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) to those responsible for providing care to the Veterans throughout all the points of health care in a timely and compassionate manner. VHA depends on CIS to meet mission goals.

The software applications that make up Essentris provide data collection, access and reporting, building of specific environments, auto-triggers, database query, real-time access to information in the ICU, 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. Essentris replaced paper records used in the VISN ICUs. Nurses, Respiratory Therapists, Physicians, and other clinical staff use the Essentris System to manage the ICU patient information. Essentris 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 Statement of Work (SOW):

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.

The listing of reference materials in this section is not intended to require the Contractor to perform any other specific tasks or services that are not expressly described in and required to be performed by other sections in this SOW.

3 SCOPE OF WORK

3.1 The Contractor shall provide all software upgrades, maintenance, and technical support services for the CliniComp Essentris systems, in both the Test and Production environments, within the VISN Veterans Affairs Medical Centers (VAMCs). The upgrades, maintenance, and support shall include all scheduled preventive maintenance, unscheduled repairs/corrective maintenance, technical support, database administration support, and training services described in this SOW. The Contractor shall provide necessary support services so that the Essentris systems operate in an efficient manner as generally intended as further defined in Attachment A, CIS System Specifications (latest version).

The terms and conditions set forth in this SOW are to provide for maintenance and support services only for the existing CliniComp Intensive Care Unit (ICU) Clinical Information System ("**ICU CIS**" or "**CliniComp CIS**") which have been previously procured and installed by seven (7) VISNs as of the present time. Generally, each VISN separately established and negotiated the requirements, including technical specifications and contractual terms and conditions

pursuant to which each CliniComp CIS was separately awarded and procured ("**VISN Procurement Contract**"). This BPA Contract awarded under this Solicitation shall govern the terms and conditions for the maintenance and support of each CliniComp CIS identified in each task order issued under this Contract within the scope of the original implementation, deployment and licensing by each VISN of the previously accepted CliniComp CIS systems.

4 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (POP) shall be one (1) twelve (12) month base period, with four (4) consecutive option periods of (12) months each. The dates set forth in the B.2 PRICE/COST SCHEDULE above for the POP applicable to the base year and each option year are not subject to change. Any VISN that adopts this contract after the beginning of the base year or any option shall only be entitled to the benefit of the period remaining in the base year or option period, as applicable.

The Contractor shall provide support 24 hours per day, 7 days per week, and 365 days per year. However, normal hours of work are defined as Monday through Friday from 7:00a.m. to 6:00p.m. Pacific Time, excluding Federal holidays or as otherwise arranged with the Contracting Officer's Representative (COR).

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. Work may be performed at remote locations other than Contractor facilities with prior approval 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 at cost in accordance with the Joint Travel Regulation (JTR). Travel costs will be determined in accordance with FAR 31.205-46, the JTR volume II and the Contractor's travel policy.

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 express delivery of replacement parts when needed to maintain full performance of the system. The Government 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 replacement parts.

The Contractor shall supply and install replacement or additional hardware components consisting of any server components (including associated operating system software) and data acquisition equipment technically required during the period of performance on account of the occurrence of the technical or functional obsolescence of such hardware. For purposes of the Contractor's responsibility, "obsolescence" means and includes only circumstances when component replacements or additions are technically required to (a) maintain the reliability of a system in compliance with the uptime requirements of the contract, (b) permit the installation and clinical use of the most recent update/upgrade version of the CliniComp CIS software made available by the Contractor for installation, (c) maintain the performance and responsiveness of a system, including performance following installation of an update/upgrade or (d) the manufacturer of the operating system software no longer supports security updates for such software for use with the installed server hardware, provided, "obsolescence" excludes, and the Contractor shall have no responsibility for, component replacements or additions that are needed on account of implementation of new clinical or administrative needs arising after the date of the applicable VISN Procurement Contract and required to be supported under such contract, including new software packages, material increases in the number of end users, quantities of electronic medical records stored on the system, additional interfaces to third party systems or new categories of medical devices or other functions or features required to be implemented by the Government that requires significant additional computing resources. While no specific replacement schedule is being established, historically the Contractor's experience is replacement of computer servers (or major components) is needed at intervals of between 3 to 5 years, and data acquisition hardware is necessary after 5 to 7 years due to the occurrence of one or more of the circumstances described in preceding clauses (a) to (d) above. The Contractor acknowledges that it is aware that many of the CIS systems previously deployed are approaching these useful life ranges.

