

Performance Work Statement
Neuromonitoring Equipment and Technician Services PWS

B.3.1. SCOPE OF WORK

B.3.1.1. The Contractor shall provide Neuromonitoring Equipment and Technician Services for surgical procedures at North Texas Veterans Health Care System (VANTHCS), 4500 South Lancaster Road, Dallas, Texas 75216 on an as needed basis. Services shall include intraoperative, preoperative, postoperative neurophysiologic monitoring services and evoked potential testing for neurosurgery patients. Services are to be conducted in the operating room and associated areas of the Dallas VA Medical Center on a **per case basis** as determined by the Chief of Surgical Service and Chief of Neurosurgery. The Chief of Neurosurgery shall notify the Administrative Officer or appropriate designee in Surgical Service when monitoring services are needed for a neurosurgical patient. The Administrative Officer or appropriate designee will contact the Contractor with the request for monitoring. All changes to the proposed monitoring, to include date/time, type of monitoring, etc., will be conveyed by the Administrative Office or appropriate designee to the Contractor.

B.3.1.2. The Contractor shall provide the equipment and services as described herein in a manner consistent with the standards of the Joint Commission for the Accreditation of Healthcare Organization (JC) requirements for this type of equipment and services.

B.3.2.HOURS/SCHEDULING OF SERVICE

B.3.2.1. Except by special alternative arrangement, scheduled services shall be rendered by the Contractor on a 24-hour bases. Upon contract award the contractor shall be available to provide Neurosurgery monitoring services as specified here in 24 / 7 365 days a year.

B.3.2.2. Federal Holidays. The ten (10) holidays observed by the Federal Government are as follows:

New Years Day	Labor Day
Martin Luther King's Birthday	Columbus Day
Presidents Day	Veterans Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

And any other day specifically declared by the President of the United States to be a National Holiday.

B.3.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR): VANTHCS shall appoint one (1) COR for this contract. When service is requested, the Contractor shall always contact the COR, Rebecca T. Quinn at 214-857-1836, or her designee.

B.3.4. CONTRACT REQUIREMENTS:

Upon arrival at the VA on each schedule day of service the Contractor shall report to the VA Human Resources (HR) Service to obtain a temporary VA Contractor badge.

B.3.4.1. EQUIPMENT SET UP/INSPECTION: Delivery activities shall consist of the following:

B.3.4.1.1. Upon arrival at the VA the Contractor shall take all equipment to BioMed Service for preoperative electrical safety check.

B.3.4.1.2. Equipment Set Up: All necessary preparation required to ready the **Neuromonitoring Equipment** for operation/service.

B.3.4.1.3. Maintenance: The Contractor shall maintain equipment in accordance with manufacture's specifications. The Contractor shall provide written documentation of Preventive Maintenance Services (PMS)/Maintenance has been performed as required for verification by the COR or his/her designee for all scheduled services. Documentation shall describe the maintenance and repair service performed on the equipment in sufficient detail so as to be acceptable by field inspectors of the Joint Commission and other inspecting bodies. This shall include a list of all parts replaced, all service performed as well as a statement that the equipment is operating per manufacturer's specifications after repair. The service report will be signed by the Contractor's service technician, and by designated VANTHCS personnel.

B.3.4.2. CONTRACTOR PROVIDED RESPONSIBILITIES:

B.3.4.2. CONTRACTOR PROVIDED RESPONSIBILITIES:

