



PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

Real-Time Location Systems

September 13, 2013

PWS Version Number: 2.2

Contents

Contents	2
1.1 Veterans Health Administration	7
2.0 RTLS SCOPE OF WORK.....	8
2.1 General.....	8
2.2 RTLS Capability.....	9
2.2.1Asset (Item) Tracking Capability	9
2.2.2SPD Workflow Automation Capability	10
2.2.3Inventory Management Capability	10
2.2.4Automated Temperature Monitoring Capability	11
2.2.5Business Process Workflow	11
2.2.6National Data Repository	11
3.0 APPLICABLE DOCUMENTS	12
4.0 GENERAL REQUIREMENTS.....	15
4.1 Contract Type	15
4.2 Performance Period.....	15
4.3 Place of Performance	15
4.4 Travel	15
4.5 Method and Distribution of Deliverables	15
4.6 Facility/Resource Provisions	15
4.7 Materials, Equipment and Facilities	16
4.7.1Government-Furnished	16
4.7.2Contractor-Furnished	16
4.7.3Non-Developmental Items and Commercial Processes	16
4.7.4Connectivity.....	17
4.7.5Marking, Handling, Storage, Preservation, Packaging, & Shipping.....	17
4.8 Section 508 Requirements	17
4.9 Safety and Environmental	17
4.10 Enterprise and IT Framework	18
4.11 Transition and Orientation Support at end of Contract	19
5.0 SPECIFIC REQUIREMENTS, TASKS, AND DELIVERABLES	19
5.1 RTLS System Architecture, Development and Implementation	19
5.1.1Architecture Design Considerations	20
5.1.2Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP)	22
5.1.3Disaster Recovery Specifications	22
5.2 Operating Environment.....	23
5.2.1PC Client.....	23
5.2.1.1 Non-PC Client (tablets, smart phones).....	23
5.2.2System Software	23
5.3 Software	23

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

5.3.1Application Capabilities	23
5.3.2Alerting	26
5.3.3Process Management	28
5.3.4Data Management.....	29
5.3.5Virus and Attack Protection	30
5.3.6Role Based System Access	31
5.3.7RTLS Software Capability for Large Wall-Mounted Monitors	32
5.4 RTLS Hardware Acquisition and Delivery	32
5.4.1RTLS Tags	32
5.4.2RTLS Readers/ Interrogators Reader and Device Management.....	36
5.4.3RTLS Display Monitors	37
5.4.4 Passive Tag Printers	37
5.4.5 Smart Cabinets	37
5.5 System Administration.....	37
5.6 Data Interfaces and Standards	38
5.6.1General Interface Requirements for RTLS	38
5.6.2VA Application Interfaces	39
5.6.3Mobile Device Application Interfaces	39
5.6.4Miscellaneous Hardware Interfaces	40
5.6.5Communication Interfaces	40
5.7 Database Design, Standardization and Management	40
5.7.1RTLS Databases.....	40
5.7.2National Data Repository (NDR)	41
5.8 Installation / Configuration / Acceptance	42
5.8.1Pre-Installation site assessment.....	42
5.8.2Site Assessment	43
5.8.3RTLS and National Data Repository Customization.....	44
5.8.4Installation	44
5.8.5Acceptance	46
5.8.6Standards.....	47
5.9 Documentation and Training	49
5.9.1Reference Documentation	49
5.9.2Training	50
5.10 Support and Maintenance of RTLS	51
5.10.1 Help Desk	51
5.10.2 Technical Engineering Services and Products.....	53
5.10.3 Service Level Agreements	53
5.10.4 Maintenance (Warranty and after Warranty)	53
5.10.4.1Warranty.....	54
5.10.4.2 Service Contract	54
5.11 Project Management	55
5.11.1 Implementation Manager	55
5.11.2 Project Management Plan.....	55
5.12 Contract Management	56
5.12.1 Government Support.....	56
5.12.2 Contractor Support.....	56