Nothing in the preceding provisions shall be interpreted to require the Contractor to supply or install: (A) server or other equipment components that are materially superior to the category, quality and relative cost to that required under the applicable VISN Procurement Contract, or (B) supply additional hard drives and associated components resulting from increases in data storage requirements beyond those contemplated under the applicable VISN Procurement Contract. Nothing in the preceding provisions shall be interpreted to require the Contractor to supply or install: (A) server or other equipment components that are materially superior to the category, quality and relative cost to that required under the applicable VISN Procurement Contract, or (B) supply additional hard drives and associated components resulting from increases in data storage requirements beyond those contemplated under the applicable VISN Procurement Contract.

The preceding paragraphs are a general description of services to be performed under the SOW and are intended as a summary overview and is subject to the clarifications or limitations in later sections of this SOW. In addition, 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 any required scheduled (preventive) maintenance in accordance with manufacturer's recommendations of all CliniComp CIS systems identified in each BPA order. The Contractor shall initiate corrective maintenance whenever equipment defects are discovered as a result of the Contractor performing scheduled/preventive maintenance services or its monitoring of the systems.

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, when a problem cannot be resolved remotely, 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 CliniComp CIS equipment and 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 or make available on line, 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 known material software and hardware issues to the COR weekly via email or by telephone. The Contractor shall respond to a request for unscheduled corrective maintenance for a software or hardware 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

5.2.3.1 SYSTEM RECOVERY SERVICES

The VAMCs will assume responsibility for any non-standard hardware and that the Contractor will not be held responsible for any damage, etc. that may result from a power or environmental failure.

In the event of a crash or major incident due to power loss or other major adverse event involving sites utilizing non-standard hardware, the Contractor shall provide evaluation/assessment and system restoration services, assuming no damage is identified ("System Recovery Services"). The cost for these System Recovery Services shall be $7,500 per incident. If damage is identified, the Contractor shall (as part of their evaluation/assessment) provide the VAMC with itemized estimated costs to restore the system to operational status.

5.2.3.2 OPTIONAL CLIN: UNINTERRUPTIBLE POWER SUPPLY (UPS)

(Optional Task – Base and All Option Periods) Upon receipt of a Delivery Order under CLIN 0004, the Contractor shall install the uninterruptible power supply (UPS) which is a part of the standard hardware configuration of the CliniComp System; this includes the UPS, batteries and power strips.

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. Upgrades, updates, and new versions generally refer to software releases or update containing patches, bug fixes and modifications, enhancements or improvements to existing applications and such items are included in the scheduled maintenance services without additional charge; provided, however, CliniComp is not required to deliver or implement any new product offering containing material new functions and features which are generally offered for purchase by CliniComp to its customers as new products and any such new products may be separately purchased by the Government. Upgrades, updates, and new versions and releases shall be deemed delivered under the original standard commercial license as modified or supplemented by the applicable VISN Procurement Contract. The maintenance services and pricing do not include supplying or developing presently unknown and undefined customer software engineering changes to add new features, functionality, enhancements or improvements to the deployed CliniComp CIS systems, whether software or hardware, However, the Contractor will maintain a formal process for receiving, recording and assessing software feature requests from all customers, including the VA, and for deciding what features to include in its future commercial software development program and new releases. Any request by the VA for enhancement will be approved on a uniform basis by the VA CliniComp Vendor User Group before submission to the Contractor

Upon VA CliniComp Vendor User Group 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 continue monitoring the system after any changes to ensure that the system continues to function in accordance with manufacturer's specifications.

Deliverable:

E. System Enhancement Services

5.2.4.1 Software Updates and Upgrades

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 CliniComp CIS including, software updates, version changes, and upgrades at no

additional charge to the Government. The Government will cooperate with the Contractor to permit the timely and uniform installation of the then current releases as and when made available by the Contractor. To the extent that the Government unreasonably prevents, delays or impedes the timely and uniform implementation of such a software improvement, release or update, the Contractor will not be required to develop and provide any improvements, changes, patches or bug fixes for then installed software release or version, nor will the Contractor be responsible for any system or operational problems, which result during an unreasonable delay that would not have been encountered if the Government had timely permitted the installation of the then current release. Notwithstanding the preceding, the Government shall not be considered to have unreasonably delayed implementation of a proposed new release so long as (a) in the case of an enhancement release requiring user training, it permits installation within 180 days of the date the new release is made available, and (b) in all other cases, within 30 days of the date the new release is made available.

5.2.4.1.1 Updates

The updates can be 1) initiated by the Contractor to improve functionality of the CliniComp CIS, 2) in response to changes in VA/VISN enterprise needs, 3) to maintain the CliniComp CIS 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.