- Provides 24/7 onsite case coverage and scheduling 365 days/year with fully credentialed Neurophysiologists available for onsite coverage before and during surgery, (up to 3 if required).
- Neuromonitoring teams accredited by ABRET, (American Board of Registration of Electroencephalographic and Evoked Potential Technologist).
- Oversight of neuromonitoring done by board certified Neurologists.
- Certificate of Neurophysiologic intraoperative monitoring (CNIM) 80% of techs or more.
- Intraoperative monitoring modalities needed include: SSEPS, TcMEP, S-EMG, T-EMG, spinal cord mapping including D-Waves, DNEPs, NMEPs, Cortical, motor, sensory, language mapping, white matter tract and brainstem nuclei mapping, brainstem auditory evoked responses, visual evoked potentials, cranial nerve monitoring, and intraoperative EEG.
- Meets joint commission clinical quality standards for intraoperative monitoring.
- Establish communication protocols with the surgical team to report monitoring activity.
- Accurately apply all recording and stimulating electrodes.
- Perform monitoring procedures and documentation according to established protocols.
- Identify monitored waveforms and any variation from baseline.
- Have an understanding of anesthetic techniques and physiologic changes that can affect the waveforms being monitored.
- Be competent in the operating of monitoring equipment, including troubleshooting and electrical safety.
- Interpret the intraoperative monitoring recording and make recommendations regarding action or consequence to the attending Neurosurgeon.
- The Neuromonitoring team will provide all resources required to ensure a smooth transition in accordance with the contract requirements.
- FPIS compliant
- Quality reports required for quality assurance needs to be JHACO certified.
- Have a diplomat of American Board of Neuromonitoring on the team.
- Provides a list of all active surgeons receiving payments in consulting arrangements, advisors, and board members.
- Provides a list of all clients served in the past 12 months to permit VANTHCS to contact any reference of our choosing.

B.3.4.3. CONTRACTOR PERSONNEL/QUALIFICATIONS/EXPERIENCE CRITERIA

B.3.4.3.1. The Contractor's Technician(s) shall be certified to operate the required equipment.

B.3.4.3.2. The Contractor shall be required to maintain following documentation for each Technician working under the contract. The Offeror shall provide the following documentation with their offer.

B.3.4.3.2.1. Qualifications, Certifications, record of credentials and competencies

B.3.4.3.2.2. Applicable License(s), including number and expiration date

B.3.4.3.2.3. Documentation of education and training

B.3.4.4. RECORD KEEPING/CONTRACT MONITORING

B.3.4.4.1. VANTHCS shall establish and maintain a record keeping system that shall record the services performed by the Contractor.

B.3.4.4.2. The Contractor shall perform services under the direction of the VANTHCS, Chief, Surgical Service and Chief, Neurosurgery Service.

B.3.4.5. CONFIDENTIALITY OF PATIENT RECORDS

B.3.4.5.1. The Contractor, as a VA provider, will assist in the provision of health care to patients seeking such care from or through VA. As such, the Contractor is considered as being part of the Department health care activity. Contractor is considered to be a VA provider for purposes of the Privacy Act, Title 5 U.S.C. 552a. Further, for the purpose of VA records access and patient confidentiality, Contractor is considered to be a VA contractor for the following provisions: Title 38 U.S.C. 5701, 5705, and 7362. Therefore, Contractor may have access, as would other appropriate components of VA, to patient medical records, including patient treatment records pertaining to drug and alcohol abuse, HIV, and sickle cell anemia, to the extent necessary to perform its contractual responsibilities. However, like other components of the Department, and notwithstanding any other provisions of the contract, the Contractor is restricted from making disclosures of VA records, or information contained in such records, to which it may have access, except to the extent that explicit disclosure authority from VA has been received. The Contractor is subject to the same penalties and liabilities for unauthorized disclosures of such records as VA.

B.3.4.5.2. The records referred to above shall be and remain the property of VA and shall not be removed or transferred from VA except in accordance with U.S.C. 551a (Privacy Act), 38 U.S.C. 5701 (Confidentiality of Claimants Records), 5 U.S.C. 552 (FOIA), 38 U.S.C. 5705 (Confidentiality of Medical Quality Assurance Records) 38 U.S.C. 7332 (Confidentiality of Certain Medical Records), and federal laws, rules and regulations. Subject to applicable federal confidentiality or privacy laws, the Contractor, or their designated representatives, and designated representatives of Federal regulatory agencies having jurisdiction over Contractor, may have access to VA 's records, at VA's place of business on request during normal business hours, to inspect and review and make copies of such records.

