

## B.2 PICIS BPA Statement of Work (SOW)/Terms and Conditions

### 1 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 Clinical Information Systems (CIS) and 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 CIS and ARK to meet mission goals.

The software applications that make up Picis Critical Care Manager and Picis Anesthesia Manager 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. Picis Critical Care Manager and Picis Anesthesia Manager replaced paper records used in the VISN's Anesthesia care areas. Certified Nurse Anesthetists, Anesthesiologists and other clinical staff use the Picis Critical Care Manager and Picis Anesthesia Manager System to manage the surgical/anesthesia patient information. Picis Critical Care Manager and Picis Anesthesia Manager 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).

### 2 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.

### 3 SCOPE OF WORK

3.1 The Contractor shall provide all software upgrades, maintenance and technical support services for the Picis Clinical Solutions Inc. Picis Anesthesia Manager system and Picis Critical Care Manager systems, in both the Test and Production environments, within the VISN Veterans Affairs Medical Centers (VAMC) as needed on a per order basis. For the purposes of this BPA, all references to "All VISNs" and "VISN wide" as used throughout this BPA refer only to those VISNs who have placed orders for maintenance against this BPA and are current on their annual maintenance fees. This maintenance and support shall include all scheduled preventive maintenance, unscheduled repairs/corrective software maintenance, technical support, database administration support and training services described in this PWS. The Contractor shall ensure that the Picis Anesthesia Manager and Picis Critical Care Manager operates in an efficient manner as intended as further defined in Attachment A, CIS/ARK System Specifications (latest

version).

## **4 PERFORMANCE DETAILS**

### **4.1 PERFORMANCE PERIOD**

The period of performance (POP) shall be one (1) twelve (12) month base period, with four (4) option periods of (12) months each.

There are ten 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

### **4.2 PLACE OF PERFORMANCE**

*Tasks under this SOW shall be performed at VISN VAMCs or may be performed remotely at Contractor facilities and will be designated on each order and at the direction of the COR.*

### **4.3 TRAVEL**

Travel shall be approved by the Contracting Officers Representative (COR), designated on each order, in advance and shall be reimbursed in accordance with the Joint Travel Regulation (JTR). Travel reimbursement rates will be determined in accordance with FAR 31.205-46, the JTR volume II and the Contractor's travel policy attached here as Schedule X.

## **5 REQUIREMENTS**

The Contractor shall perform the following:

## **5.1 KICKOFF MEETING**

The Contractor shall attend an upgrades, maintenance, and technical support Kickoff Meeting where maintenance and support shall be discussed in detail. The meeting will be conducted by conference call and coordinated by the COR within seven days after the blanket purchase agreement (BPA) is established and separately on each order.

### **Deliverable:**

- A. Kickoff Meeting

## **5.2 ANNUAL MAINTENANCE: UPGRADES, MAINTENANCE, AND TECHNICAL SUPPORT**

The Contractor shall perform all 24x7 proactive monitoring, remote and/or on-site maintenance, scheduled upgrades, preventive maintenance, unscheduled repairs, corrective maintenance, and technical support of all software listed as specified on each BPA order including all software version changes, upgrades, updates, patches, enhancements, corrections, and new releases during the performance period. VA anticipates quarterly software update releases in both the test and production environments at each facility. The Contractor shall coordinate maintenance and support with the COR and VAMC Points of Contact (POCs) as designated on each order.

The service under this task includes all labor, tools, test equipment, diagnostic software, supplies, parts, shipping, and Contractor staff supervision necessary to perform remote and/or on-site services defined herein. The Contractor shall provide overnight, next-day delivery of parts when needed to maintain full performance of the system. The Contractor shall provide shipping to return any defective parts from VA Facilities to the Contractor. There shall be no additional cost to the Government for shipping.

The Contractor shall not perform any additional services beyond those authorized at any time during the duration of the BPA orders without the expressed written approval of the CO in accordance with the terms and conditions of this BPA and each individual order.

### **5.2.1 TELEPHONE AND ON-LINE SUPPORT AND TECHNICAL CONSULTATION**

The Contractor shall provide VA with toll free corporate office telephone numbers, mobile telephone numbers and email addresses for the Contractor's key staff for both normal hours and after hours. The Contractor shall provide telephone and online remote support 24 hours per day, 7 days per week, and 365 days per year for both maintenance and technical support.

### **Deliverable:**

- B. Telephone and On-line Support and Technical Consultation

### **5.2.2 SCHEDULED MAINTENANCE**

The Contractor shall perform scheduled (preventive) maintenance in accordance with manufacturer's recommendations of all Picis Critical Care Manager and Picis Anesthesia Manager Software identified in each BPA order. The Contractor shall initiate corrective maintenance whenever software defects are discovered, in accordance with section 5.2.8, as a result of the Contractor performing scheduled/preventive maintenance services.

The Contractor shall provide scheduled maintenance and software updates during normal working hours or at a mutually agreed upon time by the COR on each order and the Contractor. The Contractor shall contact the COR and POCs to schedule mutually agreeable times for the performance of any scheduled activities. The Contractor shall recommend to the COR when equipment should be made available for scheduled maintenance. Upon COR approval, the Contractor shall finalize that schedule.

#### **Deliverable:**

- C. Scheduled Maintenance

### **5.2.3 UNSCHEDULED MAINTENANCE**

The Contractor shall provide the VISN and VAMCs with an unlimited number of unscheduled maintenance and technical support incidents during the performance period. Support includes both remote and on-site support. The Contractor shall perform all unscheduled corrective maintenance during the performance period of each order. The Contractor shall troubleshoot, repair and/or resolve, on request by the COR or POCs, all Picis Critical Care Manager and Picis Anesthesia Manager software identified in each BPA order. All software repaired by the Contractor shall be restored to manufacturer's specifications.

For technical problems, functional incidents or for questions during business hours, the Contractor shall provide the following communication options: call the Contractor Help Desk, create a field service request online or, email the incident or question.