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:

F. Updates

5.2.4.1.2 Upgrades

Upgrades are defined as hardware, software and/or firmware changes that provide additional or improved application features and functionality to an existing system. All Software Upgrades shall be included as part of maintenance at no additional cost. If a software upgrade requires a hardware upgrade in order to provide the additional functions the hardware will be made available for purchase. With the exception of the web-based product, the Contractor is not obligated to deliver or implement any new product offering containing material new functions and features which are generally offered for purchase by the Contractor generally to its customers as new products and any such new products may be separately purchased by the Government.

Deliverable:

G. Upgrades

5.2.4.2 UPDATES AND UPGRADES TRAINING

The Contractor shall provide release notes and informational training sessions or manual updates associated with any and all updates and/or upgrades that significantly affect the use of the system the by end-users at no additional cost. In addition to such documentation, the Contractor shall make available qualified personnel remotely for reasonable quantities of consulting with the VA CliniComp vendor user group in connection with a new release containing material changes to the software usability.

Deliverable:

H. Updates and Upgrades Training

5.2.4.3 NO PLANNED ONSITE TECHNICAL SUPPORT

The Contractor shall not be required to provide staffing for continuous onsite CliniComp technical support. Onsite support is required in the event a problem cannot be reasonably resolved by remote support and shall be costed using CLIN 11 and 12.

5.2.5 INTERFACE SUPPORT

As part of the unscheduled and scheduled maintenance, the Contractor shall ensure that all CliniComp CIS side interfaces, including but not limited to VistA Imaging/CPRS, Medical Devices, analytics, CIS etc., and data transfer links are maintained consistently throughout the period of performance in accordance with the processes established as part of the implementation.

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

It is the responsibility of the Government to arrange for the necessary device vendor interface support for the medical devices interfaces. The Contractor is not responsible to make any payments to any device vendor and is not obligated to incur any licensing or other obligations or liabilities to a device vendor aside from customary mutual confidentiality commitments. In addition, the Contractor obligation to maintain or develop interfaces assumes and is conditioned on the device manufacturer's compliance with an industry recognized technical means of providing device interface capability to ensure the reliability and accuracy of the available data. Any devices requiring non-standard means of interfacing will need to be evaluated for technical feasibility and separate cost on a case-by-case basis and are not included in the initial scope of this contract.

5.2.5.1 VISTA INTERFACE SUPPORT

The integration of CliniComp CIS with VistA shall be maintained by the Contractor to ensure that the CliniComp CIS side of the interface provides for transfer of clinical and administrative data between the CliniComp CIS 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 CliniComp CIS interface with VistA meets VHA National standards. The Contractor must perform ongoing testing as DataBridge updates are/or CliniComp CIS updates are released quarterly in order to verify that the CliniComp CIS retains full functionality and integration through the DSS DataBridge to VistA.

Deliverable:

J. VistA Interface Support

5.2.5.2 ANALYTICS INTERFACE SUPPORT

The Contractor shall maintain data integrations with the analytics databases s.

The Contractor shall ensure that data is inclusive of all administrative and clinical data contained within the CliniComp CIS. The Contractor shall ensure that CliniComp CIS provide the data extracts to the analytics database(s) in the proper format. The Contractor shall coordinate with analytics Contractor(s), VA data warehouse staff, VAMC staff and the COR to validate the data being transmitted by the CliniComp CIS.

Deliverable:

K. Analytics Interface Support

5.2.5.3 REPORT TEMPLATE SHARING

All CliniComp CIS report templates 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 made available 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. The Contractor will only make available templates that are based on the VA standardized terminology and workflows, and the services do not include work to modify a template or data to accommodate terminology and workflows unique to a VISN or individual facility. In all events, the Contractor reserves all rights in the templates developed by the Contractor, including all copyrights protections, and such templates are made available to the VA pursuant to the license to each VISN.

Deliverable:

L. Report Template Sharing

5.2.6 SYSTEM TESTING

A Patch Release is intended to address urgent software problems and a Maintenance Release is intended to address non critical software problems. Neither release type introduces enhancements, nor are they intended to alter any pre-existing functionality. The Contractor will perform white box testing and quality assurance testing before installing a Patch or Maintenance Release.

The Contractor shall participate in testing of any material new upgrade/enhancement releases of the CliniComp CIS software and interfaces in accordance with the current version of the Government-approved CliniComp CIS and 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 CliniComp 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 Specifications (latest version). The Contractor shall also be responsible for validating compliance with VA data standards and terminology for the clinical data in the CliniComp CIS.

