



PRODUCT DESCRIPTION TEMPLATE

**DEPARTMENT OF VETERANS AFFAIRS
Office of Healthcare Technology Management**

VISN 10 Cardiac Catheterization Lab Supply Management

Date: 09/21/2017

TAC-18-43942

Product Description Version Number: 1.7

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

PRODUCT DESCRIPTION

In Veterans Integrated Service Network (VISN) 10, the Cardiac Catheterization Labs (CCL) uses a Real-Time Location System (RTLS) solution to allow for tracking of primary and secondary inventory. Supply tracking is accomplished by the use of smart cabinets and Radio Frequency Identification (RFID) tags that are associated with catheters and other items in the cabinet. The system also tracks par levels and will provide lists of inventory items that need to be ordered. Those orders can then be placed in the VA's Generic Inventory Package (GIP) system. CCL RTLS also gives the ability to create reports detailing lost inventory, expired inventory, and other metrics of interest.

The Veterans Health Administration (VHA) requires software maintenance for WaveMark EiRTLS, WaveMark GIP interface, and the WaveMark Barcode Module as well as hardware maintenance on their existing WaveMark RTLS cabinets for VISN 10. VHA also requires software licensing and maintenance for WaveMark EiRTLS, WaveMark GIP interface, and the WaveMark Barcode Module in addition to hardware and maintenance.

VISN 10 sites are listed below:

- a. Cincinnati: 3200 Vine St, Cincinnati, OH 45220
- b. Cleveland: 10701 East Boulevard Cleveland, OH 44106
- c. Dayton: 4100 W 3rd St, Dayton, OH 45428
- d. Ann Arbor: 2215 Fuller Rd, Ann Arbor, MI 48105
- e. Detroit: 4646 John R St, Detroit, MI 48201
- f. Indianapolis: 1481 W 10th St, Indianapolis, IN 46202

A comprehensive overview of the performance, hardware, software, and maintenance requirements for all sites can be found section 1.0 Requirements

The Period of Performance (PoP) for this effort is 12 months.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

1.0 REQUIREMENTS

Table 1: Performance Requirements

Facility	Requirement Type	Details
All VISN 10 Sites	Functionality - GIP	Increased Inventory Update Frequency
All VISN 10 Sites	Monitoring - Full System	System Monitoring for all VISN 10 Cardiac Cath Lab RTLS Solutions
All VISN 10 Sites	Functionality - GIP	Immediate GIP updates upon addition of asset information into WaveMark

Table 2: Software and Maintenance Requirements – See Appendices A (Devices Ann Arbor Healthcare System VA), B (Devices Indianapolis VA – Richard L) and C (Devices Detroit VA – John D. Dingell VA Medical Center) for lists of the devices requiring maintenance.

Facility	Requirement Type	Details
Ann Arbor, Cincinnati, Cleveland, Dayton, Detroit, Indianapolis	WaveMark Hardware Maintenance	Hardware Maintenance for WaveMark RTLS Cabinets
Ann Arbor, Cincinnati, Cleveland, Dayton, Detroit, Indianapolis	WaveMark EiRTLS Software Maintenance	Maintenance for User Interface
Ann Arbor, Cincinnati, Cleveland, Dayton, Detroit, Indianapolis	WaveMark Interface Software Maintenance	Maintenance for Interfaces
Ann Arbor, Cincinnati, Cleveland, Dayton, Detroit, Indianapolis	WaveMark Barcode Module Software Maintenance	Maintenance for "Loaner" Module
Ann Arbor, Cincinnati, Cleveland, Dayton, Detroit, Indianapolis	Support Services See Appendix D – Software and Hardware Maintenance and Support Description	WaveMark Level 2 Support
Cincinnati, Cleveland, Dayton	WaveMark EiRTLS Software License	One Time License Fee for User Interface

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

Cincinnati, Cleveland, Dayton	WaveMark GIP Interface License	One Time License Fee for GIP connector
Cincinnati, Cleveland, Dayton	WaveMark EIRTLs Vista Patient Interface License	One Time License Fee for Vista Patient File Connector
Cincinnati, Cleveland, Dayton	WaveMark EIRTLs Vista Employee Interface License	One Time License Fee for Vista Employee Connector
Cincinnati, Cleveland, Dayton	WaveMark CART-CL Interface License	One Time License Fee for Cart-CL Connector
Cincinnati, Cleveland, Dayton	WaveMark Barcode Module Software License	One Time License Fee for Barcode Module