For each request, the Contractor shall communicate the following via email or telephone to VAMCs in response to each event communicated by VA to the Contractor:

- a. Brief Description of the problem
- b. What version or software is being affected
- c. What equipment or component is being affected
- d. If this issue affects patient safety
- e. Workaround (if any) and expected release date of patch, upgrade or update (if any)
- f. Status and estimated completion date/time

The Contractor shall communicate all known software issues to the COR weekly via email or by telephone. The Contractor shall respond to a request for unscheduled corrective maintenance for a software issues, malfunctions or failures, by a fully qualified

representative, in accordance with response time requirements defined in Table 1 of Section 5.2.8.

**Deliverable:**

D. Unscheduled Maintenance

## **5.2.4 SYSTEM ENHANCEMENT SERVICES**

The Contractor shall provide all software upgrades, updates, and new versions including any replacement version or name revisions of the existing perpetual unlimited, non-exclusive software licenses. Enhancement services are performed as part of scheduled maintenance. All new software versions shall be covered in this effort including all subsequent versions designed to replace a version installed under any resultant orders issued against this BPA.

As part of scheduled and/or unscheduled maintenance the Contractor shall furnish, install and maintain all software upgrades, version changes and/or updates to the system. The Contractor shall monitor and maintain the system at the most current software releases including maintaining up-to-date current security patches. The Contractor shall provide any successor versions of Picis Critical Care Manager and Picis Anesthesia Manager including, software updates, version changes, and upgrades at no additional charge to the Government.

The Contractor shall follow the VA-nationally approved PICIS Medical User Group standard operating procedures by which software and/or hardware enhancement requests submitted by the VA are evaluated, prioritized, and implemented into the application updates at no additional development cost to VA during the duration of the order. Approved enhancements shall be provided by the Contractor and must be made available upon release to all VISN's under contract with Picis Clinical Solutions, Inc. The timeframe and method of delivery must be agreed upon by the COR and Contractor on each order and must be approved by the Contracting Officer.

Upon approval, the Contractor shall coordinate and distribute enhancement and maintenance updates and releases by using an appropriate electronic media, printed media or its website in accordance with VA requirements for electronic, printed or web based media.

The Contractor shall test the system after any changes to ensure that the system continues to function in accordance with manufacturer's specifications.

### **5.2.4.1.1 Updates**

The updates can be 1) initiated by the Contractor to improve functionality of the Picis Critical Care Manager and Picis Anesthesia Manager, 2) in response to changes in VA/VISN enterprise needs, 3) to maintain the Picis Critical Care Manager and Picis Anesthesia Manager as compliant with VA data standards, and/or regulatory requirements, 4) to maintain compatibility



with other systems, including the VA Standardized Terminology 5) to maintain VA standards in regard to security updates and patching.

It is estimated that there will be no more frequently than quarterly updates per year required related to maintaining standardized terminology and compatibility among systems. Regardless of the reason for the update or upgrade, the Contractor shall plan and schedule these upgrades through coordination with the COR as designated on each order.

Updates or corrections related to patient safety, regulatory requirements or interface to VistA will be classified as a patient safety issue with urgent priority. The Contractor shall provide an action plan within 30 days and shall implement an update (fix) within 180 days from the time of notification. Regardless of the reason for the update, the Contractor shall plan, coordinate and schedule these updates across the VISN using change management. All software and supporting release notes, user and technical literature shall be updated and provided to the VISN and - Facilities as software updates are implemented as designated on each order.

Software, including commercial Operating Systems, must not be self-canceling, which is interpreted to mean the function of the software will not be stopped due to elapsing time or other condition not identified with original equipment purchase. The Contractor is responsible to ensure any third-party provided software is included in this restriction.

The Contractor shall report and distribute maintenance updates or releases by using an appropriate electronic or printed media to the COR. Alternatively, the Contractor may offer access to maintenance copies through its company website.

**Deliverable:**

E. Updates

**5.2.4.1.2 Upgrades**

As VA CIS and ARK systems evolve, new functionality that is not currently known or available and beyond the scope of quarterly updates for fixes, standard terminology compliance, etc., will be desired by the Government to enhance patient safety, quality and to improve patient care. Furthermore, other VistA applications are likely to be developed in the future; therefore, the Picis Critical Care Manager and Picis Anesthesia Manager system to be installed must have the flexibility within the application to adapt to the changing needs of VA. These types of improvements and upgrades are defined as hardware, software and/or firmware changes that provide additional application features and functionality to an existing system. An example of an update is changing from Version 4.0 to Version 6.0. All Software Upgrades shall be included as part of maintenance at no additional cost. If an upgrade requires a major hardware upgrade in order to provide the additional functions it will be made available for purchase.

**Deliverable:**

F. Upgrades

#### 5.2.4.2 UPDATES AND UPGRADE TRAINING

The Contractor shall provide release notes and online, one hour, informational training sessions associated with any and all updates and/or upgrades at no additional cost.

##### **Deliverable:**

G. Updates and Upgrades Training

#### 5.2.4.3 ONSITE TECHNICAL SUPPORT

The Contractor shall provide onsite Picis technical support for a total of approximately 40 hours per week at VISN VAMCs VA Health Care Systems option as directed on each order. The Contractor shall provide, as directed on each order, one onsite Picis Critical Care Manager and Picis Anesthesia Manager technician to be located as detailed in the below table.

Facilities Served	Main Location	Hours of Onsite Support
Facility 1		
Facility 2		
Facility 3		

\*\* Will be filled out on BPA Order at the option of the VISN

On-site technical support shall begin within ninety (90) days of BPA Order and shall continue to the end of the base period and option periods. This optional support would include:

- Technical support and troubleshooting to staff and end-users at each medical center residing in the three Health Care Systems.
- Maintenance and growth of Picis Critical Care Manager and Picis Anesthesia Manager.
- Ongoing General Staff Training.
- Support for ongoing modifications and additions to content and system.
- Management of day-to-day system operations.
- Manage implementation of additional VA provided content into the Picis Critical Care Manager and Picis Anesthesia Manager.
- Maintenance, troubleshooting, and support of the Picis Critical Care Manager and Picis Anesthesia Manager solution.
- Support for ongoing Picis Critical Care Manager and Picis Anesthesia Manager Reports and analytics.
- Participation in Picis Critical Care Manager and Picis Anesthesia Manager VA User Groups.

