Statement of Work

VISN 17

VA South Texas Health Care System

Draeger Medical Innovian Anesthesia Clinical Work Stations

Table of Contents

1.0 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations ("FAR"), shall govern this Order. Commercial license agreements may be made a part of this Contract but only if both parties expressly make them an addendum. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Order; this includes, but is not limited to, any agreement embedded in the computer software or any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation, or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (e.g., restricted computer software) are included and made a part of this Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Order.; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Order. Federal law and regulation, including without limitation, the Contract Disputes Act (41 U.S.C. §601-613), the Anti-Deficiency Act (31 U.S.C. §1341 et seq.), the Competition in Contracting Act (41 U.S.C. §2304), the Prompt Payment Act (31 U.S.C. §3901, et seq.) and FAR clauses 52.212-4, 52.227-14, 52.227-19 shall supersede, control and render ineffective any inconsistent, conflicting or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 28 U.S.C. § 516. At the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Order must be made by order modification (Standard Form 30). Nothing in this Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

2.0 BACKGROUND

The Department of Veterans Affairs (VA) Veterans Health Administration (VHA) provides health care benefits and services to Veterans of the United States. VHA provides high quality, effective, and efficient Anesthesia Record Keeper Systems (ARK) to those responsible for providing care to the Veterans throughout all the points of surgical and anesthesia health care in a timely and compassionate manner. VHA depends on ARK to meet mission goals.

In 2009, VHA Heart of Texas Veteran Integrated Service Network 17 (VISN 17) embarked on implementation of a VISN-wide Draeger Medical Innovian Anesthesia Record Keeper System initiative. VISN-wide installation of Innovian servers and software was completed in 2012 and is currently operational at the Dallas, Temple and

San Antonio VA Medical Centers (VAMCs) In 2012 a follow on contract for maintenance and support was awarded to Draeger Medical.

The software applications that make up Innovian Anesthesia provide data collection, access and reporting, building of specific environments, auto-triggers, database query, real-time access to information in the PreOp, IntraOp, Post Op and moderate sedation areas, remote and single sign-on access, inbound and outbound Health Level Seven (HL7) interfaces to VistA, inbound data from medical devices, record upload to VistA Imaging and data extracts. Innovian Anesthesia replaced paper records used in the VISN 17 Anesthesia care areas. Certified Nurse Anesthetists, Anesthesiologists and other clinical staff use the Innovian Anesthesia System to manage the surgical/anesthesia patient information. Innovian Anesthesia provides a real-time bi-directional interface with the Veterans Health Information Systems and Technology Architecture (VistA), and allows the creation and storage of a completed Portable Document Format (PDF) file that is accessible in VistA Imaging via the Computerized Patient Record System (CPRS).

Innovian Anesthesia is a distributed solution required by the VA South Texas Health Care System (STVHCS) Anesthesiology and Pain Management Service that provides comprehensive data management for the anesthesiologist. The Innovian® Anesthesia information management system works to create a complete, continuous, and paperless record of patient's anesthetic care. This system compliments existing capabilities at the STVHCS.

3.0 APPLICABLE DOCUMENTS

The following documents are required in the performance of the tasks associated with this Performance Work Statement (PWS):

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
4. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003

10. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
11. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. Health Technology Management (HTM) Service Bulletin SB2012-004; Removable Media Scanning; November 2012
16. Health Information Technology and Health Data Standards http://www.nlm.nih.gov/healthit.html
17. Healthcare Information Technology Standards Panel http://www.hitsp.org/
18. VA Directive 6500, “Information Security Program,” August 4, 2006
19. VA Handbook 6500, “Information Security Program,” September 18, 2007
20. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”
21. VA Handbook 6500.6, “Contract Security,” March 12, 2010
22. National Institute Standards and Technology (NIST) Special Publications
23. VA Directive 6550, “Pre-Procurement Assessment for Medical Devices,”
24. VA Handbook 1907.01 Health Information Management Systems (HIMS)
25. Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)
26. Personally Identifiable Information (PII) (VHA Directive 1080)
27. VA Maintenance/Installation (Warranty) Contracts; VAIQ 7058822; March 24, 2011
28. VHA Handbook 1600.01, *Business Associate Agreements*
29. VA Directive 6300, *Records and Information Management*
30. VA Handbook 6300.1, *Records Management Procedures*
31. VA Handbook 6500.1, *Electronic Media Sanitization*
32. Contractor Access Policy Guidance Bulletin, January 30, 2012, VA OIT Field Security Service (FSS) No. 26

Statement of Work

1. OVERVIEW

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA), VA Heart of Texas VA Integrated Services Network (VISN 17) VA SouthTexas Health Care System (STVHCS) is procuring Draeger Medical Innovian Anesthesia Clinical Workstations, accessories (cabling, keyboards, mice, stands, etc), operating system

software and installation/integration services. The products and services will be delivered at the STVHCS Audie L. Murphy VA Medical Center. This acquisition is required in order to meet essential anesthesia record keeping expansion requirements of the existing Draeger Innovian Anesthesia Record Keeper (ARK) and characteristics defined herein. The equipment will be used by VA personnel (doctors, medical technologists, and nurses and shall be maintained by Biomedical Engineering, Office of Information Technology (OIT) support staff and the Contractor. Equipment connectivity will be inside the VA firewall via LAN and WAN network.