Table 3: Hardware Requirements

Facility	Quantity	Product #	Description
Cincinnati, OH	12	HF1500DM-CE	5 Shelf Cabinet, Manual Doors
Cincinnati, OH	9	HFC1500DM-SHBBBS-CE	Cabinet, Hanging with Upper Shelf, Manual Doors
Cincinnati, OH	3	HFH1500DM-CE	Cabinet, Hanging Products, Manual Doors
Cincinnati, OH	4	XPOS2-USB-BTV-CE	XPOS2 Station USB (White)
Cincinnati, OH	2	TM-STATION-TAA	Tagging Station with VA Laptop
Cincinnati, OH	1	ACC-HANGSEPARATOR	Hanging Product Divider for HFH
Cincinnati, OH	8	TAG-SQ-CAH-CET	Tags - Square (2000)
Cincinnati, OH	4	TAG-SPINE-CAH-CAT	Tags - Spine (1000)
Cincinnati, OH	20	TAG-HANGM-CET	Tags - Hanging (100)
Cincinnati, OH	10	TAG-POUCH-CET	Tags - Foil Pouch (25)
Cleveland, OH	5	HF1500-CE	5 Shelf Cabinet
Cleveland, OH	4	HF1500DM-CE	5 Shelf Cabinet, Manual Doors
Cleveland, OH	3	HFC1500-SHBBBS-CE	Cabinet, Hanging, with Upper Shelf
Cleveland, OH	5	HFC1500DM-SHBBBS-CE	Cabinet, Hanging with Upper Shelf, Manual Doors
Cleveland, OH	1	HFH1500-CE	Cabinet, Hanging Products
Cleveland, OH	1	HFH1500DM-CE	Cabinet, Hanging Products, Manual Doors
Cleveland, OH	2	XPOS2-USB-BTV-CE	XPOS2 Station USB (White)
Cleveland, OH	2	TM-STATION-TAA	Tagging Station with VA Laptop
Cleveland, OH	2	90-0102-R	Laptop, VA Compatible
Cleveland, OH	9	ACC-COVER-HF	HF/HFH Cover
Cleveland, OH	2	ACC-HANGSEPARATOR	Hanging Product Divider for HFH
Cleveland, OH	8	TAG-SQ-CAH-CET	Tags - Square (2000)
Cleveland, OH	4	TAG-SPINE-CAH-CAT	Tags - Spine (1000)

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

Cleveland, OH	15	TAG-HANGM-CET	Tags - Hanging (100)
Cleveland, OH	4	TAG-POUCH-CET	Tags - Foil Pouch (25)
Dayton, OH	2	HF1500-CE	5 Shelf Cabinet
Dayton, OH	2	HF1500DM-CE	5 Shelf Cabinet, Manual Doors
Dayton, OH	1	HFC1500DM-SHBBBS-CE	Cabinet, Hanging with Upper Shelf, Manual Doors
Dayton, OH	1	HFH1500DM-CE	Cabinet, Hanging Products, Manual Doors
Dayton, OH	1	XPOS2-USB-BTV-CE	XPOS2 Station USB (White)
Dayton, OH	1	TM-STATION-TAA	Tagging Station with VA Laptop
Dayton, OH	2	ACC- COVER-HF	HF/ HFH Cover
Dayton, OH	1	ACC-HANGSEPARATOR	Hanging Product Divider for HFH
Dayton, OH	3	TAG-SQ-CAH-CET	Tags - Square (2000)
Dayton, OH	2	TAG-SPINE-CAH-CAT	Tags - Spine (1000)
Dayton, OH	3	TAG-HANGM-CET	Tags - Hanging (100)
Dayton, OH	8	TAG-POUCH-CET	Tags - Foil Pouch (25)