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

5.12.3 Government Rights	57
5.13 Technology Refresh	57
5.14 Technology Insertion	58
5.15 Engineering Change Proposals (ECP)	58
5.16 Certification and Accreditation	60
6.0 REPORTING REQUIREMENTS	61
6.1 Monthly Contract Status Report.....	61
6.2 Status of GFE Report	62
6.3 Personnel Contractor Manpower Report	62
6.4 Monthly Equipment and Service Report	63
6.5 Warranty Status Report	64
6.6 Small Business Participation Report.....	64
6.7 MEETINGS AND REVIEWS	65
6.7.1Post Award Conferences	65
6.7.2Task Order Kickoff Meetings	65
6.7.3Project Progress Reviews	65
6.7.4Organizational Chart.....	65
7.0 SECURITY	66
7.1 Systems Security	66
7.2 Personnel Security	66
7.2.1Position Risk Level and Contractor Personnel Security Requirements	66
7.2.2Security Requirements	68
7.2.3Organizational Conflict of Interest	70
ADDENDUM A	71
ADDENDUM B	76
ADDENDUM C	87
ADDENDUM D	91
ATTACHMENT A: RTLS USE CASES	92
1.0 VHA SPECIFIC USE CASES	92
1.1 Cardiac Catheterization Lab Supplies Use Case	93
1.1.1Consumables Tracking	93
1.1.2Environment Workflow Enhancement	95
1.2 SPD Workflow Use Case	96
1.3 Asset Management Workflow Use Case	100
1.4 Temperature and Humidity Monitoring Use Case	104
1.5 Patient Elopement Use Case	105
1.6 Hand Washing Use Case	107
1.7 Emergency Department Work-Flow Use Case.....	108
1.8 Surgical Work Flow Use Case.....	110
ATTACHMENT B: WIFI TECHNICAL PERFORMANCE PARAMETERS SUMMARY	113

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

ATTACHMENT C: RTLS INTERFACES TO VA SYSTEMS	116
ATTACHMENT D: VHA VISN RTLS SITE INFORMATION	117
ATTACHMENT E: Non Disclosure Agreement.....	117

1.0 BACKGROUND

The Health Care Efficiency (HCE) Major Transformation Initiative is one of the Department of Veterans Affairs (VA) Secretary's key initiatives. The goal of the HCE initiative is to reduce operational costs and create more streamlined operations in targeted program areas to enhance program efficiency across the VA enterprise.

Under the HCE initiative, the Facility Automation sub-initiative identified areas where VA currently uses manual processes (or lacks processes) for tracking and monitoring, and established the requirement to automate those areas using Real-Time Location Systems (RTLS). RTLS is an umbrella term that includes multiple technologies for locating and tracking items. It includes Wi-Fi based location finding, active and passive Radio Frequency Identification (RFID), and a number of other location technologies, including ultrasound and infrared.

The potential uses and benefits of this technology throughout VA are significant, and include improvement of quality of patient care, improved patient satisfaction, reduction of health care asset management costs, improvement of capacity/resource planning, improvement of employee and patient safety, as well as improvement of general asset management and inventory. Currently, a handful of VHA facilities utilize components of RTLS to accomplish niche applications. Data from industry, private sector RTLS users, and current VA RTLS users promises a substantial return on investment through the adoption of this technology.

As a part of the VA RTLS program, VA initiated a small number of technology demonstrations to evaluate various RTLS technologies and use cases in actual service throughout the Department. During these demonstrations VA used defined and documented success criteria and measurement methods for both business processes and technology outcomes. Although VA will evaluate a variety of technologies in the demonstrations, not all will be selected for enterprise deployment. Technologies and tools that are not selected may have opportunity for re-consideration in the future through VA's Innovation process. Ongoing evaluation and insertion of new RTLS technologies will be managed nationally, in accordance with this acquisition.

VA requires a turnkey integrated, enterprise RTLS solution. The RTLS solution is composed of two major components - the RTLS "Front-End" and the National Data Repository (NDR). The RTLS Front-End is the combination of tags (active and/or passive), the databases located at each deployment site that collect the data from the tags, and a Graphical User Interface (GUI) software application that allows users to interact with the RTLS data. The NDR is a method of aggregating data from all individual VA RTLS databases, to a central national database, to enable an enterprise-wide view of the RTLS data, as well as use of predictive analytic tools and business intelligence tools on an enterprise basis. The purpose of the RTLS solution is to improve the efficiency of targeted business processes in its hospitals, clinics, offices and cemeteries to support the missions of VHA and other VA entities.