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

Contractor shall in conjunction with VA create for approval release documentation.
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 CliniComp CIS; and for testing the integrations of the CliniComp CIS with VistA/Interfaces and with any data extraction or transfer.

Deliverable:

M. 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 agreement and any subsequent orders.

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the purchase order or contract.

Deliverable:

N. Mandatory Check In/Out and Removable Media Scanning

5.2.8 RESPONSE TIME

The Contractor shall provide the 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 and diligently to rectify the problem without undue delay without any additional cost to the government. The contractor shall be responsible to coordinate the method of response with the COR as designated on each order.

Urgent priority is defined as any issue that affects patient safety, regulatory compliance, and/or CliniComp CIS side interfaces which affect life and/or property. Urgent priority applies when malfunction or failure can result in patient injury or death or significant damage to equipment. This includes any issue that adversely impacts patient care. Examples include partial or complete system outages, interruptions making a critical functionality inaccessible, interruptions causing a severe impact on application availability, or data corruption resulting in missing or incorrect patient information, duplicate records, loss of data, etc. Urgent priority requires immediate action by the Contractor.

High priority is defined as having a potential to affect patient care such as degradation in performance or functionality, work flow interruptions or delays, etc. High priority warrants special attention and takes precedence over normal and low priorities. Examples include interruption to critical functionality, access denied to data and systems, sustained degraded or unusable capabilities, not life threatening but having a potential for impact on services availability if not resolved. High priority also requires immediate action by the Contractor in order to minimize risk of becoming an urgent priority event.

Normal priority is defined as a defect or fault event but the system is operable with no impact to patient care. Normal priority requires same day initial action but resolution may take more time. Examples include impairment of non-critical functions or procedures, capabilities that have become unusable or hard to use but with no direct impact on patient care services or system availability. Normal priorities will typically have a workaround available. Normal priorities take precedence over low priorities.

Low priority is defined as preventive maintenance or issues that do not require immediate action or attention.

Table 1 list response times by priority types as defined by VA. The Contractor shall meet the response time requirements associated with each priority:

Priority	Call Back Response	Remote-Log In Response	Anticipated Turn Around Time (to restore to full performance)
Urgent	**1 hour**	**1 hour**	**8 hours**
High	**2 hours**	**2 hours**	**16 hours**
Normal	**2 hours**	**8 hours**	**40 hours**
Low	**4 hours**	**10 hours**	**48 hours**

TABLE 1

If full performance cannot be restored within the above anticipated timelines, an on-site response may be required as agreed upon by VA and the Contractor. . A failure to meet the anticipated timelines will not be a default so long as the Contractor uses the requisite level of effort required for the applicable problem priority. Full performance means that all defective software, hardware, and / or parts have been repaired or replaced with equivalent to or better than the original manufacturer's parts that replacement meets original performance specifications. Except in the case of Urgent priority problems, such Response Times shall apply only during normal business hours (i.e. Monday through Friday from 7:00 a.m. to 6:00 p.m. Pacific Time, excluding Federal holidays) and in the case of service requests received outside of the normal hours, the start times shall be measured from the beginning of normal business hours for next business day. In the case of Urgent or High priority problems, the Contractor will use its commercially reasonable best efforts and proceed diligently and on a substantially continuous basis to resolve the problem so that the system is restored to an operational condition and available for its intended use as soon as technically feasible. In the case of normal or low priority problems, the Contractor will proceed during normal business hours in a reasonable manner to resolve the problem within a reasonable time. The Contractor may reduce the severity level of a problem by implementing reasonable work-arounds to mitigate or eliminate the problem subject to the COR's reasonable approval of such work-around.

Deliverable:

O. Response Time

5.2.9 SYSTEM UPTIME

The system uptime shall be operable and available for use at least 98.9% of the time, 24/7/365. Downtime will be computed from notification of problem. Scheduled maintenance will be excluded from downtime during normal working hours as detailed herein. Operational Uptime will be computed during a month long time period. Repeated failure to meet this requirement can subject the Contractor to Termination for Default action. "Downtime" means periods when the malfunctions of hardware or software supplied by the Contractor that render the central production system unavailable for its intended use.