##### **Deliverable:**

H. Onsite Technical Support



### **5.2.5 INTERFACE SUPPORT**

As part of the unscheduled and scheduled maintenance, the Contractor shall ensure that all Picis Critical Care Manager and Picis Anesthesia Manager side interfaces, including but not limited to, VistA, VistA Imaging/CPRS, Medical Devices, analytics, CIS, ARK, etc., and data transfer links are maintained consistently throughout the period of performance.

The VA shall coordinate with other Vendors and/or Contractors when necessary to accomplish this task.

#### **5.2.5.1 VISTA INTERFACE SUPPORT**

The integration of Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager with VistA shall be maintained by the Contractor to ensure that the Picis Critical Care Manager and Picis Anesthesia Manager side of the interface provides for transfer of clinical and administrative data between the Picis Critical Care Manager and Picis Anesthesia Manager and the VistA systems at each VAMCs. VAMCs shall implement the VistA side of the interfaces under a separate contract using the Document Storage Systems (DSS) DataBridge interface. The Contractor shall certify to the Contracting Officer and COR, as designated on each order, that its Picis Critical Care Manager and Picis Anesthesia Manager interface with VistA meets VHA National standards. The Contractor must perform ongoing certification as DataBridge updates are/or Picis Clinical Solutions, Inc. updates are released quarterly in order to verify that the Picis Critical Care Manager and Picis Anesthesia Manager retains full functionality and integration through the DSS DataBridge to VistA.

#### **Deliverable:**

- I. VistA Interface Support

#### **5.2.5.2 ANALYTICS INTERFACE SUPPORT**

The Contractor shall implement and maintain data integrations with the analytics databases.

The Contractor shall ensure that data is inclusive of all administrative and clinical data contained within the Picis Critical Care Manager and Picis Anesthesia Manager. The Contractor shall ensure that Picis Critical Care Manager and Picis Anesthesia Manager provide the data extracts to the analytics database(s) in the proper format. The VA shall coordinate with analytics Contractor(s), VA data warehouse staff, VAMC staff and the COR to validate the data.

The VA shall coordinate with other Vendors and/or Contractors when necessary to accomplish this task.

#### **Deliverable:**

- J. Analytics Interface Support

### **5.2.5.3 REPORT TEMPLATE SHARING**

All Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager reports produced using data aggregation, analytics, stored procedures, extractions, reporting services, business intelligence tools, or any other method, for information gathering and expressing (in any format) including but not limited to statistical analysis, compliance measures, performance measures, audits, quality improvement, usage trends, etc., that are developed by the Contractor for any VA facility or a VISN, must be made available to all other VISNs having the same Contractor at no additional cost to VA. Any services necessary to deploy, configure and/or customize the standard VA report will require additional cost to be quoted at time of request by the individual VAMC or VISN.

#### **Deliverable:**

K. Report Template Sharing

### **5.2.6 SYSTEM TESTING**

The Contractor shall participate in testing of the Picis Critical Care Manager and Picis Anesthesia Manager software and interfaces in accordance with the current version of the Government-approved Picis Critical Care Manager and Picis Anesthesia Manager Test Script (see Attachment B) (latest version), including connectivity tests with VistA, medical devices, VA networks, servers, work stations, data marts and data extractions for VA and/or commercial analytics systems.

Upon completion of any Picis Critical Care Manager and Picis Anesthesia Manager software repairs, updates, upgrades and installations, the Contractor shall test the system to ensure it is fully functional in accordance with the manufacturer specifications and the requirements in Attachment A, CIS/ARK System Specifications (latest version). The Contractor shall also be responsible for validating compliance with VA data standards and terminology for the clinical data in the Picis Critical Care Manager and Picis Anesthesia Manager.

Testing shall be coordinated and scheduled with the COR and facility POCs as designated on each order.

The Contractor shall in conjunction with VA create for approval Test Plan for installation of updates and upgrades including comprehensive test scripts that shall include a comprehensive actual-patient, parallel test. The Test Plan shall encompass a phased approach in which the integration with Interfaces is demonstrated in Phase I to ensure that no changes that were made to the system following the initial validation caused unintended effects that degraded the integration of the Picis Critical Care Manager and Picis Anesthesia Manager with the Interfaces.

Phase II shall demonstrate the validation of existing Picis Critical Care Manager and Picis Anesthesia Manager Reports to ensure they function properly after the update or upgrade and data extraction capability of the Picis Critical Care Manager and Picis Anesthesia Manager to the analytics database(s) to similarly show no degradation to the capability during the system development and integration. It is anticipated that continued refinement of the test scripts will

occur throughout the life of the contract at no additional costs to VA and will be reviewed as needed by VA.

The third phase shall demonstrate the full end-to-end functionality of the Picis Critical Care Manager and Picis Anesthesia Manager prior to final acceptance of an update or upgrade in a patient environment. In addition to testing for the immediate functionality of the Picis Critical Care Manager and Picis Anesthesia Manager in accordance with the System Specification, this test plan shall specifically incorporate user management, session management with VistA; data exchange with VistA; and extraction of data for completeness and for compliance with data standards and VA terminology. The Contractor must provide initial detailed scenarios for testing that demonstrate full functionality of the application. These scenarios may be modified by VA to include specific elements of the interface as defined in System Specifications.

The Contractor shall participate with VA in the system testing in accordance with the VA-approved Test Plan, including connectivity with medical devices and for readiness for operation at the VA facilities and on the VA networks and servers. The Contractor shall also be responsible for validating compliance with VA data standards and terminology for the clinical data in the Picis Critical Care Manager and Picis Anesthesia Manager ; and for testing the integrations of the Picis Critical Care Manager and Picis Anesthesia Manager with VistA/Interfaces and with any data extraction or transfer. If on-site Contractor services are required for these tests/integrations Time & Materials as well as Travel & Expenses will be billed at current rates and as per Schedule X.