1.1 Veterans Health Administration

VHA is comprised of 21 Veterans Integrated Service Networks (VISNs) that are each responsible for managing health care activities within their geographic area. A VISN generally includes six to ten medical facilities and a number of supporting outpatient facilities. (Details can be found at http://www.va.gov/directory/guide/division_flash.asp?dnum=1). VA Medical Centers (VAMCs) within a VISN work together to provide efficient, accessible health care to Veterans in their areas. With 152 VAMCs nationwide, VHA manages one of the largest health care systems in the United States.

In addition to the 21 VISNs, there are also seven Consolidated Mail Outpatient Pharmacy (CMOP) facilities located at Leavenworth, KS; Tucson, AZ; Chelmsford, MA; Dallas, TX; Murfreesboro, TN; Hines, IL; and Charleston, SC. When combined, these CMOPs process more than 110 million prescriptions annually.

VHA facilities are responsible to account for all property. VHA currently employs asset-tracking tools that incorporate bar coding technology with unique inventory locator numbers assigned to individual assets as they are deployed at VHA sites. Data about these assets, including equipment maintenance records, are managed by software called Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS) which is a module of Veterans Health Information Systems and Technology Architecture (VistA). While these tools allow for identification of the assets and associated data maintenance, locating the assets in the facility is accomplished manually. Inventory management in medical facilities often demands special tracking, for example, devices requiring sterilization for reuse and specimens that must be stored under specific climate conditions. Care delivery and process flows can be improved upon through the use of real-time data and back-end analytics that track the location and movement of hospital staff and patients.

1.2 Objectives

The overall program objectives of the enterprise RTLS solution are:

- NDR: Deploy a single instance of a NDR solution, for aggregation and in-depth analysis of data from individual “front-end” RTLS instances.
- Establish a capability that is compatible and interoperable with existing information systems internal and external to VA. Ensure integration, scalability and ease of sustainment across technologies.
- Enterprise Implementation: Deploy the set of nationally standardized RTLS solutions to:
 - VHA Medical Centers, Clinics, non-patient care locations
 - Other VA entities to be identified at the Task Order (TO) level
- Improve operational efficiency and the quality of Veteran care
- Decrease operational costs
- Maximize equipment utilization
- Increase efficiencies and staff productivity
- Reduce delays and improve patient care

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- Minimize lost and misplaced items
- Improve customer and staff satisfaction
- Improve the quality and safety of service from patient, physician, and institution perspectives
- Provide medical centers and other VA facilities with the real-time capability to actively track selected assets, significant medical supplies, staff, patients, and environmental conditions (e.g., temperature and humidity) through a common interface and reporting tool.

2.0 RTLS SCOPE OF WORK

This Performance Work Statement (PWS) establishes the requirements for an Indefinite-Delivery/Indefinite-Quantity (IDIQ) contract for Contractor-provided solutions in support of RTLS. The Contractor shall provide VA with a total, integrated RTLS solution to include hardware, software, documentation, and incidental services to authorized VA users across the enterprise. Incidental services include training, warranty and maintenance services, and technical engineering services (TES). Hardware and software delivery and installation, as well as performance of associated training, warranty, maintenance, and documentation shall be required at continental United States (CONUS) and outside the continental United States (OCONUS) government sites in Hawaii, Puerto Rico and Manila.

RTLS, for the purposes of VA, is defined as all systems providing real-time locating services as well as related technologies (such as active and passive RFID) for the purpose of identifying, locating, and monitoring assets, supplies, and people, within and between facilities. This does not include any enhancements to the VA wireless or wired network infrastructure. VA understands that enhancements to the VA network infrastructure / wireless network are not within the scope of this contract. The Government takes ownership of this responsibility upon Contractor notifying VA of any enhancements that are required. Notification should be provided early enough in the process to allow the Government to complete any required enhancements without affecting implementation schedules. Details of the VA wireless standard are included in Attachment B of this PWS.