1.1 Hardware Acceptance Requirements

Hardware shall be delivered to the Ohio sites within 60 days after award. The schedule for delivery shall be determined upon award. The Contractor shall install the delivered WaveMark Cardiac Catheterization Lab Supply Management hardware and shall upstart the system and demonstrate the full functionality of the WaveMark hardware and software and its data connections to GIP and CART-CL. During upstart, the facility RTLS point of contact (Dayton: Kevin Hutcherson, Cleveland: Dale Wood, Cincinnati: Shane Thompson) shall be present and the VISN 10 RTLS office shall be notified of the date and time of the activities. All installations and deliveries shall occur outside of normal operating hours, normal operating hours are 7 am – 5 pm. These activities shall include the following:

- 1) The Contractor shall tag all CCL assets in supply at Cincinnati, Cleveland, and Dayton sites and demonstrate for the staff in logistics, nursing, and engineering the process to associate a tag to a new asset in the WaveMark system.
- 2) The Contractor shall give informal instruction staff in logistics, nursing, and engineering regarding how to operate and interact with its hardware and software system. The material to be presented in shall be submitted to the VISN 10 RTLS office two weeks prior to delivery for review and approval. These sessions shall be informal hands on training for 3-7 personnel with the system within 1 week of installation.
- 3) The Contractor shall demonstrate the connection between GIP, WaveMark, and CART-CL by means of a Trial Case. Successful connections shall be

**VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942**

documented and provided in the Trial Case Report.

Deliverable:

A. Trial Case Report

2.0 SECTION 508

NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL ELECTRONIC AND INFORMATION TECHNOLOGY PROCUREMENTS

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

2.1. Section 508 – Electronic and Information Technology (EIT) Standards:

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:

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

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

2.2. 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.

2.3. 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.

2.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at <http://www.section508.va.gov/section508/Resources.asp>.

3.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, FEMP designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at www.femp.energy.gov/procurement. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products.
4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

4.0 WINDOWS OS PC-LAPTOP ACCEPTANCE TESTING:

The Contractor shall provide all PCs or laptops or both PCs and laptops to be delivered under this contract without an operating system. The Contractor shall provide PCs or

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

laptops or both PCs and laptops for pre-production testing.

Within ten (10) business days after contract award the Contractor shall furnish, at no additional cost to VA (this cost shall be part of the overall unit price of the PCs or laptops or both PCs and laptops), the Windows OS PCs or laptops or both PCs and laptops under contract (one of each configuration) software and licenses. The software shall include all hardware drivers and shall be delivered either via disk or via download from a website. Delivery or provision of the download address shall be made to the VA Pre-Production Test Facility at 113 Holland Avenue, OIFO D417, ATTN: Kevin Overholt, Albany, NY 12208 (or other pre-production test facility address as specified in the order).

The VA Pre-Production Test Facility will test the PCs or laptops or both PCs and laptops to ensure that it functions correctly within the current VA IT infrastructure. Regression testing must be performed involving VA application software and paying special attention to the encryption product listed at <http://vawww.eie.va.gov/SysDesign/CS/Shared%20Documents/Standards/Software%20Configuration.xlsx> to ensure that the VA-specific hard drive image is functioning correctly.

VA must complete pre-production testing (a minimum of thirty (30) days is required) before PCs or laptops or both PCs and laptops can be delivered.

1. Upon completion of successful pre-production testing, the Contracting Officer shall notify the Contractor. Accepted PCs or laptops or both PCs and laptops that pass pre-production testing will not be returned to the Contractor.
2. If the equipment provided fails to pass pre-production testing, VA will return the failed equipment to the Contractor or designated manufacturer point of contact, solely at the Contractor's cost, and the Contractor shall provide new PCs or laptops or both PCs and laptops to the designated VA Pre-Production Test Facility.
3. The Contractor shall assist VA staff as needed to address any questions and/or problems encountered during the testing process.

As part of the Gold imaging process, for all PCs or laptops or both PCs and laptops, the Contractor shall set the PC BIOS to PXE as the first boot option and set the hard drive controller to AHCI (no RAID enabled). VA reserves the right to have the Contractor change these settings before any deliveries. Accepted computers must support SCCM-deployed OSD (pre-OEM) images currently delivering the hard drive as blank (no operating system) including proactive driver management driver packs that are small and optimized for SCCM OSD specifically The PC or laptop shall support multiple image file formats including .wim, the main file format used by VA.

