes for names of speakers and technical terminology
- Prepare transcripts for the record
- Edit transcripts for typographical errors
- Provide copies of transcripts and recordings to the court, counsels, and parties involved
- Court reporters create word-for-word transcripts of speeches, conversations, legal proceedings, meetings, and other events. They play a critical role in legal proceedings and other meetings where it is important to have a record of exactly what was said. They are responsible for producing a complete, accurate, and secure legal record.
- Court reporters often specialize in a specific method of recording, such as using stenotype machines, steno masks (covered microphones), or digital recording.

1.5 SECURITY REQUIREMENTS

1. 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:
 - i. 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;
 - ii. Successfully complete annual Information Security Awareness and Privacy and HIPAA Focused Training via Talent Management System (TMS) Self – Enrollment Instructions link:
<http://vaww.visn8.portal.va.gov/northflorida/cos/education/shared/MSE-Profile-Creation-Contractors-JobAid-508.pdf>. Required Classes:

- ✓ VA Privacy and Information Security Awareness Training and Rules of Behavior (VA10176)
 - ✓ Privacy and HIPAA Focused Training PowerPoint Presentation 2017 (VA10203)
- iii. 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 training and documents are complete.

1.5.1 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. Contracted employees will have to complete VA's Cyber Security and Privacy Act Training annually, and sign the VA's Rules of Behavior document.

1.5.2. The information obtained in the performance of this contract is considered to be confidential and shall 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.

1.5.3. 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.

1.5.4. In the performance of official duties, the Contractor's employees shall have access to information containing sensitive data, which shall be protected under the provisions of the Privacy Act of 1974 (5 USC 552a); the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"); Federal Regulations and statutes; and VAMC policies and standard operating procedures. The Contractor and Contractor's employees are responsible for:

- Protecting that data from unauthorized release or from loss, alteration, or unauthorized deletion.
- Completing annual privacy training that conforms to the requirements of VHA Privacy Training.
- Completing annual security awareness training that conforms to the requirement of the Department of Veterans Affairs Office of Cyber and Information Security Training.
- Within 24 hours of first becoming aware of a HIPAA Electronic Transaction and Code Set, Privacy, Security or Standard Identifier Incident, or use or Disclosure of PHI not provided for by this contract, notify the COR and CO, and promptly provide a report to the COR and CO.
- An incident will be considered any attempted or successful unauthorized access to, use, disclosure, modification, or destruction of, or interference with PHI, or an event that causes the VAMC to be considered non-compliance with the Administrative Simplification provisions of HIPAA as determined by the Department of Health and Human Services.
- Use only contractors or agents who are physically located within a jurisdiction subject to the laws of the United States. Ensure there is no use or disclosure of PHI received from the VAMC.
- Upon completion of the applicable contract(s), return all VA sensitive information gathered, created, received or processed during the performance of the contract(s), and no data will be retained by the Contractor, or any agents or subcontractors, unless retention is required by law or regulation or expressly permitted herein.
- All VA sensitive information will be stored in a locked area with access limited to those individuals directly involved in rendering the agreed upon services to the VA. Transport of VA sensitive information will be performed only by those individuals directly involved in rendering the agreed upon services to the VA. During transport, VA sensitive information will be housed in a locked container. Approved deliverables, such as transcripts, will qualify as an exception and may be transported via the postal service.
- All mobile devices used to generate, store, or collect VA sensitive information shall be encrypted. The contractor will verify device encryption by providing a certificate of encryption for all such mobile devices.
- Assure that all VA sensitive information has been returned to the COR.
- If immediate return of all data is not possible, assure that all VA sensitive information retained will be safeguarded to prevent unauthorized uses or disclosures. Until assurance is provided, the Department of Veterans Affairs may withhold 15% of the final payment of the contract(s).

1.5.5. Computer Security is a vital part of patient rights and privacy. All computer information from VAMC is considered sensitive and shall not be disclosed to anyone by the Contractor, or its employees. The Contractor and its employees shall follow all VAMC computer security guidelines. Violation of this Policy could result in the Federal prosecution of the individual(s) involved.

1.5.6. Confidentiality. All Contractor personnel performing services under this contract shall complete a confidentiality certification.

1.6. QUALITY CONTROL.

1.6.1. 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.

1.6.2. 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.

1.7. PERFORMANCE ASSESSMENT (QUALITY ASSURANCE SURVEILLANCE PLAN)

1.7.1 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	(AQL)
5.3	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
5.7	Timely Delivery	Transcribed paper copies (no digital, e-mailed, etc.) of reports are delivered as stated in paragraph 5.7.	Less than 1% of the reports are late
5.8 – 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 shall 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.

1.7.2. 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, Quality & Performance Improvement or other convening authority – i.e., EEO Manager, Human Resources Specialist, 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.

1.8. HOURS OF OPERATION.

1.8.1. Normal Business Hours. The VA Medical Center's normal business hours are 8:00AM to 4:30PM, Monday through Friday, excluding Federal Holidays. Services required by this contract will only be required during normal business hours.