This PWS provides general requirements. Functional and Nonfunctional requirements for the RTLS system are captured in this PWS and in the attached Requirements Specification Document (RSD), attached in Addendum D. The Contractor shall provide the capabilities as outlined in this PWS and the RSD. Specific requirements will be defined in individual TOs, as requirements for each VA site will vary based upon size, complexity, and priorities of a given facility. These specific tasks may supplement but not replace the task requirements identified in this base PWS.

2.1 General

VA intends to use RTLS technology in applications that demand performance on a higher level than that currently available with bar code technologies. The Contractor shall provide services necessary to assess, acquire, configure, install, interface, and integrate the appropriate hardware and software to satisfy desired system capabilities

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

and functions. The Contractor shall integrate all solutions and interface with existing VA systems (referenced on Attachment C of this PWS) such as relevant modules of Vista and other VA equipment and inventory management systems. All RTLS data from a given facility must roll up into a single database, and be accessible via a single user interface.

For active tracking, the Contractor shall provide a Wi-Fi-based technology with one add-on technology (802.11 with Infrared or 802.11 with Ultrasound, as examples) for the RTLS solution. The add-on technology will be required to help VA meet location proximity goals for applications and use cases where greater location accuracy (bed/bay level as an example) is required. The goal is to ensure that one active tag per item can be deployed to meet all location proximity and accuracy goals (e.g. VA is not looking to place multiple active tags on devices for each type of technology). In addition, the VA requires that tags are standardized and consistent from one facility to the next to ensure our ability to track assets as they are transported from one location to another.

“Wi-Fi-based” means use of Wi-Fi for communication between active tags and the RTLS readers/receivers (in this case, Wi-Fi access points). Although Wi-Fi is the required “base” technology for active RTLS in VA, there may be specific locations where the use of Wi-Fi is not technically or economically feasible (e.g. a facility being leased by VA on a short-term basis.) For such locations (as determined solely by VA), Contractor shall be capable of identifying, procuring and installing the appropriate infrastructure to support a single, nationally standard alternate RTLS technology. Since VA’s primary goal in such locations is to avoid investing in permanent infrastructure, (i.e. cabling) the alternate technology provided shall be one that requires minimal or no permanent infrastructure in order to operate. Additionally, Contractor’s solution shall be capable of tracking items in outdoor spaces (such as between buildings on a VA campus).

2.2 RTLS Capability

The RTLS solution shall, at minimum, support the following initial capability areas:

2.2.1 Asset (Item) Tracking Capability

The RTLS solution shall provide VA staff with the capability to locate assets used throughout each facility; varying levels of discrimination should be offered to meet site-specific requirements from area-level discrimination to more discrete level discrimination in real time. The assets to be tracked under RTLS include hospital or other equipment, computer equipment, medical devices, surgical instruments, staff, patients, grave markers and other categories identified by the specific implementation of RTLS use cases at each facility. Exact numbers of required tags (active / passive/other) and type of tag will be defined at the TO level.

Discrimination Levels	Description
Campus or Cemetery	Multiple Buildings on an area of land belonging to a facility
Building	Free-standing structure

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

Floor	Entire level in a building
Zone	Defined area on a floor: multiple spaces
Room	Smaller unit on a floor / zone. Has defined entrance / exit point. (3 meters)
Individual Workspace	Designated area within a room or zone. Bed or Bay area. (1 meter)
Cabinet	Storage device for supplies.
Shelf	Area within a cabinet or room in the vertical plane.
Bin	Smaller defined area within a cabinet or shelf.

2.2.2 SPD Workflow Automation Capability

The RTLS solution shall enhance Sterilization, Processing and Decontamination (SPD) business processes and support SPD staff responsible for tracking, cleaning and distributing medical equipment to clinical staff throughout the medical facility by automating the tracking of tasks, instruments, and supplies.

The Contractor shall provide a monitoring solution with graphic and tabular displays of instrument and equipment location and cleaning state, throughout the workflow process. The solution shall be user friendly, hands-free (to the greatest extent possible) and support incorporation of video clips, pictures, diagrams, sketches, and/or other media presentation of individual instruments for ease of identification of components that must be disassembled for cleaning/maintenance and reassembled prior to sterilization. The display shall provide time intervals to indicate the length of time instruments sit waiting to be cleaned, providing alerts when the instruments have surpassed a user programmable dwell time threshold.