Deliverable:

P. System Uptime

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 CliniComp CIS 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 CliniComp CIS 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 CliniComp CIS are compliant with VA data standards in data representation and in exchange of data over interfaces with other systems. VA updates these standards quarterly and the Contractor shall ensure that the CliniComp CIS 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 are loaded onto the VISN Facility CliniComp CIS production servers within (30) days, and shall ensure that they are locked to preclude any change to the CliniComp CIS 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. The Contractor and VA agree to adding up to 75 database items (DBI), which may contain multiple items, per quarter.

Deliverable:

Q. Data and Terminology Standardization

5.2.10.1 INTRA-VISN DATA STANDARDIZATION

The Contractor and VA shall ensure that the CliniComp CIS systems in each VISN function and operate as part of a unified and standardized data solution for clinical and administrative data throughout the VISN. The CliniComp CIS data must be fully available across the VISN, and also integrated utilizing the current DSS interfaces 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. Data and templates for entering or accessing data have been implemented and shall be managed at the VISN-level. To the extent the VISN or any facility elects to include 3rd party-owned content in the configurations used at a site(s), the VISN or facility is responsible for obtaining the 3rd party's permission for use of such content and the Contractor's pricing does not include the cost of procuring any such rights.
Functionality is to be implemented in CliniComp CIS for individualized displayed configurations as needed to respond to unique needs in patient care delivery and management at the facility level. Upon reasonable notice, the Contractor must provide near real-time technical and clinical consultations upon requests from VA for any regulatory agency which is examining the Contractor's quality control.

CliniComp CIS 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 CliniComp CIS version for the VISN that meets its specific needs.. The VISN-level version is generally based on a National CliniComp CIS 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:

R. Intra-VISN Data Standardization

5.2.10.2 INTER-VISN DATA STANDARDIZATION

In compliance with the National CliniComp CIS, the Contractor shall provide maintenance services for the VISN current software and any versions' upgrade of its CliniComp CIS to all VISNs at no additional costs. In addition, reports and/or enhanced reporting tools purchased by any individual VISNs for use shall be made available to all VA VISNs utilizing CliniComp CIS.

The national version of the CliniComp CIS 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 provide all subsequent, future versions of the CliniComp CIS software/build at no additional cost. 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 requirement for the standardized National CliniComp CIS Version, the VA Change Control Board includes participation from VA representatives, as well as representative of and also participation of the Contractors for interfaces and the analytics. The Contractor shall ensure that all software updates are coordinated and 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 User Group that will address CliniComp CIS configuration changes proposed by the Contractor or the VA User Group.

The Contractor shall ensure proper functionality and operation of the CliniComp CIS at each facility by complying with VA standardized data principals. The Contractor shall coordinate changes to the CliniComp CIS data elements and standards, and interfaces with the COR under VA Change Management. The Contractor shall provide all CliniComp CIS updates with all VISNs on contract, including VAMCs, at no additional cost to VA thereby achieving standardization goals within the National User Group.

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. In all events, the Contractor shall be entitled to rely on such VA Change Control Board approvals and the Contractor is not required to independently obtain approval from each VISN.

Deliverable:

S. Inter-VISN Data Standardization

5.2.11 CHANGE MANAGEMENT AND CONFIGURATION CONTROL

Change management refers to the managing of any event that alters, or has the potential to alter, the existing state of VISNs Test or Production systems, at any facility, including software, hardware, networks and facilities. Proper functionality and operation of the CliniComp CIS at VISNs involve VA standardized data and interfaces with other systems. If maintenance and support requires, or will result in, any changes to the system software or hardware, the Contractor shall ensure that the same software components and hardware components are in place at each facility to the extent compatible with software or hardware components not changed, in order to ensure that any such change is consistent with a goal of achieving a total standardized integrated system to the extent feasible.

To facilitate the requirement for a national CliniComp CIS version, the Government established a Change Management process. The process includes participation from Government representatives, as well as the CliniComp CIS Contractor and third party interface Contractors. This process ensures that all software updates are coordinated among software providers. Software updates must be tested in non-clinical environments before making them available to all VISNs.

The Contractor shall participate in a Government-led CliniComp CIS Change Management Board and National User Group that shall address any proposed CliniComp CIS configuration changes. CliniComp CIS User Group meetings address CliniComp CIS configuration changes proposed by the Contractor or changes that are necessitated by interface changes proposed by the VA National User Group responsible for various components of the system or by Government standards changes. Participation may include telephone conference calls, online live meetings and, if necessary, face to face meetings. The Contractor shall coordinate scheduling of all system changes with the appropriate representatives at each VISN

Deliverable:

T. Change Management and Configuration Control

5.2.11.1 Synchronization of Product Warranty Expiration

During the performance period, VAMCs will have or may have CliniComp CIS products that were acquired under a previous or separate acquisition/contract. In the event that items not listed in CliniComp. 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 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. 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:

U. 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 an on-site service call prior to departing the VAMC or after the conclusion of remote service. In case of remote service, the Service Report may be made available via an Electronic Service Log for tracking of services. The Service Report shall document the services rendered and, when applicable, shall include equipment description, model, equipment entry (barcode) number, serial number, 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, labor and parts information.