1.8.2. Federal Holidays. The ten holidays observed by the Federal Government are: New Year's Day; Martin Luther King'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.

SECTION 2 STANDARD DEFINITIONS

Acceptable Quality Level (AQL). The AQL is the maximum percent defective that, for purposes of sampling inspections can be considered satisfactory.

Administrative Investigation (AI). A process of gathering evidence and ascertaining facts about particular matters, conducted primarily to enhance administrative effectiveness and efficiency.

Administrative Investigation Board (AIB). The standard procedures established under VA Directive 0700 and this Handbook for collecting and analyzing evidence, ascertaining facts, and documenting complete and accurate information regarding matters of interest to VA. "Members" are the person or persons appointed by a Convening Authority to conduct the AIB.

Contracting Officer (CO). A sole individual appointed with the authority to enter into and administer contracts on behalf of the U.S. Government.

Contracting Officer's Representative (COR). An individual designated by the CO to act as his representative to assist in administering a contract. The source and authority for a COR are contained in the written letter of designation from the CO.

Convening Authority. The authority responsible for convening and supervising administrative investigations under VA Directive 0700. Convening Authorities include the Heads of VA Administrations and Staff Offices, Chief executives of VA facilities, and authorities senior to any of them in the VA organization.

Defective Service. A service output that does not meet the standard of performance associated with it in the Performance Requirements Summary (PRS).

Federal Acquisition Regulations (FAR). The laws governing Government contracting procedures.

Investigative Report (IR). The standard format for conveying the results of an AIB, designed to enhance clarity and to facilitate review and decision-making. The essential components an investigative report are findings of fact, conclusions, and exhibits.

Performance Requirements Summary (PRS). Identifies the key service outputs of the contract that will be evaluated by the government to assure contract performance standards are met by the contractor.

Performance Work Statement (PWS). A statement that outlines the services needed for a Performance Based Service contract.

Quality Control. Those actions taken by a contractor to control the performance of services so that they meet the requirements of the PWS.

SECTION 3 GOVERNMENT FURNISHED PROPERTY AND SERVICES.

The government will provide to the contractor for contract performance at no cost a shared meeting location, utilities, and the use of a telephone (local calls only). Normally, the usage of cell phones within the Medical Center are permitted. However, there are some areas of the hospital where the usage of such devices are restricted because of their possible interference with operating medical equipment. Strict adherence to the rules concerning the usage of these devices shall be observed throughout the Medical Center.

SECTION 4 CONTRACTOR FURNISHED ITEMS AND SERVICES.

4.1. GENERAL. Except for those items or services specifically stated to be government furnished in Section 3, the contractor shall furnish everything required to perform this contract.

SECTION 5 SPECIFIC TASKS.

5.1. The contractor agrees that, at a minimum, all assigned court reporters shall:

- Prior to the scheduled meeting time:
 - Present himself/herself to the presiding COR in order to obtain a Temporary Identification badge from the appropriate VA Office. (Estimated time for this evolution is 30 minutes.) This badge will have to be returned by the Contracted Employee to the VA issuing office upon completion of the assignment.
 - After receipt of badge, proceed to the designated hearing location and have all equipment set up and ready by the scheduled hearing time.
- Adhere strictly to the instructions of the presiding official in matters affecting the composition of the record, adjourning to other times or places, the hours of hearing, and associated matters.
- Report everything spoken while a hearing is in session unless the presiding official directs an off-the-record proceeding for which notes have been taken as required.

5.2. Hearings shall be properly recorded by Court Reporters using electronic recording devices, in addition to their physical presence at the hearing. The Contractor shall provide a back-up system to whichever primary recording method is used. When proceedings are recorded by an electronic recording device, it shall at a minimum:

- have two (2) channels.
- be continuously monitored by an operator.
- have simultaneous playback, listening pre-amplification and speaker identification capabilities.
- have an equipment malfunction indicator.

The Court Reporter shall maintain an audio recording of the testimony, available to the team leader or COR for the process as needed to clarify issues associated with testimony content.

5.3. An experienced, competent Court Reporter shall be present in the room when witnesses are interviewed, testimony is given and/or when witnesses are called back for additional testimony. The team leader or other designated VA staff member will inform the Court Reporter of the anticipated duration of the process, and when the process has been completed.

5.4. 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.

5.5. When actual discrepancies in the transcribed testimony and the audio recording are identified and verified by the team leader or other designated point of contact, the Court Reporter shall produce a corrected version at no additional cost to the Government.

5.6. The contractor shall be fully responsible for all loss or damage to materials associated with this PWS while in the contractor's care and custody. The contractor shall keep accurate records of the materials picked up from the government. The listing shall include a list of materials, the status of the assignment and the case number assigned by the Government.