2. GENERAL REQUIREMENTS

The scope of the VISN 17 San Antonio ARK Work Stations includes delivery of equipment, services and warranty defined herein.

The Contractor shall provide all labor, travel, tools, materials, project management, shipping and delivery, hardware, software, installation, integration, documentation, acceptance testing and warranties required for the ARK workstations functionality with the existing ARK including three (3) each Draeger Medical clinical work station hardware (computer, monitor, mouse, keyboard, cabling).
Delivery of equipment shall be to the Audie L. Murphy VA Medical Center. After delivery, the Contractor shall be responsible for unpacking, assembly, delivery to specific areas within the Medical Center's Anesthesiology Service, installation, configuration and testing in accordance with the STVHCS policy and standard operating procedures. The Contractor must perform all Innovian Anesthesia database configurations such as adding each workstation to Innovian, completing entries, changes and licensing each new workstation to the Innovian Anesthesia database.

The solution must be fully compatible with the existing Innovian Anesthesia system used at Audie L. Murphy Medical Center meaning that the workstation hardware and software configurations shall be the same manufacturer as the existing Innovian products. Applicable software shall be Windows 7 and the exact same application and version currently in use (Innovian Anesthesia 4.2).

The Contractor shall provide VISN 17 a description and complete set of work station and monitor specifications for the Contractor's proposed ARK work station solution.

All equipment and components proposed by the Contractor shall provide VISN 17 with full functionality and compatibility with existing Draeger Medical Innovian Anesthesia software.

The Contractor shall have current 510k clearance to market its products and an adequate quality assurance system, such as ISO 9001.

3. PERFORMANCE PERIOD

The period of performance shall be March 1, 2016 through September 30, 2016, with no option periods.

The Contractor shall provide support 24 hours per day, 7 days per week. Normal hours of work are defined as Monday through Friday from 7:00 a.m. to 5:30 p.m. Central Time, excluding Federal holidays or as otherwise arranged with the Contracting Officer's Representative (COR).

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

Under current definitions, four are set by date:

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

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

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

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

4. PLACE OF PERFORMANCE

Tasks under this contract shall be performed at VISN 17 South Texas Veterans Health Care System, Audie L. Murphy Medical Center. Remote support may be performed remotely at Contractor facilities. Work may be performed at remote locations other than Contractor facilities with prior approval of the COR. On-site support shall be performed at the VA Medical Center located in the following location:

> South Texas Veterans Health Care System: Audie L. Murphy VA Medical Center, 7400 Merton Minter Blvd., San Antonio, Texas 78229. Phone: 210-617-5300, ext 17109

5. TRAVEL

All Contractor transportation, lodging, and subsistence expenses incurred by the Contractor shall be incorporated into the Contractor's fees and are the sole responsibility of the Contractor. Travel will be scheduled at the most cost effective rate and fare, and by the most cost effective mode of travel in accordance with the General Services Administration.

6. SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

6.1. KICKOFF MEETING

The Contractor shall attend a Project Kickoff Meeting where the project shall be discussed in detail. The meeting will be conducted by conference call and coordinated by the COR within seven (7) days after the contract award.

6.2 DELIVERY, INSTALLATION and INTEGRATION

Equipment shall be delivered to each HCS as listed in the Deliver Equipment to Location section 13.

Upon delivery of the equipment, the Contractor shall provide on-site project management, set-up and assembly, installation and integration of new equipment and software to the existing ARK based on STVHCS policy and procedures.

During the installation, the Contractor shall provide on-site as well as remote support, as needed, and must be available to respond to any questions asked by the Facility POCs. The Contractor shall provide same day resolution of any issues related to the new equipment. The Contractor is responsible for providing STVHCS staff with configuration instructions and guidance for all equipment and accessories procured under this contract.

At a minimum, the Contractor shall provide on-site and remote technical support staff on duty from 6 AM Central Standard Time to 6 PM Central Standard Time, Monday through Friday, excluding federal holidays. The Contractor shall provide a daily Status Report via e-mail for any issue that requires action. The report will describe the time the issue was identified, problem summary, steps taken to resolve the problem, time to complete the task and system or component down-time.

6.3 ACCEPTANCE TESTING

The Contractor is responsible for coordinating and performing technical testing. Equipment will be put into clinical use during implementation. Implementation must be

100% (all equipment operational with 100% functionality before being considered as complete and accepted by the Government.

If deficiencies found at the time of Government acceptance are corrected within 30 calendar days after receipt of the deficiency letter from the Contracting Officer, final acceptance will be issued upon validation of deficiency correction by the Government, and the warranty start date shall be back-dated to the date the initial acceptance testing was completed.

Clinical testing will be performed by the Government.