Deliverable:

V. 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 and hardware to the COR as designated on each order.

Pursuant to the terms of the Software License identified in the original VISN Procurement Contract, the requested documentation (particularly documentation, such as user manuals, which exposes functions or features of the software) or other commercial items, are all confidential and proprietary of CliniComp. The documentation is being made available for Government purposes only. The manuals may be copied, subject, however, to the Government's obligation to protect the proprietary and confidential nature of such documentation. No hardware maintenance or support documentation is required to be furnished since no preventive maintenance for the hardware is required or intended to be performed by the VISN support personnel, and such support is included in CliniComp Intl.'s maintenances and support services. Any assistance requested from site technical personnel for replacement of any specific peripheral hardware (e.g.

Bedside UDAS box) will be performed based on specific instructions and direction from CliniComp technical personnel.

Deliverable:

W. Manuals, Release Notes, and Service Bulletins

5.2.12.3 Disaster Recovery and Failover Plan

Generally, the Annual Maintenance fixed pricing in CLIN 0001 for the basic maintenance and support services described in this SOW does not include providing services or equipment made necessary as a result of casualties or disasters of any nature, such as fire, flood, inclement weather, fire sprinkler discharge, failure of electrical power or power surges, spikes or disturbances or any other similar events or acts of God, customer misuse or abuse and other similar event or circumstances not the fault of CliniComp and not resulting from a defect or deficiency in the system itself.

The Contractor shall provide a disaster recovery plan in the event of the occurrence of general hardware or software failure, a major system outage resulting from such disasters or other causes not covered by the Contractor's basic support responsibilities. Such plan shall provide detailed information concerning the process, resources, implementation schedule and costs for restoration of the system to full capability as soon possible. Approval of the plan for implementation shall be made by modification signed by the COR under the applicable order.

CLIN 0014 provides pricing for the optional purchase by each VISN of a "Disaster Operational Continuity" feature that Contractor will make available. This critical enterprise fail-over solution consists of both hardware and software. This feature permits another CIS system server to be installed at a physically separate location from the other main production servers (This can be a secondary data center, a VAMC, or another location available via the WAN from the main server location. This "Disaster Operational Continuity" server is updated by the main production servers on a per-transaction basis. Should a catastrophic failure occur involving an entire CIS System at a site or data center (fire, flood, or other unplanned major outage) this fully redundant Disaster Operational Continuity server continues full operations of all CIS activities with all the patient data intact. The server is immediately available for use by any clinical users via remote access via the VISN's WAN. Once the main production server at the sites or data centers comes back on line, the Disaster Operational Continuity server can be used to restore the data to the affected production systems. The Disaster Operational Continuity server, like the site servers, is intended to run without any operator intervention.

Deliverable:

X. Disaster Recovery 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:

Y. Product Modification, Removal or Recall

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 CliniComp CIS during an emergency.

When any disruption of the Contractor's 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:

Z. Emergency and Continuity of Operations Plan

5.2.15 TRANSITION / ORIENTATION SUPPORT

5.2.15.1 OUTGOING TRANSITION / ORIENTATION SUPPORT

In the event the Government elects to replace the CliniComp CIS with a different technical solution, then the Contractor agrees to make available transition services at the FFP labor rates for general services in **B.2 PRICE/COST SCHEDULE** upon receipt of a mutually agreed modification task order. Such transition services shall consist of assistance to the order authority in the planning of the transition and general consultation concerning the roles, responsibilities and tasks performable by a contractor responsible for the implementation and maintenance of a ICU clinical information system, provided the Contractor shall not be required to disclose to another contractor information concerning any specific trade secret or proprietary tasks, processes, procedures or information.

Deliverable:

AA. Outgoing Transition Plan

5.2.16 TRAINING

As set forth below, the Contractor shall provide remote and on-site user training to both clinical and non-clinical staff on the use and operations of the CliniComp CIS software/hardware 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 CliniComp CIS, 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. Training for updates and upgrades will be conducted in accordance with 5.2.4.2. 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.
In accordance with the preceding, the following training will be available as Optional Items:

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.