The Contractor shall provide a reporting solution that will enable determination of SPD department productivity, as well as utilization rate, and Return on Investment (ROI) for all RME, instrument sets, and individual instruments based upon generally accepted industry standard calculations. Systems redesign efforts, to include the use of time in motion studies, should be incorporated into the Contractor's proposal to standardize these processes across the VA system. The Contractor shall provide a reporting solution to measure and analyze average time period that devices of a selected classification spend at each stage of the SPD workflow as well as total SPD cycle time.

2.2.3 Inventory Management Capability

The RTLS solution shall monitor the usage of supplies and equipment necessary for patient procedures, particularly in specialty labs, such as cardiac catheterization. RTLS solutions in these areas shall provide real-time insight for designated items that are "on the shelf", used in a case, or missing. The RTLS solution shall support par-level maintenance to ensure maximum efficiency and availability of a wide range of supplies and equipment.

The Contractor shall provide a solution to track consumables, instruments, implantable devices, and medical equipment used in the Cardiac Catheterization (Cardiac Cath)

Laboratories. (VA expects to do supply management in other areas in the future.) The end goal is to implement a system that automates the inventory management process, thereby reducing the effective level of effort exerted by facility staff, enhancing the granularity of consumables tracking, and reducing the number of errors with respect to patient-consumable/implant interaction. A passive RFID tag solution shall be provided by the Contractor to be associated with and applied to selected consumables. If an item comes with a manufacturer-installed passive tag, the solution shall track this tag in the same manner as tags provided by the RTLS solution.

The solution shall have the ability to track the location of all instruments, Reusable Medical Equipment (RME), and tagged assets in order to respond to Food and Drug Administration (FDA) recalls and hazard alerts (reference vaww.recalls.ncps.med.va.gov). The solution shall be able to relate the recalled items to a list of patients who interacted with such items within the past 12 months of recall acknowledgement.

2.2.4 Automated Temperature Monitoring Capability

The RTLS solution shall provide real time temperature monitoring (e.g. refrigerated areas that store pharmaceuticals, tissues, organs, blood, food, and other items at specified temperatures). The system shall monitor and record temperatures at predetermined time intervals and immediately report any temperature anomalies based on configured thresholds.

The RTLS solution shall provide a temperature monitoring display solution that provides graphical and tabular displays of current temperature and trends for every tag in the system. The system shall have the capability of recording discrete “real time” temperatures, mean temperatures, trending, and logging of significant events such as refrigerator temperature measurements out of acceptable range. Data collection events (frequency of record) shall be set by the user for each sensor with the collected data updated in the RTLS database at user-defined times. Data will be required to be able to be maintained and accessed for a period not less than three (3) calendar years.

2.2.5 Business Process Workflow

The RTLS solution shall offer the ability to track equipment, staff and patients at VA facilities, (and the interactions thereof) with the objective of monitoring business and clinical activities, such as tracking a patient presenting to the Emergency Department from arrival to discharge, hand washing validation, and SPD processes in real time. The goal is to improve workflow through analysis of the data provided by the RTLS.

2.2.6 National Data Repository

The RTLS solution shall provide a national view (as well as more limited views) of the data stored at the facility and/or regional levels. The NDR shall house sophisticated business intelligence, predictive analytics, and reporting capabilities used for workflow analysis, as well as medical research and analysis purposes.

Throughout the remainder of the document, the RTLS will refer to RTLS tags and system components at the facility and regional levels. The NDR shall refer to the national repository of which there is expected to only be one instance nationally.

3.0 APPLICABLE DOCUMENTS

Documents referenced or germane to this PWS are listed below. The Contractor shall be guided by the information contained in the documents in performance of this PWS.