6.4 INTERFACE SUPPORT

The Contractor shall ensure that all Innovian Anesthesia side interfaces associated with the new workstations, including but not limited to, VistA, VistA Imaging/CPRS, Medical Devices, Innovian Reporting Tool, and data transfer links are configured, testing and maintained consistently. The Contractor shall coordinate with other Contractors when necessary to accomplish this task.

7. WARRANTY

Warranty shall start at acceptance. During the 12 month warranty period, the Contractor shall furnish warranty maintenance service support that includes, as a minimum, preventive and corrective maintenance services for the equipment. and all associated hardware, firmware and software, parts, labor, travel and expenses necessary to perform such services at no additional cost to the Government. Parts cost incurred during maintenance calls shall be included in the base warranty/maintenance price and shall not be billed as additional costs. In those emergency situations when a system component(s) is down and the Government places the call for corrective action to the Contractor, the Contractor shall respond within the prescribed response time The Government representative will make formal notification of the problem by phone to the Contractor POC as soon as the problem is identified by the Government.

Warranty Maintenance & Support Help Desk: The Contractor shall provide be provided with remote (connectivity to VA network) access for maintenance and support. The Contractor shall provide contact information to the Contractor’s Support Help Desk. The Government will call and/or email the Contractor to report problems and to coordinate technical support. Maintenance under the warranty periods shall include access to new versions, updates, patches, upgrades and to the equipment components as they are released as well as scheduled maintenance (preventive maintenance inspections,

electrical safety testing, calibration, scheduled releases) and unscheduled corrective maintenance. The Contractor Help Desk shall permit STVHCS staff to report problems, ask questions, request services, query historical data and request reports. The Help Desk shall provide real time information to include current status, total equipment down time, who initiated the service ticket, the original complaint, response time, the service technician, work performed, replacement parts and completion date and time.

Warranty Maintenance & Support Hours of Coverage: Contractor support staff will work with the User's schedule to ensure efficient operation. Contractor support staff are stationed at home offices. The Contractor shall provide a Help Desk telephone line with live-support which shall be available 27X7X365. The Contractor shall provide an Online Help Email address which received messages 24X7X365. The Contractor shall provide an Online Help Desk Website Access which shall be available 24X7X365.

Warranty Maintenance and Support Response Time: The Contractor shall responds to maintenance and support requests made by the STVHCS by telephone or email within 1 hour from the time the request was made. Response time shall commence at the time the Government POC places the maintenance and support call to the Contractor maintenance and support POC and shall end at the time the Contractor maintenance and support provider contacts the Government by email or telephone. The Contractor is required to provide a reliable maintenance and support POC for 24 hour service call notification. The Contractor maintenance and support POC shall provide a telephonic response of acknowledgment of receipt of an emergency call within 1 hour following notification. Failure of the maintenance and support POC to answer valid attempts made by the Government within the response time will result in the start of both downtime and response time.

Warranty Hardware Upgrades: If hardware upgrades become available after award of a delivery order but prior to delivery of the equipment, the Contractor is requested to offer them to the Contracting Officer for consideration. The Contractor's proposal for such upgrades shall include the following information: Pricing information, to include both the price of the equipment to be added and the equipment to be deleted. Specific awarded items that shall be changed if the proposal is awarded. Performance data, including both comparisons to the specification requirements and to the equipment on contract. A detailed description of the differences between the awarded items and those being proposed, and a specific analysis of the comparative advantages/disadvantages of the items involved. An evaluation of the effect proposed changes will have on the life cycle of the equipment and an associated cost impact as it relates to site preparation, installation, maintenance, and operational expense. An analysis of the timeframe required to institute the change.

Warranty Replacement Components and Parts: The Contractor shall make available to the Government all components and spare parts required to maintain the equipment herein. The Contractor shall furnish all parts at no additional cost. All parts supplied shall be the original equipment manufacturer or equivalent and fully compatible with existing equipment. The Contractor shall provide new parts. Replacement components and parts (hardware, firmware, software, and any work station discrete components) shall receive a full 12 month warranty from the time of replacement. The Contractor shall deliver components and parts by next business day from the date/time requested by the Government. The Contractor shall provide a guarantee that the Government will be able to obtain all required spare parts from the Contractor for a period of seven (7) years from the date of final system acceptance. During the equipment life cycle, if the Government elects not to upgrade existing systems to new versions (either hardware, software, and spare components and parts), the Contractor shall guarantee that they will continue to provide support all hardware, software, and spare components and parts for the equipment for a minimum of seven (7) years, after release of the upgrade.