3. Reporting Tool/Analytics User training at each individual facility.

Deliverable:

BB. Outgoing Transition/Orientation Support

6 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise mutually agreed 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 blood test.

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

TASK	DELIVERABLE ID	DELIVERABLE DESCRIPTION	DUE	FREQUENCY
A	5.1	KICKOFF MEEETING	7 DAYS AFTER	ONCE

			AGREEMENT AWARD/ AS DESIGNATED ON EACH ORDER	
B	5.2.1	TELEPHONE AND ON-LINE SUPPORT AND TECHNICAL CONSUTATION	ON-GOING	24/7/365
C	5.2.2	SCHEDULED MAINTENANCE	ON-GOING AS DESIGNATED	ON-GOING AS DESIGNATED
D	5.2.3	UNSCHEDULED MAINTENANCE	ON-GOING	24/7/365
E	5.2.4	SYSTEM ENHANCEMENT SERVICES	ON-GOING AS DESIGNATED	ON-GOING AS DESIGNATED
F	5.2.4.1.1	UPDATES	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
G	5.2.4.1.2	UPGRADES	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
H	5.2.4.2	UPDATES AND UPGRADES TRAINING	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
I	5.2.4.3	ONSITE TECHNICAL SUPPORT	N/A	N/A
J	5.2.5.1	VistA INTERFACE SUPPORT	ON-GOING AS DESIGNATED	ON-GOING AS DESIGNATED
K	5.2.5.2	ANALYTICS INTERFACE SUPPORT	AS NEEDED ON EACH	AS NEEDED ON EACH

			ORDER	ORDER
L	5.2.5.3	REPORT TEMPLATE SHARING	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
M	5.2.6	SYSTEM TESTING	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
N	5.2.7	MANDATORY CHECK IN/OUT AND REMOVABLE MEDIA SCANNING	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
O	5.2.8	RESPONSE TIME	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
P	5.2.9	SYSTEM UPTIME	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
Q	5.2.10	DATA AND TERMINOLOGY STANDARDIZATION	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
R	5.2.10.1	INTRA-VISN DATA STANDARDIZATION	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
S	5.2.10.2	INTER-VISN DATA STANDARDIZATION	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
T	5.2.11	CHANGE MANAGEMENT AND CONFIGURATION CONTROL	ON GOING AS DESIGNATED	ON GOING AS DESIGNATED
U	5.2.11.1	SYNCHRONIZATION OF PRODUCT WARRANTY EXPIRATION	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
V	5.2.12.1	SERVICE REPORTS	AS NEEDED	AS NEEDED
W	5.2.12.2	MANUALS, RELEASE NOTES AND SERVICE	AS NEEDED	AS NEEDED

		BULLETINS		
X	5.2.12.3	DISASTER RECOVER AND FAILOVER PLAN	AS NEEDED ON EACH ORDER	AS NEEDED ON EACH ORDER
Y	5.2.13	PRODUCT MODIFICATION, REMOVAL OR RECALL	WITHIN 48 HOURS	AS NEEDED
Z	5.2.14	EMERGENCY OPERATIONS	10 DAYS AFTER AGREEMENT AWARD	UPDATED AS NEEDED
AA	5.2.16	TRAINING	AS NEEDED	AS NEEDED

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 (COR):
Name: TBD per VISN 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

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.

13.0 SECTION 508 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS

The following Section 508 Requirements supersede Addendum A, Section A3 from the T4 Basic SOW.
The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

1_§ 1194.21 Software applications and operating systems
1_§ 1194.22 Web-based intranet and internet information and applications
1_§ 1194.23 Telecommunications products
1_§ 1194.24 Video and multimedia products
1_§ 1194.25 Self contained, closed products
1_§ 1194.26 Desktop and portable computers
1_§ 1194.31 Functional Performance Criteria
1_§ 1194.41 Information, Documentation, and Support

The Contractor shall use the appropriate Section 508 Standards Checklists to ensure conformance with Section 508 Standards. The Standards Checklists along with additional information are available at http://www.section508.va.gov/section508/Standards_Checklist.asp. Automated test tools and manual techniques are used in the VA compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.
The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

13. 1 EQUIVALENT FACILITATION

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

13.2 COMPATIBILITY WITH ASSISTIVE TECHNOLOGY

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

14. Security Requirements

This CliniComp CIS 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 four requirements per 38 U.S.C. §§ 5723 and 5725:

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 officer 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.

14.1 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.

14.2 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 SOW, 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.