1. Federal Information Processing Standard (FIPS) 140-2. FIPS can be found at <http://www.itl.nist.gov/fipspubs/>
2. National Fire Protection Association (NFPA) 70 – National Electric Code
3. National Fire Protection Association (NFPA) 99 – Standard for Healthcare Facilities
4. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
5. Federal Information Processing Standard (FIPS) FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
6. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” June 4, 2010 (<https://voa.va.gov/> in the Security Library)
7. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
8. VA Directive 6500, “Information Security Program,” August 4, 2006 (<https://voa.va.gov/> in the Security Library)
9. VA Handbook 6500.6, “Contract Security,” March 12, 2010 (<https://voa.va.gov/> in the Security Library)
10. Technical Reference Model (TRM) (reference Contractor Library at <http://www4.va.gov/TRM/TRMHomePage.asp>)
11. EPC Global Tag Data Translation v1.4
http://www.gs1.org/sites/default/files/docs/tdt/tdt_1_4-standard-20090610.pdf
12. EPC Global UHF Class 1 Gen 2 Standard v. 1.2.0
http://www.gs1.org/sites/default/files/docs/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf
13. EPC Global Low Level Reader Protocol Standard v1.0.1
http://www.gs1.org/sites/default/files/docs/llrp/llrp_1_0_1-standard-20070813.pdf
14. EPC Global Discovery Configuration & Initialization Standard v1.0
http://www.gs1.org/sites/default/files/docs/dci/dci_1_0-standard-20090610.pdf
15. EPC Global Reader Management Standard v1.0.1
http://www.gs1.org/sites/default/files/docs/rm/rm_1_0_1-standard-20070531.pdf
16. EPC Global EPC Information Services Standard v1.0.1
http://www.gs1.org/sites/default/files/docs/epcis/epcis_1_0_1-standard-20070921.pdf

17. EPC Global Application Level Events Standard v1.1.1
http://www.gs1.org/sites/default/files/docs/ale/ale_1_1_1-standard-core-20090313.pdf
http://www.gs1.org/sites/default/files/docs/ale/ale_1_1_1-standard-XMLandSOAPbindings-20090313.pdf
18. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
19. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
20. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
21. 10 U.S.C. § 2224, "Defense Information Assurance Program"
22. Software Engineering Institute, Software Acquisition Capability Maturity Model (SA CMM) Level 2 procedures and processes
23. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
24. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
25. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
26. VA Handbook 6500, "Information Security Program," September 18, 2007
27. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
28. VA Handbook 6550, "Pre-procurement Assessment for Medical Devices",
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=361&FTYPE=2
29. National Institute Standards and Technology (NIST) Special Publications
30. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005
31. VA Handbook 7002, Logistics Management Procedures, July 10, 2009
32. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005
33. 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
34. Program Management Accountability System (PMAS) Guide V2.1, June 28, 2011
35. International Organization for Standardization (ISO) 9000 – Quality Management
http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/quality_management.htm
36. International Organization for Standardization (ISO) 9001:2008
http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/quality_management/iso_9001_2008.htm
37. International Organization for Standardization (ISO) IWA 1:2005 - ISO 9000 Improved Guidelines for Health Sector
http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/specific_applications/specific-applications_health.htm

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

38. International Organization for Standardization (ISO) 13485:2003 - Health Care and Medical Devices
http://www.iso.org/iso/iso_catalogue/management_and_leadership_standard/s/specific_applications/specific-applications_medical.htm
39. International Organization for Standardization (ISO) 13485:2003 Quality Management Systems for the Medical Device Industry
http://www.iso.org/iso/iso_catalogue/management_and_leadership_standard/s/specific_applications/specific-applications_medical.htm
40. AEMS/MERS Technical Engineering V. 7.0 Technical Manual (Revised 04/2008)
<http://www.va.gov/vdl/application.asp?appid=37>
41. AEMS/MERS Engineering Release Notes and Installation Guide, Version 7.0 (08/1993)
42. AEMS/MERS Engineering V. 7.0 User Manual, August 1993 (Revised 04/2008)
43. Mental Health Areas Installation Guide
<http://www.cfm.va.gov/til/dGuide/dgMH.pdf>
44. Aviva Project Site
<http://hi2.med.va.gov/>

4.0 GENERAL REQUIREMENTS

The Contractor shall provide and/or acquire the services, hardware, and software required by individual Task/Delivery Orders pursuant to the general requirements specified below.

4.1 Contract Type

This is an Indefinite Delivery/Indefinite Quantity (IDIQ) contract. Individual TOs shall be issued on a performance-based Firm-Fixed-Price (FFP) basis.

4.2 Performance Period

The ordering period for the basic contract shall be five (5) years from the effective date of award.