Warranty Maintenance and Support Reports: The Contractor shall maintain historical warranty service records on each component of the system, which will be provided to the Government upon request and made available in electronic format. Warranty Service reports of all services performed shall be verified by the STVHCS POC, maintained and turned over to the STVHCS POC and filed with the equipment history file. The Contractor shall also provide service reports to the Contracting Officer and COR upon request. As a minimum, the report shall include: (a) date and time notified, (b) date and time of actions taken, (c) description of malfunction or service to be performed, (d) model number/serial number and location of the equipment, (e) time spent to resolve, (f) parts used/replaced, and (g) parts cost if applicable, (h) description of service performed, (i) name of government POC, (j) name of Contractor maintenance and support staff, (k) telemaintenance methods used, if any, (l) designation of user error, if appropriate. Documentation such as Service Bulletins, Product Modifications, Removals, Recalls, and End of Support Notifications shall be sent to the CO, COR and HCS POCs.

8. DOCUMENTATION

Documentation and reports will be provided to STVHCS by the Contractor in accordance with facility policies and procedures. Documentation includes equipment, components and parts specification data sheets, user and technical manuals, schematics and diagrams, written preventive maintenance and calibration procedures, software license agreements, training documentation, service bulletins, product

modification, removal, recall or end of support notifications and maintenance and support reports.

Non-compliance with the documentation requirements specified herein may result in actions as deemed appropriate by the Contracting Officer.
Specification Data Sheets, User and Technical Manuals, Schematics and Diagrams, Preventive Maintenance and Calibration Procedures, Software License Agreements, and Training Documentation (software and hardware).

The Contractor shall certify that manufacturer manuals provided with the equipment and the system's software accurately reflect the configuration of the delivered equipment and system's software or the operation and maintenance thereof. The Contractor shall furnish their commercial system administration's manuals, operator's manuals, and maintenance manuals for the supplied equipment.

Copies of document corrections and revisions shall be supplied by the Contractor for the life of the equipment and software. The Contractor shall furnish unlimited e-copies in PDF format to the STVHCS. All software and supporting literature is to be updated as required software upgrades are fielded.

9. MANDATORY CHECK IN/OUT AND REMOVABLE MEDIA SCANNING

For any services performed on-site the Contractor shall, upon arrival at the VAMC, report to the Facility POC to check in before proceeding to the any department and before performing any services. Prior to leaving the medical center, the Contractor shall check out with the POC. This check in and check out is mandatory. Upon check in with the Facility POC and before performing any services, the Contractor shall ensure that any removable media is scanned by the Biomedical Engineering Section prior to connecting to any VAMC network, device or system. The Contractor shall provide any removable media to Biomedical Engineering staff. Biomedical Engineering staff will perform a malware/virus scan of the Contractor's removable media. If "nothing found" is displayed, the Contractor may proceed and use the removable media. If "nothing found" is not displayed and/or the number of detections is greater than zero (0), the removable media shall be presumed infected with malware and shall not be allowed to be used. The media shall be returned to the Contractor for virus removal. The Government will not perform any virus or malware removal on the Contractor's removable media. Biomedical Engineering will report any detection to the Facility Information Security Officer (ISO). Failure by the Contractor to check in, check out, provide removable media for scanning, or use of any infected media is a breach of security and shall be acted upon in accordance with the terms and conditions of this contract.

10. PHYSICAL SECURITY & SAFETY REQUIREMENTS

The Contractor personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

10.1 The Contractor personnel shall wear visible identification at all times while they are on the premises.

10.2. VA does not provide parking space at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.

10.3 Smoking is prohibited inside/outside any building other than the designated smoking areas.

10.4 Possession of weapons is prohibited.

10.5 The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

11. FACILITY/RESOURCE PROVISIONS

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

12. SCHEDULE FOR DELIVERABLES

TASK	DELIVERABLE ID	DELIVERABLE DESCRIPTION
1	6.1	KICKOFF MEETING
2	6.2	DELIVERY, INSTALLATION AND INTEGRATION
3	6.3	ACCEPTANCE TESTING
4	6.4	INTERFACE SUPPORT
5	7.0	WARRANTY
6	8.0	DOCUMENTATION

13. SPECIAL SHIPPING INSTRUCTIONS

Prior to shipping and parts or supplies, the Contractor shall notify Site POCs, by phone and by email, of all incoming deliveries including line-by-line details for review of requirements. The Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of hardware or other material to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, will bear the VA Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA PO number shall indicate total number of containers for the complete shipment (i.e. "Package 1 of 2"), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

PO #: _____

Total number of Containers: Package ___ of ___. (i.e., Package 1 of 3)

DELIVER EQUIPMENT TO LOCATION:

Audie L. Murphy VA Medical Center
7400 Merton Minter Blvd.
San Antonio, TX 78229
Attention: Mr. Manuel Posada
Purchase Order Number: _____

14. POINTS OF CONTACT

Contracting Officer's Representative:
Name: Manuel Posada
Address: 7400 Merton Minter Blvd
Voice: 210-617-5300, ext 17109
Email: manuel.posada@va.gov

15.0 VA FURNISHED PROPERTY AND VA FURNISHED INFORMATION

There will be no government furnished property.