**Deliverable:**

L. System Testing

### **5.2.7 MANDATORY CHECK IN/OUT AND REMOVEABLE 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, 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.

**Deliverable:**

### 5.2.8 RESPONSE TIME

The Contractor shall provide the upgrades, maintenance and technical support within a specified time published in the response time requirements below in Table 1. If the problem cannot be resolved over the phone or remotely, then an authorized representative of the company will commence work within the designated time identified, and will proceed progressively to rectify the problem without undue delay. Costs incurred by the Contractor for short-notice travel and additional per-diem charges per the Contractors travel policy for travel on weekends or holidays will be approved and reimbursed by the VA with appropriate receipts. A copy of the completed urgent service request will be accepted as “justification” for these additional costs as required per FAR 31.205-46 (b). The contractor shall be responsible to coordinate the method of response with the COR as designated on each order.

**TABLE 1**

<b>Severity &amp; Service Levels</b>	<b>Total Time to Respond/Resolve</b>
<b>Level 1</b> – System is down; major functionality is not working; material data loss or data corruption; unable to document a record; and end users unable to perform essential functions. (e.g. unable to document record)	Initial response to Incident Report within 1 hour, immediate attention by responding staff member; updates to user as applicable until resolve; Issue to be resolved or workaround implemented within 24 hours.
<b>Level 2</b> – System intermittently unable to perform essential functions, moderate to severe impact on documentation (e.g. intermittent slowness, periodic crashing and corruption of standing database tables)	Initial response to Incident Report within 2 hours, immediate attention by responding staff member; updates to user as applicable until resolve; Issue to be resolved or workaround implemented within 48 hours.
<b>Level 3</b> – Small number of end users intermittently unable to perform non-essential functions; Application functions and continues to be used (e.g. intermittently receive error message when booking a patient from one workstation)	Initial response to Incident Report within 24 hours; updates to User as required until resolved; Issue to be resolved or workaround implemented within 96 hours.
<b>Level 4</b> – Does not impact the delivery of documentation, does not impact the validity of data in the application (e.g. spelling error, misalignment of data on screen). Application clarification and enhancement requests.	Acknowledge receipt of issue within one week, Licensor resource assigned. Licensor work collaboratively with Licensee to resolve the issue. Software Program corrections are queued and evaluated by Picis for inclusion in a future service pack or version release
<b>Level 5</b> – Question regarding product usage. Inquiries about application functionality that do not impact patient care or major application function	Acknowledge receipt of issue within two weeks, Licensor resource assigned. Licensor work collaboratively with Licensee to resolve the issue/question.

If Full Performance cannot be restored within the above timelines an on-site response may be required as agreed upon by VA and Contractor. Full performance means that all defective software has been replaced with equivalent to or better than the original and that replacements meet or exceed the manufacturer’s original performance specifications.

### **5.2.9 SYSTEM UPTIME**

The system uptime shall be operable and available for use at least 99% of the time, 24/7/365, excluding acts of God, scheduled downtime and operator or hardware/network error.

Performance guarantees are subject to the system being installed as per the provided hardware and third-party software specifications. Downtime will be computed from notification of problem. Scheduled maintenance will be excluded from downtime. Operational Uptime will be computed during a month long time period.

### **5.2.10 DATA AND TERMINOLOGY STANDARDIZATION**

The Contractor shall support and participate in VHA data and terminology standardization.

Data and terminology standardization is critically important to the VHA and this agreement requires the implementation and use of VHA standardized data and terminology in the Picis Critical Care Manager and Picis Anesthesia Manager application. As such, the Contractor shall ensure use of standardized data and terminology in the software application.

The Contractor shall be responsible for representing and maintaining the clinical data of the Picis Critical Care Manager and Picis Anesthesia Manager in compliance with VA standards for data. The standards are maintained by VA and include sets of standard terminology, as well as a system of alpha-numeric data unique identifiers (term serial numbers) for representing the terminology. The Contractor shall ensure that Picis Critical Care Manager and Picis Anesthesia Manager are compliant with VA data standards in data representation and in exchange of data over interfaces with other systems. The most current listing of this standardized terminology will be provided to the Contractor in an Excel Spreadsheet by the National Picis Clinical Solutions, Inc. User Group Chair and COR. VA updates these standards quarterly and the Contractor shall ensure that the Picis Critical Care Manager and Picis Anesthesia Manager use the most current version throughout the period of performance.

Upon receipt of the new approved version, the Contractor shall ensure that data and templates loaded onto the VISN Facility Picis Critical Care Manager and Picis Anesthesia Manager production servers within twelve (12) weeks, and that they are locked to preclude any change to the Picis Critical Care Manager and Picis Anesthesia Manager database by VISN facility personnel. The Contractor shall be responsible for maintaining the currency of the data and templates during the performance period.

The Government anticipates updating its standardized data and terminology no more frequently than quarterly.

#### **Deliverable:**

N. Data and Terminology Standardization

#### **5.2.10.1 INTRA-VISN DATA STANDARDIZATION**

The Contractor shall ensure that the Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager functions and operates as part of a unified and standardized data solution for clinical and administrative data throughout the VISN. The Picis Critical Care Manager and Picis

Anesthesia Manager data must be fully available across the VISN, consistent for the data that it represents, consistent in the templates that it provides to enter and access data, integrated at the facilities, and also integrated with the VistA systems within the VISN, and with the VISN's analytics solution(s). Availability of data across the VISN shall be near real-time, and is subject to data management that supports the clinical and administrative needs of the VISN, its facilities and its services. Data and templates for entering or accessing data are to be implemented and managed at the VISN-level. Functionality is to be implemented in Picis Critical Care Manager and Picis Anesthesia Manager for individualized displayed configurations as needed to respond to unique needs in patient care delivery and management at the facility level. The Contractor must provide near real-time technical and clinical consultations upon requests from VA for any regulatory agency which is examining quality control.

Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager versions implement function and operations for implementation of VA standardized data, integration with VistA and extracts to analytics systems, and for providing data access and availability throughout the VISN. The Contractor shall maintain a standardized Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager version for the VISN that meets its specific needs. The VISN-level version is based on a National Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager Version, which implements national VA Standardized Data, interfaces with VistA and extracts to analytics and the data warehouse that accounts for the specifics of the VISN, its facilities and its departments.

The database and content updates delivered by the Contractor shall contain exactly and only the VA National Standardized Terminology.

**Deliverable:**

O. Intra-VISN Data Standardization

**5.2.10.2 INTER-VISN DATA STANDARDIZATION**

In compliance with the Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager Version, the Contractor shall provide maintenance services for the VISN current software and make available any upgrades of its Picis Critical Care Manager and Picis Anesthesia Manager to all VISNs with active and in good standing delivery orders for no additional license fees. In addition, non-proprietary reports and/or non-proprietary enhanced reporting tools purchased by any individual VISNs for use shall be made available for purchase to all VA VISNs utilizing compatible versions of Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager.

The current version of the Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager shall be planned, tested and validated for proper functionality and operation with versions of VA standardized data, and versions of the Interfaces with VistA and with extracts and transfers to analytics and the data warehouse. The Contractor shall maintain the current release, and then shall offer all subsequent, future versions of the Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager software for no additional license fees to VISNs who are current on their annual maintenance fees. These future software updates may be mandated from



regulatory requirements. The future software updates shall be managed under National Change Management/VISN directions in coordination with VA Central Office (VACO).

To facilitate the potential for the standardization of Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager Versions, the VA Change Control Board includes participation from VA representatives, as well as representative of Picis Clinical Solutions, Inc. and also participation of the Contractors for interfaces and the analytics. The Contractor shall ensure that all software updates are tested in non-clinical environments before making them available to VISNs. This includes the applicable interfaces.

The Contractor shall participate in a VA-led Picis Clinical Solutions, Inc. User Group that will address Picis Critical Care Manager and Picis Anesthesia Manager configuration changes proposed by the Contractor or the VA User Group.

The Contractor shall ensure proper functionality and operation of the Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager at each facility by complying with VA standardized data principals. The Contractor shall coordinate changes to the Picis Critical Care Manager and Picis Anesthesia Manager data elements and standards, and interfaces with the COR under VA Change Management. The Contractor shall make available all Picis Critical Care Manager and Picis Anesthesia Manager updates to all VISNs on contract who are current on their annual maintenance fees, including VAMCs, at no additional costs for licenses to these VAs thereby making it possible to achieve the standardization goals within the National Picis Clinical Solutions, Inc. User Group. Implementation or Installation Services required will be quoted and paid to the Contractor on a Time and Materials basis plus any associated travel expenses.

The VA Change Control Board approves all changes to data standardized terms. The VISN will request an urgent change to the standardized terms and VA Change Control Board may offer a “quick” approval to this “urgent” need by the VISN. The Contractor shall change the standardized terms based on these approved changes to these standardized data terms. “Urgent is defined as: A requirement by Federal Law, Congressional Mandate, Joint Commission Requirement, or New VA Directive.”

#### **Deliverable:**

P. Inter-VISN Data Standardization

### **5.2.11 CHANGE MANAGEMENT AND CONFIGURATION CONTROL**

To facilitate the requirement for a national Picis Critical Care Manager and Picis Anesthesia Manager version, the Government has established a Change Management process. The process includes participation from Government representatives, as well as the Picis Critical Care Manager and Picis Anesthesia Manager Contractor and third party interface Contractors. This process ensures that all software updates are coordinated among software providers. Proper functionality and operation of the Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager at VISNs involve VA standardized data and interfaces with other systems. The Contractor shall ensure that the Picis Critical Care Manager and Picis Anesthesia Manager software components are made available to each facility within the VISN which is current in their



maintenance. Software updates must be tested in non-clinical environments before making them available to all VISNs.

The Contractor shall participate in a Government-led Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager Change Management Board and Picis Clinical Solutions, Inc. User Group that shall address any proposed Picis Critical Care Manager and Picis Anesthesia Manager configuration changes. Picis Critical Care Manager and Picis Anesthesia Manager User Group meetings address Picis Critical Care Manager and Picis Anesthesia Manager configuration changes proposed by the Contractor or changes that are necessitated by interface changes proposed by the VA Picis Clinical Solutions, Inc.

User Group responsible for various components of the system or by Government standards changes. Participation may include telephone conference calls, online live meetings and face to face meetings. Face to face meetings will incur additional costs for the Contractor's time plus related travel expenses. The Contractor shall coordinate all system changes with VA's Change Control Board using VA's change procedures and through the VA COR for the system.

The Contractor shall implement all changes to the Picis Critical Care Manager and Picis Anesthesia Manager application or interfaces approved by the COR into routine quarterly update and version upgrades to Picis Critical Care Manager and Picis Anesthesia Manager or associated interfaces such that Picis Critical Care Manager and Picis Anesthesia Manager continues to function and operate correctly. Changes will be coordinated and managed with the COR and prioritized with the Contractor.

**Deliverable:**

Q. Change Management and Configuration Control

**5.2.11.1 Synchronization of Product Warranty Expiration**

During the performance period, VAMCs will have or may have Picis Critical Care Manager and Picis Anesthesia Manager products that were acquired under a previous or separate acquisition/contract. In the event that items not listed in Picis Clinical Solutions, Inc. Inventory List, provided at each order, reach the warranty expiration date, those items will be added to, and maintained under, this agreement through a modification by the Contracting Officer on each order. As items not listed in the Picis Clinical Solutions, Inc. Inventory list reach warranty expiration, those items will be considered for addition to this agreement through a modification by the Contracting Officer on each order. New orders/items will be assigned the same expiration date and the associated fees for these items/orders ONLY will be prorated such that all orders/items will be maintained on the same annual renewal schedule. If items on the Inventory List are removed from service, likewise, the agreement and or order will be modified to remove items no longer requiring these services.