Work at a Government facility may require off-hour work due to network loading or other patient care operations as directed by the Contracting Officer's Representative (COR). For planning purposes, typical administrative hours at a VA facility are 8:00am to 4:30pm. The Contractor may also be required to support 24/7 operations 365 days per year as identified in individual TOs.

4.3 Place of Performance

The place of performance shall be identified in individual Task Orders. Locations will be Government or Contractor sites within the continental United States (CONUS) and/or outside the continental United States (OCONUS) at VA locations in Hawaii, Puerto Rico and Manila. Locations may include Federal, State, VA, or military data centers, facilities, treatment facilities, health clinics and Tricare facilities as defined in individual Task Orders. A map of VA locations is available at <http://www2.va.gov/directory/guide/division.asp?dnum=1>

4.4 Travel

Travel shall be in accordance with individual TO requirements. The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences through the period of performance. Include all estimated travel costs in the TO firm-fixed-price line items. These costs will not be directly reimbursed by the Government.

4.5 Method and Distribution of Deliverables

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007, MS PowerPoint 2000/2003/2007, MS Project 2000/2003/2007, MS Access 2000/2003/2007, MS Visio 2000/2002/2003/2007, AutoCAD 2002, and Adobe Portable Document Format (PDF).

4.6 Facility/Resource Provisions

The Government may provide office space, telephone service and system access when authorized contract staff work at a Government location, as required, in order

accomplishing the tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

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

VA shall provide access to VA-specific systems/network, as required, for execution of the task via a site-to-site VPN or other technology, including VA-specific software such as Veterans Health Information System and Technology Architecture (VistA). The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc., as required, for the development, storage, maintenance and delivery of products within the scope of this PWS. The Contractor shall transmit, store or otherwise maintain sensitive data or products within VA firewall in accordance with VA Handbook 6500.6 dated March 12, 2010.

4.7 Materials, Equipment and Facilities

4.7.1 Government-Furnished

Government Furnished Property, (GFP) which includes Government Furnished Material (GFM), Government Furnished Information (GFI), and Government Furnished Equipment, (GFE) may be provided if identified in the individual TO. The Contractor shall be responsible for conducting all necessary examinations, inspections, maintenance, and tests upon receipt. The Contractor shall be responsible for reporting all inspection results, maintenance actions, losses, and damage to the Government through the COR.

VA may provide VA-specific software, as appropriate and required, in individual TOs. The Contractor shall utilize VA-provided software development and test accounts, document and requirements repositories and others as required for the development, storage, maintenance and delivery of products. Contractors shall comply with VA security policies and procedures with respect to protecting sensitive data. See Section 8.0 for detailed security requirements.

4.7.2 Contractor-Furnished

All equipment, materials, and other property necessary to perform the work requirements and not specified for delivery to VA shall be the contractor's responsibility.

4.7.3 Non-Developmental Items and Commercial Processes

Non-Developmental Items (NDI), Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products shall be used to the maximum extent possible. The

Contractor shall apply commercially available and industry best processes, standards and technologies to the maximum extent possible.

4.7.4 Connectivity

VA will allow the Contractor use of Virtual Private Network (VPN), or equivalent, as appropriate. VA may install equipment at the Contractor's site to ensure security requirements are in place. The Contractor shall bear the cost to provide external connectivity to the VA from a non-Government work site through VPN, and VA will provide the required account access accordingly. Other connectivity to VA systems may be authorized as appropriate in individual TOs.

4.7.5 Marking, Handling, Storage, Preservation, Packaging, & Shipping

The Contractor shall establish and sustain procedures for handling, storage, preservation, packaging, and shipping to protect the quality of products and prevent damage, loss, deterioration, degradation or substitution of products. For each TO, all hardware shipments in support of RTLS will contain a bulletin on the packing list, which shall include the Integrated Funds Control, Accounting and Procurement (IFCAP) Purchase Order # (PO), and a short description of the hardware purpose. The Contractor shall obtain COR concurrence that all hardware is properly added to the VA Property Record prior to installation at field facilities.