16.0 SECURITY REQUIREMENTS

This Draeger Medical Innovian Anesthesia Workstations contract involves the Contractor's access, use of VA secure networks and equipment and exposure to VA sensitive personal information while implementing contract services defined herein. This contract does not intentionally involve the use or disclosure of sensitive information as the object of this contract. Any access to sensitive information by the Contractor personnel in completion of their services is considered incidental. Access and exposure to VA sensitive personal information occurs as a bi-product of Contractor personnel duties and is not be reasonably prevented. As such, in accordance with Department of Veterans Affairs Memorandum, "VA Maintenance/Installation (Warranty) Contracts (VAIQ 7058822), dated March 24, 2011, such disclosures are incidental and permitted by the HIPAA Privacy Rule (see 45 CFR 164.502 (a)(1). Furthermore, this contract includes the following five requirements per 38 U.S.C.§§ 5723 and 5725:

Each documented initiative under this contract incorporates the VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix A, is included in this document as Attachment B.

a. Prohibition on unauthorized disclosure: "Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contracting in performance or administration of this 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. See Handbook 6500.6, Appendix C, paragraph 3.a.

b. Data breach notification: Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including the contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the Designated ISO and Privacy Officer for the contract. The term "security incident" means an event that has or could have resulted in the unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. See VA Handbook 6500.6, Appendix C, paragraph 6.a.

c. Requirement for pay liquidated damages in the event of a data breach: In the event of a data breach or privacy incident involving sensitive personal information the contractor processes or maintains under this contract, the contractor shall be liable to VA for liquidated damages for a specified amount

per affected individual to cover the cost of providing credit protection services to those individuals. See VA Handbook 6500.6, Appendix C, paragraph 7.a, 7.d.

d. Requirement for annual security/privacy awareness training: Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall complete on an annual basis either: (i) the VA security/privacy awareness training (contains VA's security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA's security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the contractor. If the contractor provides their own training that conforms to VA's requirements, the Contractor shall provide the COR or CO, a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in VA's contract have received their annual security/privacy training that meets VA's requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9.

e. Requirement to sign VA's Rules of Behavior: Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall sign on an annual basis an acknowledgement that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior which is attached to this contract or by completing the VA Talent Management System (TMS) "VA Privacy and Information Security Awareness and Rules of Behavior" course. See VA Handbook 6500.6, Appendix C, paragraph 9, Appendix D. Note: If a medical device vendor anticipates that the service under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the vendor's designated representative. The contract must reflect by signing the Rules of Behavior on behalf of the vendor that the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing the VA's information and information systems

16.1 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

The contractor/subcontractor shall request logical (technical) and/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.

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.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

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

16.2 GENERAL:

The Contractor, contractor personnel, subcontractors, and subcontractor personnel shall follow, and 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, handling of privacy information and shall be subject to penalties associated with the release of such data.

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

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and this PWS, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall.

Any security violations or attempted violations shall be reported to the VA Program Manager, COR and VA Information Security Officer as soon as possible.

The Contractor shall not transmit, store or otherwise maintain sensitive data or products in the Contractor systems (or media) within, or outside, the VA firewall in accordance with VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times.

16.3 NATIONAL CONTRACTOR ACCESS PROGRAM, INTERCONNECTION SECURITY AGREEMENT /MEMORANDUM OF UNDERSTANDING AND REMOTE ACCESS

The Draeger Medical Innovian Anesthesia Upgrades, Maintenance and Technical Support contract involves Contractor remote access to VA VISN 17 networks in accordance with the VA OIT National Contractor Access Program (NCAP). Inter-connection between the Contractor and VA shall be via an approved Site to Site Virtual Private Network (VPN) under an Interconnection Security Agreement/ Memorandum of Understanding/ (ISA/MOU) approved for the Site to Site VPN. VA will provide access to VISN 17 Draeger Medical Innovian Anesthesia systems as required for execution of the tasks via the remote access site to site VPN technology which will provide Contractor access to VAMC's Innovian Anesthesia specific hardware and software enabling the Contractor to perform the required Upgrades, Maintenance and Technical Support.

The Draeger Medical Innovian Anesthesia/VA utilizes a Memorandum of Understanding (MOU) to document the terms and conditions for sharing data and information resources in a secure manner. The supporting information within the MOU will define the purpose of the interconnection, identify relative authorities, specify the responsibilities of both organizations, and define the terms of the agreement. Additionally, the MOU provides details pertaining to apportionment of cost and timeline for terminating or reauthorizing the interconnection.

Technical details on how the interconnection is established or maintained are included within the Interconnection Security Agreement (ISA). A system interconnection is a direct connection between two or more information technology (IT) systems for the purpose of sharing data and other information resources. The Draeger Medical Innovian Anesthesia/VA uses the ISA to formally document the reasons, methodology, and approvals for interconnecting IT systems; to identify the basic components of an interconnection; to identify methods and levels of interconnectivity; and to discuss potential security risks associated with the interconnections.

The ISA specifies the technical and security requirements of the interconnection and the MOU defines the responsibilities of the participating organizations.

The purpose of the ISA/MOU is to establish a management agreement between the Contractor and VISN 17 regarding the development, management, operation, and security of a connection between Draeger Medical Innovian Anesthesia and VA. The agreement governs the relationship between Draeger Medical and VA including

designated managerial and technical staff, in the absence of a common management authority.