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

The CliniComp CIS 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 CliniComp CIS 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 CliniComp CIS specific hardware and software enabling the Contractor to perform the required Upgrades, Maintenance and Technical Support.

The CliniComp CIS 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 CliniComp CIS 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 the CliniComp CIS and VA. The agreement governs the relationship between and VA including designated managerial and technical staff, in the absence of a common management authority.

14.4 NOT USED

14.5 NON-DISCLOSURE AGREEMENT

In performance of this effort, contract support personnel will be required to execute a Non-Disclosure Agreement and report any Organizational Conflict of Interest. The Contractor shall not disclosure 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. Notwithstanding the preceding provisions, the Contractor is authorized to make available patient data in compliance with the integration requirements of the SOW, for example to DSS and the analytics solution, via the interfaces and the Contractor shall not have any responsibility for any errors or omissions of third parties to whom the Contractor is directed by the VISN to provide patient information or other confidential information. 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 personal 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.

14.6 BUSINESS ASSOCIATE AGREEMENT

The contractor shall have a Business Associate Agreement (BAA) and safeguard Personal Health Information (PHI) agreements. Notwithstanding any other provision, the Contractor shall be determined to be in compliance with the requirements of this section so long as it maintains a National Business Associate Agreement **(**BAA) with the Veterans Health Administration (VHA) in compliance with a VISN Procurement Contract.

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).

14.7 VA INFORMATION CUSTODIAL LANGUAGE

Confidential and sensitive 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. This clause expressly limits the contractor/subcontractor's rights to use patient data as described in Rights in Data - General, FAR 52.227-14(d) (1).

VA confidential or sensitive information should not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to 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 it is determined 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 VA 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 and for a protective order excusing or limiting any legal obligation of the Contractor to makes such records available.

14.8 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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 provide for 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 applies to security fixes which may be necessary to correct and bring into compliance all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems, provided, if additional or upgraded hardware is required to avoid or mitigate any potential impact, a cost modification will be necessary.
The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than five days. In the event additional time is needed to test and install the patch, the Contractor will work closely with the VA to ensure it is accomplished as quickly as possible.

When the Security Fixes involve installing third party patches, the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within ten working days When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within three days. In the event additional time is needed to test and install the patch, the Contractor will work closely with the VA to ensure it is accomplished as quickly as possible.

All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g.

for the convenience of VA) shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology or authorized representative.

14.9 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 CliniComp CIS 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.

14.10 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.

14.11 LIQUIDATED DAMAGES FOR DATA BREACH

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

The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

1. Nature of the event (loss, theft, unauthorized access);
2. Description of the event, including:
   (a) Date of occurrence;

(b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3. Number of individuals affected or potentially affected;
4. Names of individuals or groups affected or potentially affected;
5. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
6. Amount of time the data has been out of VA control;
7. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
8. Known misuses of data containing sensitive personal information, if any;
9. Assessment of the potential harm to the affected individuals;
10. Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
11. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1. Notification;
2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3. Data breach analysis;
4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

14.12 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.

14.13 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 and/or Puerto Rico. The Contractor shall not access any VA data/information (for example, by remote computer access) from locations that are outside the above-stated borders. Furthermore, the Contractor shall not send, transfer, mail or otherwise transmit any VA data/information to locations outside the above-stated borders.

14.14 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 the TMS, the Contractor personnel shall contract the VA TMS Help Desk at vatmshelp@va.gov or at 1 (866) 496-0463.

For the initial training, the contractor shall provide the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 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.

14.14.1 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 Contactors are NOT required to manually or electronically sign a separate Rules of Behavior.

14.14.2 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.

14.14.3 SECURITY TRAINING COURSES

14.14.3.1 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.

14.14.3.2 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.

14.14.3.3 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.

14.14.4 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.

14.15 BACKGROUND INVESTIGATIONS

14.15.1 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 back ground 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.

14.15.2 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 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

14.15.3 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.

14.15.4 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.).

14.15.4.1 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.

14.15.5 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 or Personnel Management (OPM). The VSC will submit the investigation request to the SIC simultaneously and keep tabs on the SIC status for a submitted investigation. Once the investigation is completed, all issues identified as unfavorable will be addressed with the contractor employee at that time. A determination can then be made and forwarded to OPM.

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

14.15.6 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.

14.15.6 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.

14.16 POSITION / TASK RISK DESTINATION LEVEL(S)

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

The position sensitivity for this any orders under this agreement is LOW and the level of background investigation is National Agency Check with Written Inquiries (NACI)..

14.17 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 performing services under the contract. 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)