**Deliverable:**

R. Synchronization of Product Warranty Expiration

**5.2.12 Reports/Documentation**

### **5.2.12.1 Service Reports**

The Contractor shall provide a Service Report to the pertinent Facility VA Point of Contact (POC) designated by the COR at the completion of a service call prior to departing the VAMC or at the conclusion of remote service. The Service Report shall document the services rendered and shall include date and time of service, description of services, the latest version of software patch or upgrade, results of services, name of individual who performed the services, and travel, and labor information.

#### **Deliverable:**

- S. Service Reports

### **5.2.12.2 Manuals, Release Notes, and Service Bulletins**

The Contractor shall provide an electronic copy of the user manuals, system administrator manuals, operating/maintenance and/or technical manuals, release notes, service bulletins, etc. necessary for the operation and support of the software to the COR as designated on each order.

#### **Deliverable:**

- T. Manuals, Release Notes, and Service Bulletins

### **5.2.12.3 Disaster Recovery and Failover Plan**

The Contractor shall provide a disaster recovery and failover plan, in the occurrence of hardware (to those VISN locations where the Contractor has provided hardware), software failure, an outage, natural occurrence (such as hurricanes, tornadoes, earthquakes, etc.). The Contractor shall provide support for roll over to other servers.

#### **Deliverable:**

- U. Disaster Recover and Failover Plan

## **5.2.13 PRODUCT MODIFICATION, REMOVAL, OR RECALL**

If any product supported under this agreement and subsequent orders requires modification, is removed or recalled by the Contractor or manufacturer, or if any required modification, removal or recall is suggested or mandated by a regulatory or official agency, the Contractor shall notify the COR within forty-eight (48) hours via email notification that includes the following information:

- a. Complete item description and identification
- b. Reasons for modifications, removal or recall
- c. Necessary steps for return for credit, replacement or corrective action.

The Contractor shall provide the above information to all VA Facilities who purchased the product. The COR shall be provided a copy of the notification and a list of all VA facilities notified. The Contractor shall perform all steps required for return for credit, replacement or corrective action for all affected Facilities.

#### **Deliverable:**

#### **5.2.14 EMERGENCY OPERATIONS**

The Contractor shall provide an Emergency Plan and continuity of operations plan. If there is a disaster or emergency situation the Contractor shall provide a back out or failover process. The emergency and continuity of operations plan shall be provided ten calendar days after award of agreement and shall be reviewed and updated as needed. The plans shall document the Contractor strategy, plan and procedures to maintain Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager during an emergency.

When any disruption of normal, daily operations occur, the Contractor shall promptly open an effective means of communication and verify the following:

- Key points of contact (VA and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- Planned temporary work locations or alternate facilities
- How the Contractor will communicate with VAMC's, VISN's and VA during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
- Telephone numbers
- E-mail addresses
- Procedures for protecting VA furnished equipment (if any)
- Procedures for safeguarding sensitive and/or classified VA information (if applicable)

#### **Deliverable:**

W.            Emergency and Continuity of Operations Plan

#### **5.2.15 TRANSITION / ORIENTATION SUPPORT**

##### **5.2.15.1 OUTGOING TRANSITION / ORIENTATION SUPPORT**

The Contractor shall develop and deliver an Outgoing Transition Plan, at additional cost, in the event that all or part of the tasks are terminated or completely transitioned to the Government or a new Contractor at the end of the period of performance on each order.

The Contractor shall submit details for the Outgoing Transition Plan, and execute the Outgoing Transition Plan upon Government approval. The Outgoing Transition Plan may be exercised by the Government anytime during the period of performance. The Draft Outgoing Transition Plan shall be delivered within ten business days of award of order. The Contractor shall provide subject matter expert (SME) support to affect the requisite knowledge transfer in accordance with the resulting Transition Plan and schedule. VA will approve the final Outgoing Transition Plan.

The Contractor shall work collaboratively with VA personnel and DSS, Inc (for DataBridge concerns). As part of collaboration, the Contractor shall convey information, at the Contractors' discretion, as it pertains to VA, its processes, diagrams and reports that emanate from the system that may be determined to support this collaboration. This support shall also consist of providing advice, clarification or explanation to facilitate the understanding of the information presented.

At a minimum, the Contractor shall address the following areas in the Outgoing Transition Plan:

- a) Roster of key POCs with email address and telephone numbers
- b) Transition timeline with key milestones
- c) Data/databases migration/archiving
- d) Inventory and transition of historical data
- e) Procedural manuals/guidelines
- f) Operating instructions
- g) Templates used in day-to-day operations
- h)
- i) Procedures to introduce Government personnel, programs and users to the Contractor t processes
- j) Strategy and approach regarding personnel staffing and training during the transition period
- k) Process for transfer of on-hand inventory, if applicable
- l) Transition checklist
- m) Signed turnover agreements

**Deliverable:**

- X. Outgoing Transition Plan

### **5.2.16 TRAINING**

The Contractor shall provide remote and on-site user training to both clinical and non-clinical staff on the use and operations of the Picis Critical Care Manager and Picis Anesthesia Manager software/ as designated on each order. Final dates and times for all training at each location shall be mutually agreed upon between the Contractor and with the POC at each individual site. The Contractor shall contact the COR and POC to discuss and schedule training.

Training shall be conducted as designated on each order, but not be limited to, initial training of new personnel in operation and care of the Picis Critical Care Manager and Picis Anesthesia Manager, as well as an actual demonstration of the system, and its interaction with the existing systems identified, i.e., VistA, medical device integration, GDR and VA and/or commercial analytics solutions. The Contractor shall provide guidance on completing any adjustments or other actions that may be undertaken by operating personnel in the event of malfunction or failure. The Contractor shall provide training manuals and instruction materials with implementation with each update to each attendee. VA will provide the total number of personnel to be trained. Training shall be provided in various forms of media such as, but not limited to, tutorials, manuals, computer-based training, distance and on-site training, as appropriate. The Contractor must provide web-based training, self-paced to include modular training for clinical, technical and

administrative that must be shared across VISNs at no additional cost to VA.