16.4 VA DIRECTIVE 6550 PRE-PROCUREMENT ASSESSMENT

The Contractor shall complete the VA Directive 6550 Pre-Procurement Assessment and Manufacturer's Disclosure Statement worksheet as necessary for networked Innovian Anesthesia devices. These must be completed to assure that Innovian Anesthesia devices are integrated effectively and securely. A sample manufacture disclosure statement, pre-procurement assessment and pre-implementation items are included in Attachment X of this PWS.

16.5 BUSINESS ASSOCIATE AGREEMENT

The contractor shall have a Business Associate Agreement (BAA) and safeguard Personal Health Information (PHI) agreements.

Business Associate Agreements (BAA) are mandated by the Health Insurance Portability & Accountability Act (HIPAA) and defined at 45 CFR 160.103 and amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).

16.6 VA INFORMATION CUSTODIAL LANGUAGE

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).

VA information should not be co-mingled 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.

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.

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.

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.

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.

If a VHA contract is terminated for cause, the associated BAA and ISA/MOU 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.

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.

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.

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.

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.

16.7 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

The contractor/subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows 7 and Vista (in Protected Mode on Vista) and future versions, as required.

The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration.

Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C.

552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

The contractor/subcontractor agrees to comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.

> (1) “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.
>
> (2) “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
>
> (3) “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of

the system). Such issues shall be remediated as quickly as is practical, but in no event longer than five (5) days.

When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within three (3) days.

All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology.

16.8 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

The contractor/subcontractor must document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the system may need to be reviewed, retested and re-authorized. This may require reviewing and updating all of the documentation (6550, Contingency Plan, Disaster Recovery Plan, etc.).

VA prohibits the installation and use of personally-owned or contractor/subcontractor owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, the equipment must be transferred to ownership of the VA during it's use.. All of the security controls required for government furnished equipment (GFE) must be funded by the original owner before it is transferred to VA ownership and will be maintained as a component of the System. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Original owners of equipment that is transferred to VA ownership are responsible for providing and maintaining the anti-viral software and the firewall of the transferred equipment..

All Draeger Medical Innovian Anesthesia systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end

of use, lease, for trade-in, or other purposes. Storage media shall be retained by the VA and shall not be returned to the Contractor.

16.9 SECURITY INCIDENT INVESTIGATION

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

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.

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.

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.

16.10 LIQUIDATED DAMAGES FOR DATA BREACH

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.

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.

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.

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.

16.11 SECURITY CONTROLS COMPLIANCE TESTING

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

16.12 PROHIBITION OF CONTRACT PERFORMANCE OUTSIDE THE U.S.

The entire performance of the contract shall be within the borders of the United States of America, the District of Columbia and/or Puerto Rico. The Contractor shall not access any VA data/information (for example, by remote computer access) from locations that are outside the above-stated borders. Furthermore, the Contractor shall not send, transfer, mail or otherwise transmit any VA data/information to locations outside the above-stated borders.

16.13 CONTRACTOR RULES OF BEHAVIOR AND SECURITY TRAINING

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:
The Contractor shall complete all mandatory training courses identified on the current external VA training site, The VA Talent Management System (TMS) web site at https://www.tms.va.gov/learning/user/login.jsp. The site is intended for employees and Contractors of the Department of Veterans Affairs. The Contractor will use the VA training provided in TMS. The contractor personal shall self-enroll into TMS at https://www.tms.va.gov/learning/user/SelfRegistrationUserSelection.do. For assistance with the TMS, the Contractor personnel shall contract the VA TMS Help Desk at vatmshelp@va.gov or at 1 (866) 496-0463.

For the initial training, the contractor shall provide 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.

Failure to complete the mandatory annual training and/or failure to sign the Contractor 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.

16.14. RULES OF BEHAVIOR

Rules of Behavior for Automated Information Systems: Contractor personnel having access to VA Information Systems are required to read and sign a Contractor Rules of Behavior statement which outlines rules of behavior related to VA Automated Information Systems. The COR will provide, through the facility ISO, the Rules of Behavior to the Contractor for the respective facility. The Contractor shall sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior.

NOTE: Rules of Behavior are also included as part of VA TMS 10176 “VA Privacy and Information Security Awareness and Rules of Behavior”. If the Contractor completes this course, the Contactors are NOT required to manually or electronically sign a separate Rules of Behavior.

16.14.1 ELEVATED PRIVILEGES (EP) RULES OF BEHAVIOR

The Contractor’s representative shall also ensure and certify that Contract employees who require system administrator level access (elevated privileges) to VA information

systems under this contract have also completed the Elevated Privileges Rule of Behavior. This must be completed at least once and is not required annually unless directed by the VA system owner through the COR or CO.