5.7. HEARING AND DELIVERABLES TIMELINES:

5.7.1. The Administrative Investigation Boards have an established timeframe for completion of 45 calendar days of the date the AIB is convened; whereby sworn or affirmed testimony is obtained by a team charged with investigating a particular issue or event. Transcribed testimony shall be returned to the Team Leader within 10 business days of each testimony in order for the deadline to be met. In the event that an extension of time should become necessary for completion beyond the initial 45 day period, the presiding official/Team Leader will notify the Court Reporter of this change.

5.7.2. EEO Hearings may have a short turnaround time for completion of 3 Days to 14 Days as established by a judge. Transcribed testimony shall be returned to the Team Leader within 3 business days of each testimony in order for the deadline to be met.

5.7.3. MSPB processes rarely exceed 3-5 days. Transcribed testimony shall be returned to the Team Leader within 3 business days of each testimony in order for the deadline to be met.

5.8. TRANSCRIPTION FORMAT:

5.8.1. 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.

5.8.2. The transcribed testimony product shall 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 shall 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.

5.8.3. 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.

5.8.4. Visible Black Character.

5.8.4.1. 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	-	=	[]	\	;	'	,	.	/	"				

5.8.4.2. 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.

5.8.5. All documents shall be 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.

5.8.6. 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.

5.8.7. 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.

5.8.8. 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.

5.8.9. 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

5.9. 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.

5.10. 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.

VA Information and Information System Security/Privacy Language

2. 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.

3. Access to VA Information and VA Information Systems:

- a. The provisions of the Contract do not include logical (technical) or physical access to VA information and VA information systems for Contract employees.
- b. The contract does not include any IT computer or remote connection to a VA internal trusted network. Therefore, C & A requirements do not apply and a Security Accreditation Package is not required.
- c. All contractors 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 shall 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.
- d. The contractor shall notify the Contracting Officer immediately when an employee with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer shall also be notified immediately by the contractor prior to an unfriendly termination.

4. VA Information Custodial Language:

- a. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor 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 shall be allowed to meet the requirements of the business need, the contractor shall 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 shall 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 shall 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 shall be sent to the VA Contracting Officer within 30 days of termination of the contract.

- d. The contractor shall 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 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 electronic storage media for restoration in case any electronic equipment or data used by the contractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies shall 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. The contractor firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
- h. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor 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 shall refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.
- i. Notwithstanding the provision above, the contractor 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 shall

immediately refer such court orders or other requests to the VA contracting officer for response.

- j. 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 shall complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

5. Information System Hosting, Operation, Maintenance, or Use

- a. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, shall 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) shall be submitted and approved prior to the collection of PII.
- b. This contract does not allow for outsourcing or subcontracting by the selected contractor.
- c. The contractor/subcontractor's system shall 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 shall be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor shall 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 shall be corrected within the timeframes approved by the government. Contractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor activities shall 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.
- d. The contractor shall conduct an annual self assessment on all systems and services as required. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor shall 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.
- e. VA prohibits the installation and use of personally-owned or contractor owned equipment or software on VA's network. If non-VA owned equipment shall be used to fulfill the requirements of a contract, it shall be stated in the service agreement, PWS or contract. All of the security controls required for government furnished equipment

(GFE) shall be utilized in approved other equipment (OE) and shall be funded by the owner of the equipment.

- f. 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 shall 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 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 shall be returned to the VA for sanitization or destruction or the contractor shall self-certify that the media has been disposed of per 6500.1 requirements. This shall be completed within 30 days of termination of the contract..

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 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 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 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 shall 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 shall 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 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 processes or maintains under this contract.

- b. The contractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA shall 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:
 - i. Nature of the event (loss, theft, unauthorized access);
 - ii. Description of the event, including:
 - 1. Date of occurrence;
 - 2. Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
 - iii. Number of individuals affected or potentially affected;
 - iv. Names of individuals or groups affected or potentially affected;
 - v. 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;
 - vi. Amount of time the data has been out of the VA control;
 - vii. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - viii. Known misuses of data containing sensitive personal information, if any;
 - ix. Assessment of the potential harm to the affected individuals;
 - x. Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
- d. Whether the 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.

- e. 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 the affected individuals consisting of the following:
 - i. Notification;
 - ii. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
 - iii. Data breach analysis;
 - iv. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
 - v. One year of identity theft insurance with \$ 20,000.00 coverage at \$ 0.00 deductible; and
 - vi. 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 the 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 shall fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information security systems are developed, operated, maintained, or used on behalf of the VA, including those initiated by the Office of the 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. Records Management Language for Contracts

The following standard items relate to records generated in executing the contract and should be included in a typical Electronic Information Systems (EIS) procurement contract:

- a. Citations to pertinent laws, codes and regulations such as 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.
- b. Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

- c. Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.
- d. Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.
- e. Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.
- f. The Government Agency owns the rights to all data/records produced as part of this contract.
- g. The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor shall deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.
- h. Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].
- i. No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.
- j. Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.