B.3.4.6. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA):

Contractor must adhere to the provisions of Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the National Standards to Protect the Privacy and Security of Protected Health Information (PHI). As required by HIPAA, the Department of Health and Human Services (HHS) has promulgated rules governing the security and use and disclosure of protected health information

by covered entities, including the Department of Veterans Affairs (VA). In accordance with HIPAA, the Contractor may be required to enter into a Business Associate Agreement (BAA) with VA.

B.3.4.7. LIABILITY AND INSURANCE REQUIREMENTS:

B.3.4.7.1. The Contractor shall provide insurance coverage in accordance with Federal Acquisition Regulation (FAR) Clause 52.228-5, *Insurance – Work On a Government Installation (Jan 1997)*, VA Acquisition Regulation (VAAR) Clause 852.237-7, *Indemnification and Medical Liability Insurance (Jan 2008)*, and *Supplemental Insurance Requirements* incorporated herein under the Clauses Section.

B.3.4.7.2. Before commencing work under the contract, the Contractor shall furnish to the Contracting Officer a certificate of insurance indicating the coverage outlined herein and containing an endorsement to the effect that cancellation of, or any material change in the policies which adversely affect the interests of the Government in such insurance shall not be effective unless a 30-day advance written notice of cancellation or change is furnished the Government.

B.3.4.8. ID BADGES/PARKING/SMOKING POLICY:

B.3.4.8.1. BADGES. All Contractor personnel are required to wear Contractor issued identification (ID) badges during the entire time they are on the VA grounds. Upon arrival at the VA on each schedule day of service the contractor shall report the VA Human Resources (HR) Service to obtain a temporary VA Contractor badge.

B.3.4.8.2. PARKING. It is the responsibility of Contractor personnel to park only in designated parking areas. Parking information is available from the VA Security Service. The VA will not invalidate or make reimbursement for parking violations of the Contractor's personnel under any circumstances.

B.3.4.8.3. SMOKING. Smoking is not permitted within or around the VA Healthcare System facilities, except in designated areas.

B.3.4.9. RECORDS MANAGEMENT: All records (administrative and program specific) created during the period of the contract belong to VA North Texas Health Care System(VANTHCS) and must be returned to VANTHCS at the end of the contract or destroyed in accordance to the VHA Record Control Schedule (RCS)10-1. NARA RM Language Clause to be included in contracts:

B.3.4.9.1 Citations to pertinent laws, codes and regulations such as 44 U.S.C Chapter 21 , 29, 31and 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.3.4.9.2. 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.

B.3.4.9.3. 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.

B.3.4.9 4. 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.

B.3.4.9.5. Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract or identified in the RCS 10-1.

B.3.4.9.6. The Government Agency owns the rights to all data/records produced as part of this contract.

B.3.4.9.7. 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 must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

B.3.4.9.8. 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.].

B.3.4.9.9. 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.

B.3.4.9.10. 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.

B.4 IT CONTRACT SECURITY – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY

B.4.1. GENERAL: Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks.

B.4.2. CONTRACTOR PERSONNEL SECURITY REQUIREMENTS:

B.4.2.1. All Contractor employees having or requiring access to the Department of Veterans Affairs' computer systems or to sensitive data (to include patient or beneficiary records), shall be the subject of a background investigation and must receive a favorable adjudication from the VA Office of Security and Law Enforcement prior to contract performance. This requirement is applicable to all subcontractor personnel requiring the same access.

B.4.2.2. The Contracting Officer will provide the appropriate Background Investigation information to the Contractor for completion. Required background investigation initiation documentation must be completed and returned to the Contracting Office within five (5) calendar days after receipt.

B.4.2.3. Contractor staff shall not begin performance until notification is received from the Contracting Officer that the Security Package has been received and is considered a complete package. It is not necessary that the full Investigation be complete prior to commencement of work. However, if the investigation is not completed prior to the start date of the contract, the Contractor shall be responsible for the actions of those individuals they provide to perform work for VA.