16.15. SECURITY TRAINING COURSES

16.15.1 VA PRIVACY AND INFORMATION SECURITY AWARENESS AND RULES OF BEHAVIOR TRAINING COURSE

The Contractor personnel must complete the *VA TMS 10176 VA Privacy and Information Security Awareness and Rules of Behavior Training* initially and annually thereafter: Each contractor assigned work under the contract is required to receive and document completion of the VA Privacy and Information Security Awareness and Rules of Behavior Training. This course can be found at https://www.tms.va.gov/learning/user/login.jsp under the contractor personnel's TMS account. The Contractor shall provide documented proof to the contracting officer that all contractor employees servicing a VA contract have received annual training.

16.15.2 PRIVACY AND HIPAA TRAINING COURSE

Successfully complete the appropriate VA TMS 10203 Privacy and HIPAA Training and annually thereafter; Each contractor assigned work under the contract is required to receive and document completion of Privacy and HIPAA Training. This course can be found at https://www.tms.va.gov/learning/user/login.jsp under the contractor personnel's TMS account. The Contractor shall provide documented proof to the contracting officer that all contractor employees servicing a VA contract have received annual training.

16.15.3 SYSTEM ADMINISTRATOR: YOUR ROLE IN INFORMATION SECURITY TRAINING COURSE

The Contractor's representative shall also ensure and certify that Contract employees who require system administrator access (elevated privileges) to VA information systems under this contract have also successfully completed the VA TMS 1357076 "System Administrator: Your Role in Information Security" role based training. This training must be completed at least once and is not required annually unless directed by the VA system owner, through the COR or CO.

16.15.4 ANNUAL CONTRACTOR SECURITY TRAINING COMPLIANCE REPORT

The Contractor shall provide the COR with an annual report (due each year on the date of the contract initiation) stating that all applicable employees involved this

contract have received their annual security/privacy training that meets VA's requirements. The report shall include the name of each employee and a copy of each training certification. VA anticipates the scope of this contract will require ten (10) or more contract individuals who will have incidental access to VA sensitive personal information. As such, in accordance with VAIQ 7058822, the Contractor's representative shall certify annually that all contractor employees and subcontractor employees, having access to VA sensitive personal information, have read, initialed each page and signed the last page of the Contractor Rules of Behavior (Attachment xx). The Contractor shall provide the COR with an annual report (due each year on the date of the contract initiation) stating that all applicable employees involved this contract have reviewed, initialed and signed the annual Contractor Rules of Behavior. The report shall include the employee name and the total number of employees who completed the Contractor Rule of Behavior. By signing the Rules of Behavior on behalf of the contract employees, the Contractor's representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing the VA's information and information systems. If TMS course 10176, described below, which includes Rules of Behavior, the manual Rules of Behavior is not required.

Note: To ensure Contractor personnel account(s) are not disabled, the Contractor must submit the training certificates to the COR at least two weeks prior to the training expiration date. Any remote access account having training certificates in an expired status will be automatically disabled by the remote access system.

16.16 BACKGROUND INVESTIGATIONS

16.16.1 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

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

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

c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.

e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award for back ground requests for elevated privleges by Contractor personnel who required elevated privileges to the system.

f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC); through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).

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

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

i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

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

All Contractor employees who require access to the Department of Veterans Affairs' computer systems or have access to sensitive information shall be the subject of a background investigation.

A Contractor's employee shall not commence working at VA under contract until the Contractor and the Contracting Officer receive notification from the VA Office of Security and Law Enforcement (OSLE) and/or Veteran Service Center (VSC) that the contract employee's background screening application was received complete. A favorable adjudication from the VA OSLE, via the VSC, must be received in order for a Contractor employee to proceed with contract performance. This requirement is applicable to all sub-Contractor personnel.

In accordance with VA OIT Field Security Service Bulletin No. 26 "*Contractor Computer Access Policy Guidance*", the background screening, known as a Special Agreement Check (SAC) and/or National Criminal History Check (NCHC), must be completed prior to starting work or being granted computer access. Contractor personnel can start work once the fingerprint SAC/NCHC has been favorably adjudicated by the OSLE or VSC. There are no current requirements for the full background investigation (under this contract it is the National Agency Check with Written Inquiries [NACI]) to be initiated. However, the NACI should be initiated within fourteen (14) days after appointment.

16.16.2 BACK GROUND INVESTIGATION SECURITY FORMS

Completed forms must be legible...

After the contract is awarded, the Contractor personnel shall complete all forms required for the back ground check and identification badge. The Contractor personnel shall submit the forms to the COR. The Contractor is encouraged to have its employee immediately download the background investigation packet from http://www.osp.va.gov/Security_and_Investigations_Center_FF.asp upon notification of contract award.

The Contractor shall provide complete Background Investigation application forms, for all Contract Employees, to the VSC, promptly and in sufficient time to meet the contract performance or delivery schedule (*or:* within five (5) calendar days after contract award).

If a delay in the notification from OSLE or VSC to the Contractor that a complete application has been received is due to the failure of the Contractor to provide a complete application as soon as practicable (*or:* within five (5) calendar days) after contract award, this delay shall not excuse the Contractor from meeting the contract performance or delivery schedule and may result in termination for cause.