In addition to the training outlined above, training will also include, but not be limited to, the following:

1. System Administrator training which may be conducted at multiple sites including but not limited to off-duty tours selected by the VISN COR and VAMC POCs.
2. End User training at each individual facility The Contractor will work with the VA to develop a recorded WebEx-style version of this training that can be voice recorded and played back by attendees on demand. This will be an additional service and quoted on a fixed-fee basis at then-current rates for the work.
3. Reporting Tool/Analytics User training at each individual facility The Contractor will work with the VA to develop a recorded WebEx-style version of this training that can be voice recorded and played back by attendees on demand. This will be an additional service and quoted on a fixed-fee basis at then-current rates for the work..

**Deliverable:**

Y. Training

## **6 METHOD AND DISTRIBUTION OF DELIVERABLES**

The Contractor shall deliver documentation in electronic format, unless otherwise directed on each order. Acceptable electronic media include: MS Word 2010 or current version, MS Excel 2010 or current version, MS PowerPoint 2010 or current version, MS Project 2010 or current version, MS Visio 2010 or current version, and Adobe Postscript Data Format (PDF) current version.

## **7 PHYSICAL SECURITY AND SAFETY REQUIREMENTS**

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.

1. The Contractor personnel shall wear visible identification at all times while they are on the premises.
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.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
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.

## **8 TB SCREENING**

Prior to performing on-site visits, the Contractor shall provide written certification that all contract employees assigned to the work site have had a pre-placement tuberculin screening within 90 days prior to assignment to the worksite and been found have negative TB screening reactions as requested. The Contractor shall be required to show documentation of negative TB screening reactions for any additional workers who are added after the 90-day requirement before they will be allowed to work on the work site.

NOTE: This can be the Center for Disease Control (CDC) and Prevention and two-step skin testing or a Food and Drug Administration (FDA)-approved bloodtest.

Contract employees manifesting positive screening reactions to the tuberculin shall be examined according to current CDC guidelines prior to working on VHA property.

Subsequently, if the employee is found without evidence of active (infectious) pulmonary TB, a statement documenting examination by a physician shall be on file with the employer (construction contractor), noting that the employee with a positive tuberculin screening test is without evidence of active (infectious) pulmonary TB.

If the employee is found with evidence of active (infectious) pulmonary TB, the employee shall require treatment with a subsequent statement to the fact on file with the employer before being allowed to return to work on VHA property.

Information shall be provided directly to the COR at each facility

## **9 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 designated on each order, 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.

## **10 SCHEDULE FOR DELIVERABLES**

SCHEDULE FOR DELIVERABLES WILL BE DETERMINED UPON DETERMINATION OF DUE DATES AND FINAL DELIVERABLES

TASK	DELIVERABLE ID	DELIVERABLE DESCRIPTION	DUE	FREQUENCY

5.1	A	KICKOFF MEEETING	7 DAYS AFTER AGREEMENT AWARD/ AS DESIGNATED ON EACH ORDER	ONCE
5.2.1	B	TELEPHONE AND ON-LINE SUPPORT AND TECHNICAL CONSUTATION	ON-GOING	24/7/365
5.2.2	C	SCHEDULED MAINTENANCE	ON-GOING AS DESIGNATED	ON-GOING AS DESIGNATED
5.2.3	D	UNSCHEDULED MAINTENANCE	AS DESIGNATED ON EACH ORDER	24/7/365
5.2.4.1.1	E	UPDATES	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
5.2.4.1.2	F	UPGRADES	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
5.2.4.2	G	UPDATES AND UPGRADES TRAINING	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
5.2.4.3	H	ONSITE TECHNICAL SUPPORT	AS DESIGNATED	AS DESIGNATED
5.2.5.1	I	VistA INTERFACE SUPPORT	ON-GOING AS DESIGNATED	ON-GOING AS DESIGNATED
5.2.5.2	J	ANALYTICS INTERFACE SUPPORT	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
	K	REPORT TEMPLATE	AS NEEDED	AS NEEDED



5.2.5.3		SHARING	ON EACH ORDER	ON EACH ORDER
5.2.6	L	SYSTEM TESTING	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
5.2.7	M	MANDATORY CHECK IN/OUT AND REMOVABLE MEDIA SCANNING	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
5.2.10	N	DATA AND TERMINOLOGY STANDARDIZATION	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
5.2.10.1	O	INTRA-VISN DATA STANDARDIZATION	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
5.2.10.2	P	INTER-VISN DATA STANDARDIZATION	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
5.2.11	Q	CHANGE MANAGEMENT AND CONFIGURATION CONTROL	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
5.2.11.1	R	SYNCHRONIZATION OF PRODUCT WARRANTY EXPIRATION	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
5.2.12.1	S	SERVICE REPORTS	ON GOING	MONTHLY
5.2.12.2	T	MANUALS, RELEASE NOTES AND SERVICE BULLETINS	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
5.2.12.3	U	DISASTER RECOVER AND FAILOVER PLAN	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
5.2.13	V	PRODUCT MODIFICATION, REMOVAL OR RECALL	WITHIN 48 HOURS	AS NEEDED
5.2.14	W	EMERGENCY OPERATIONS	10 DAYS AFTER AGREEMENT AWARD	UPDATED AS NEEDED
5.2.15.1	X	OUTGOING	END OF POP	ONCE

		TRANSITION/ORIENTATION SUPPORT	AS DESIGNATED	
5.2.16	Y	TRAINING	COMPLETED NLT 30 DAYS AS DESIGNATED ON EACH ORDER	AS NEEDED ON EACH ORDER

## 10.1 SPECIAL SHIPPING INSTRUCTIONS

Prior to shipping any 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 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)

## 11 .0 POINTS OF CONTACT

### VA Program Manager:

Name: TBD per facility based upon issuance of the order.

Address:

Phone:

Email:

### Contracting Officer's Representative:

Name: TBD per facility based upon issuance of the order.