B.4.2.3.1. Position Sensitivity - The position sensitivity has been designated as **Low Risk**.

B.4.2.3.2. Background Investigation - The level of background investigation commensurate with the level of access is **National Agency Check with Written Inquiries (NACI)**.

B.4.2.3.3. Contractor Responsibilities –

B.4.2.3.3.1. The Contractor shall bear the expense of obtaining background investigations. The VA Is responsible for payment to the Security Investigations Center; however, upon final payment, the VA will submit a Bill of Collections to the Contractor. The Contractor is responsible for reimbursement to the VA within 30 calendar days. The current cost for a low risk background investigation is \$231 per case.

B.4.2.3.3.2. Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

B.4.2.3.3.3. Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

B.4.2.3.4. Fingerprinting Requirements - Contractor/subcontractor employees will be required to have fingerprints taken as part of the background Investigation process. The preferred method of obtaining fingerprints is to have them taken electronically at the Human Resources Service at a VA facility. If fingerprints cannot be obtained at a VA facility the Contracting Officer will provide the Contractor with a Form FD258 fingerprint chart, which can be taken to any local police station for fingerprints. However, local entities may assess a fee for this service.

B.4.3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS:

B.4.3.1. A Contractor/subcontractor shall be granted 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.4.3.2. All Contractors/subcontractors 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.

B.4.3.3. 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.

B.4.4. VA INFORMATION CUSTODIAL LANGUAGE:

B.4.4.1. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information development 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.4.4.2. 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 or completion of the contract.

B.4.4.3. 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 into this contract.

B.4.4.4. The Contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement.

B.4.4.5. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provision 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.

B.4.4.6. 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.

B.4.4.7. 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.

B.4.5. SECURITY INCIDENT INVESTIGATION:

B.4.5.1. 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 procedure. 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.4.5.2. 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.

B.4.5.3. With respect to unsecured protected health information, the Contractor/subcontractor is deemed to have discovered a data breach when the Contractor/subcontractor knew or should have known of a breach

of such information. Upon discovery, the Contractor/ subcontractor must simultaneously notify the COTR, ISO and Privacy Officer.

B.4.5.4. 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 010 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 the 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.

B.4.6. LIQUIDATED DAMAGES FOR DATA BREACH

B.4.6.1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

B.4.6.2. 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.

B.4.6.3. Each risk analysis shall address all relevant information concerning the data breach, including the following:

B.4.6.3.1. Nature of the event (loss, theft, unauthorized access);

B.4.6.3.2 Description of the event, including:

B.4.6.3.2.1. date of occurrence;

B.4.6.3.2.2. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

B.4.6.3.2.3. Number of individuals affected or potentially affected;

B.4.6.3.2.4. Names of individuals or groups affected or potentially affected;

B.4.6.3.2.5. 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;

B.4.6.3.2.6. Amount of time the data has been out of VA control;

B.4.6.3.2.7. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

B.4.6.3.2.8. Known misuses of data containing sensitive personal information, if any;

B.4.6.3.2.9. Assessment of the potential harm to the affected individuals;

B.4.6.3.2.10. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

B.4.6.3.2.11. 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.

B.4.6.4. 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:

B.4.6.4.1. Notification;

B.4.6.4.2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

B.4.6.4.3. Data breach analysis;

B.4.6.4.4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

B.4.6.4.5. One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and

B.4.6.4.6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B.4.7. SECURITY CONTROLS COMPLIANCE TESTING: On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B.4.8. TRAINING:

B.4.8.1. 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:

B.4.8.1.1. Sign and acknowledge (either manually or electronically) understanding of and responsibility for compliance with the Contractor Rules of Behavior, attached, relating to access to VA information and information systems.

B.4.8.1.2. Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training;

B.4.8.1.3. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

B.4.8.1.4. 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.4.8.2. The Contractor shall provide 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 one week of the initiation of the contract and annually thereafter, as required.

B.4.8.3. 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 documents are completed.

B.4.9 Quality Assurance

See Attached Quality Assurance Plan