The following required forms must be submitted to the VSC by the Contractor personnel before contract performance begins.

- Form #1-Contract Security Services Request Form
- Form #2-Fingerprint Request
- Form #3 PIV Sponsorship
- Standard Form 85, Questionnaire for Non-Sensitive Positions
- Optional Form 306, Declaration for Federal Employment
- Standard Form 86A, Continuation Sheet for Questionnaire
- Form 710, Authorization for Release of Information
- Self-Certification of Continuous Service
- Special Agreement Check Form
- Other forms as determined by VA

16.16.3 FINGER PRINTING

The Contractor personnel must make appointments at a VAMC nearest them for finger printing. The Contractor shall go to https://va-piv.com/ to schedule an appointment. The Contractor must bring a completed Finger Print Request form and two forms of photo identification with them to the appointment.

16.16.4 NATIONAL CRIMINAL HISTORY CHECK / SPECIAL AGREEMENT CHECK (NOTICE TO PROCEED)

The Contractor employee is cleared for proceeding upon completion of finger print screening/adjudication of the National Criminal History Check (NCHC) or Special Agreement Check (SAC) notification by the VSC. The NCHC is also referred to as the SAC. The NCHC form gives permission to the contract employees to begin work as long as the non-security contract requirements are met, (i.e. training, ROB, etc.).

16.16.4.1 UNFAVORABLE NCHC/SAC

Contract personal that do not have a favorable criminal history check will be identified and will not be permitted to perform work. The Contractor, when notified of an unfavorable determination by the VA, shall withdraw the employee from consideration from working under the contract, and at the request of the VA, submit another employee for consideration.

16.16.5 VETERANS SERVICE CENTER AND THE LITTLE ROCK SECURITY INVESTIGATION CENTER

After the Background Screening/investigate request has been submitted to the VA VSC or the Little Rock Security Investigation Center (SIC), a VSC or SIC representative will contact the Contractor personnel and provide further instructions for background screening signature pages. The VSC ensures that the background investigation is received and completed by the Office or Personnel Management (OPM). The VSC will submit the investigation request to the SIC simultaneously and keep tabs on the SIC status for a submitted investigation. Once the investigation is completed, all issues identified as unfavorable will be addressed with the contractor employee at that time. A determination can then be made and forwarded to OPM.

Upon completion of the background investigation, OPM will issue a Certificate of Investigation (CIO) which will be sent to the Contractor personnel by the SIC or VSC.

16.16.6 PIV BADGES

In accordance with VA OIT Field Security Service Bulletin No. 26 “Contractor Computer Access Policy Guidance”, the Contractor cannot get a PIV card until the full investigation is scheduled at OPM.

The VSC will contact the CO, COR and the Contractor personnel and provide further instructions for their PIV badges. The VSC will provide instructions on how to be issued a PIV badge. The VSC will complete the PIV badge application and will send notification for issuance.

16.16.6.1 PIV BADGE TYPE

Under this contract, the PIV badge type is “PIV” because the contract is greater than 180 days in a one year period. The Contractor shall present two forms of ID and will need a NCHC/SAC. The risk level is low as described in the following section.

16.17 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, “Personnel Security Suitability Program,” Appendix A)
Low	National Agency Check with Written Inquiries (NACI) A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, “Personnel Security Suitability Program,” Appendix A)
Moderate	Moderate Background Investigation (MBI) A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High	Background Investigation (BI) A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity is LOW and the level of background investigation is National Agency Check with Written Inquiries (NACI) and shown in Table 4 below.

Position Sensitivity and Background Investigation Requirements			
Task Number	Low/NACI	Moderate/MBI	High/BI
1	☒	☐	☐
2	☒	☐	☐
3	☒	☐	☐
4	☒	☐	☐
5	☒	☐	☐
6	☒	☐	☐

Table 4

16.18 CONTRACTOR PERSONNEL ROSTER

The Contractor shall deliver, maintain and update a Contractor Personnel Roster throughout the performance period. The submitted Contractor Staff Roster shall contain, at a minimum, the following data for each individual employee. It is imperative for the

Contractor to provide, at the request of VA, a listing of Contractor personnel performing services under the contract in order for the background investigation process to commence. This list will include the following information:

- Personal
  - Company Name
  - Full Name
  - Full Social Security Number
  - Date of Birth
  - Place of Birth
  - Position/Title

- Background Screening
  - NACI Submission to VCS Date
  - NACI VSC NCHC/SAC date
  - NACI VSC Notice of Completion
  - CIO

- PIV
  - VSC PIV Sponsorship Date
  - VSC PIV Card Issue Date
  - VSC PIV Card Expiration Date

- Training
  - Self-Domain User TMS ID
  - Privacy and HIPPA Training Completion Date (and copy of certificate)
  - VA Privacy, Information Security Awareness and Rules of Behavior Training Completion Date (and copy of certificate)
  - Elevated Privileges Training Completion Data (an copy of certificate)