Address:

Phone:

Email:

**BPA Contracting Officer:**

Name: Brian Love

Address: 10300 Spotsylvania Avenue, Suite 400, Fredericksburg, VA 22408

Phone: (202) 531-0557

Email: [brian.love@va.gov](mailto:brian.love@va.gov)

**11.1 FACILITY POINTS OF CONTACT**

The COR shall provide a list of facility point of contacts to the Contractor upon issuance of a BPA Order.

**12. VA FURNISHED PROPERTY AND VA FURNISHED INFORMATION**

There will be government furnished property for the on-site technical support engineer. The VA shall provide contract staff with end user computing equipment (desktop or laptop) including common desktop computing software and hardware to perform the required services. The VA shall provide VA-specific software such as Virtual Private Network (VPN) and SharePoint access.

**13. Security Requirements**

This Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager upgrades, Maintenance and Technical Support 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:

- 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 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 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 one 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.
- d. 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 VA’s information and information systems.

### **13.1 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 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.

### **13.2 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.

### **13.3 NATIONAL CONTRACTOR ACCESS PROGRAM, INTERCONNECTION SECURITY AGREEMENT / MEMORANDUM OF UNDERSTANDING, AND REMOTE ACCESS**

The Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager Upgrades, Maintenance and Technical Support contract involves Contractor remote access to VAVISN 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 Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager 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 Picis Critical Care Manager and Picis Anesthesia Manager specific hardware and software enabling the Contractor to perform the required Upgrades, Maintenance and Technical Support.

The Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager /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 Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager /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 regarding the development, management, operation, and security of a connection between Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager and VA. The agreement governs the relationship between Picis Clinical Solutions, Inc. and VA including designated managerial and technical staff, in the absence of a common management authority.

### **13.4 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 Picis Critical Care Manager and Picis Anesthesia Manager devices. These must be completed to assure that Picis Critical Care Manager and Picis Anesthesia Manager devices are integrated effectively and securely. A sample manufacture disclosure statement, pre-procurement assessment and pre-implementation items are included in Attachment C of this PWS.

### **13.5 NON-DISCLOSURE AGREEMENT**

The Contractor shall not disclose any information encountered during the conduct of this work.

The Contractor shall keep confidential, not disclose, or make use of VA information, at any time either during or subsequent to the contract performance period, any confidential information, knowledge, data or other information of VA relating to processes, test data, customers, business plans and strategies, budgetary information or other subject matter pertaining to any business of VA. This agreement also pertains to any deliverable during the course of this contract. The Contractor shall not deliver, reproduce or in any way allow any such confidential information, knowledge, data or other information or any documentation relating thereto, to be delivered to or used by any third parties, including the Contractor, without specific direction or consent of a duly authorized representative of VA. The Contractor must maintain VA proprietary and otherwise confidential information, knowledge and data in confidence shall only be relieved by written consent from VA. At the conclusion of this contract or in the event of termination of Contractor personnel with the Contractor, the Contractor personnel agree to promptly surrender and deliver to VA all records, materials, equipment, documents and data of any nature pertaining to the business of VA. The Contractor personnel will not take with them any confidential information knowledge, data or other information, or any documentation, which may be produced or obtained during the course of this contract.

### **13.6 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).

### **13.7 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 VA.

VA information should not be co-mingled with any other data on the Contractor/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 VA or destroyed in accordance with VA's sanitization requirements.

VA reserves the right to inspect the contractor's and subcontractor's process on how they remotely access the VA system 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 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 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.

The Contractor shall not store VA information off site. VA information is only stored at the VAMC's.

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.

### **13.8 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 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 specific to the vendor's products,. 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 vendor's Systems (including the confidentiality or integrity of its data and operations, or the availability of the vendor's system). Such issues shall be remediated as quickly as is practical, but in no event longer than five days.

All other vendor product specific 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.

## **13.9 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 VA during its use. All of the security controls required for any government furnished equipment (GFE) issued 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 Picis Clinical Solutions, Inc. Picis Critical Care Manager and Picis Anesthesia Manager systems containing media (hard drives, optical disks, etc.) with VA sensitive information will not be returned to the vendor at the end of use, lease, for trade-in, or other purposes. Storage media shall be retained by VA and shall not be returned to the Contractor.

## **13.10 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.

### **13.11 DATA BREACH PROCEDURE**

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.

### **13.12 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 ten 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.

### **13.13 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, Puerto Rico and/or Canada. 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.

### **13.14 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 theTMS, the Contractor personnel shall contract the VA TMS Help Desk at [vatmshelp@va.gov](mailto: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 one 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.

#### **13.14.1 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 Contractors are NOT required to manually or electronically sign a separate Rules of Behavior.

#### **13.14.2 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.



### **13.14.3 SECURITY TRAINING COURSES**

#### **13.14.3.1 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.

#### **13.14.3.2 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.

#### **13.14.3.3 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.

### **13.14.4 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 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. 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 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.**

## **13.15 BACKGROUND INVESTIGATIONS**

### **13.15.1 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 background requests for elevated privileges 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 adjudicate 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 14 days after appointment.

### **13.15.2 BACKGROUND 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](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.

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

### **13.15.3 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.

### **13.15.4 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.).

#### **13.15.4.1 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 VA, shall withdraw the employee from consideration from working under the contract, and at the request of VA, submit another employee for consideration.

### **13.15.5 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 of 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.

### **13.15.6 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.

### **13.15.7 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.

### **13.16 POSITION / TASK RISK DESTINATION LEVEL(S)**

<b>Position Sensitivity</b>	<b>Background Investigation</b> (in accordance with Department of Veterans Affairs 0710 Handbook, “Personnel Security Suitability Program,” Appendix A)
-----------------------------	---

<b>Low</b>	<b>National Agency Check with Written Inquiries (NACI)</b> 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.
<b>Moderate</b>	<b>Moderate Background Investigation (MBI)</b> 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.
<b>High</b>	<b>Background Investigation (BI)</b> 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 for this any orders under this agreement is LOW and the level of background investigation is National Agency Check with Written Inquiries (NACI)..

### 13.17 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)