5.0 SHIPMENT OF HARDWARE OR EQUIPMENT

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

Inspection: Destination

Acceptance: Destination

Free on Board (FOB): Destination

Ship To and Mark For:

Primary:

Name: _____
Address: _____
Voice: _____
Email: _____

Alternate:

Name: _____
Address: _____
Voice: _____
Email: _____

5.1. Special Shipping Instructions

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

Contractors must coordinate deliveries with Site POCs before shipment of hardware to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall 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 will indicate total number of containers for the complete shipment (ex. "Package 1 of 2"), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall include the following:

IFCAP PO # _____ (e.g., 166-E11234. The IFCAP PO number is located in block #20 of the SF 1449.)

Project Description: (e.g., Tier I Lifecycle Refresh)

Total number of Containers: Package ____ of _____. (e.g., Package 1 of 3)

INFORMATION SECURITY CONSIDERATIONS:

The Assessment and Authorization (A&A) requirements do not apply and a Security Accreditation Package is not required.

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

all systems/LAN's accessed while performing the tasks detailed in this Product Description.

- a. 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 contractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA." See VA handbook 6500.6, Appendix C, paragraph 3.a.
- b. A requirement for data breach notification: Upon discovery 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, 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 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. A requirement to pay liquidated damages in the event of a data breach: "In the event of a data breach or privacy incident involving SPI the contractor processes or maintains under this contract, the contractor shall be liable to VA for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals." See VA handbook 6500.6, Appendix C, paragraph 7.a., 7.d.
- d. A 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 security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA's security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the contractor. If the contractor provides their own training that conforms to VA's requirements, they will provide the COR or CO, a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in the VA's contract have received their annual security/privacy training that meets VA's requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9.
- e. A 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 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." See VA Handbook 6500.6, Appendix C, paragraph 9, Appendix D. Note: If a medical device vendor anticipates that the services under the contract will be performed by 10 or more individuals, the

**VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942**

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.

**ADDENDUM B- VA INFORMATION AND INFORMATION SYSTEM SECURITY /
PRIVACY LANGUAGE**

**VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY
LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010**

B.1 GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B.2 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B.3 VA INFORMATION CUSTODIAL LANGUAGE

a. 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 data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling 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 conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, Contractor/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 the VA Contracting Officer within 30 days of termination of the contract.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

d. 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.

e. 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.

f. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. 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.

i. 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.

j. 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.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

k. 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.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B.4 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the *TIC Reference Architecture*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*.

b. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

c. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

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

e. 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, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

f. 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.

g. The Contractor/Subcontractor agrees to:

1) 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:

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the Contractor/Subcontractor is to perform;

2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

3) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

h. 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

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

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.

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

j. 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, based upon the severity of the incident.

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

l. 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.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

B.5 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP)

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and Interconnection Security Agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The Contractor/Subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

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 A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. 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, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. 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. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
 - (a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
 - (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 preapproved and described in the purchase order or contract.
 - (c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B.6 SECURITY INCIDENT INVESTIGATION

- a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/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.
- b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/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.

B.7 LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b. 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.

c. 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:

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

- (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 Breaches Involving Sensitive Personal Information*, 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.
- d. 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

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

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

B.8 SECURITY CONTROLS COMPLIANCE TESTING

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

B.9 TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - 1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and annually complete this required privacy and security training; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.
 - 2) Successfully complete the appropriate VA Privacy training and annually complete required privacy training;
 - 3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*
- b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

- c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

VISN 10 Cardiac Catheterization Lab Supply Management
TAC Number: TAC-18-43942

POINT(S) OF CONTACT:

VA Program Manager

Name: Ryan Knight
Address: 11500 Northlake Drive
Suite 200
Cincinnati, OH 45249
Voice: (513) 247-4288
Email: ryan.knight@va.gov

Contracting Officer

Name: Lino Vera
Address: Technology Acquisition Center - Austin
1701 Director's Blvd., Suite 600
Austin, Texas 78744
Voice: (512) 831-9664
Email: lino.vera@va.gov

**Contracting Officer's
Representative**

Name: John Michael
Address: 11500 Northlake Drive
Suite 200
Cincinnati, OH 45249
Voice: (513) 906-0071
Email: john.michael5@va.gov