4.8 Section 508 Requirements

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, 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. The Contractor shall comply with all required Federal or agency standards, as specified in the individual TO. Section 508, the Federal Information Technology Accessibility Initiative (36 CFR 1194), is incorporated into and made a part of this contract. Section 508 applies to all TOs. Specific Section 508 standards or other Section 508 requirements shall be stated in each TO. The standards and information on how to administer the Section 508 requirements are covered at <http://www.section508.gov>. Compliance with the applicable Section 508 standards is a material requirement of the contract.

4.9 Safety and Environmental

Safety and environmental procedures shall be identified in individual TO requirements.

The Contractor shall comply with the Office of Federal Procurement Policy Green Acquisition initiatives, as identified in individual TOs, in accordance with the policies referenced at http://www.whitehouse.gov/omb/procurement_index_green.

4.10 Enterprise and IT Framework

The Contractor shall support the VA enterprise management framework. The Contractor shall contact the facility TO COR as soon as possible with any issues, questions and concerns. In association with the framework, the Contractor shall comply with OIT Technical Reference Model (One-VA TRM) for VA acquisitions. One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. The Office of Enterprise Strategy, Policy, Plans & Programs (ESPPP) within the VA Office of Information & Technology (OI&T) has overall responsibility for the One-VA TRM. Exceptions to the One-VA TRM shall be submitted to the government for approval.

Additional frameworks may be specified in individual TOs.

The Contractor shall support VA efforts in accordance with the Program Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for Information and Technology, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget. Aligned with the PMAS process is the need for VA to assess Lessons Learned with new technology deployments and continuously maintain a quality improvement cycle. Contractor shall be required to work with VA to capture and implement solutions to lessons learned.

ProPath is a VA-wide process management tool that provides an 'at-a-glance' perspective of nearly every step in the software development process. The Contractor shall utilize the tools and templates, and shall file documents in ProPath as a central resource as required by the VA Process.

The Contractor shall support the VA's Software Quality Assurance and Release Management processes as defined in ProPath and shall develop the required artifacts. As per the requirements of the individual TO, the Contractor may be required to submit the following ProPath artifacts:

1. Formal Test Results
2. Primary Developer Checklist
3. Secondary Developer Checklist
4. Software Quality Assurance (SQA) Checklist
5. Defect Log
6. Defect Resolution Plan
7. Defect Fix/Status Report
8. Evaluation Summary

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

9. TRR Agenda
10. Package/Patch Completion Transition Document
11. Installation Guide Update
12. Release Notes
13. Security Guide
14. Technical Manuals
15. User's Guides
16. Interface Control Documents
17. Field Test Certification (a.k.a. Test site concurrence)
18. Initial Operating Capability Documentation
19. Deployment Plan
20. Software and Source Code

Based on the requirements in the individual TO's, the Contractor may additionally need to attain one or more of the following certifications:

- A. Field Testing Certification from each Test Site upon completion of Field Testing via email,
- B. Certification for National Deployment provided by Testing Service
- C. Conformance Validation Statement (508 compliance certificate)
- D. Interim Authority To Operate/Authority To Operate issued by the Authorizing Official

4.11 Transition and Orientation Support at end of Contract

The Contractor shall perform transition and orientation services (e.g., develop Phase-In/Phase-Out Transition Plan) to insure continuity of services as specified in the individual TO upon completion of contract. Transition and orientation support may include transitioning to Government or Contractor personnel.

5.0 SPECIFIC REQUIREMENTS, TASKS, AND DELIVERABLES

5.1 RTLS System Architecture, Development and Implementation

The Contractor shall establish the system architecture for the RTLS solution. All RTLS data from a given facility shall be integrated by the Contractor into a single database, and be accessible via a single user interface. The requirement is all RTLS data from a given facility is viewable within a single application that allows all RTLS data from that facility to interact with all other RTLS data from that facility. Constituent niche systems (e.g. SPD) will likely have their own user interfaces, optimized for the niche use case. Those niche user interfaces can be utilized within the niche area for staff working only with the given niche use case. However, the data from that niche system must *also* be available in the facility's "main" RTLS database, so that it can be viewed using the general-purpose RTLS user interface and so that the niche data can interact with other RTLS data from the facility. The RTLS at each facility must also be capable of exchanging data with VA information systems (such as VistA) and with a single national database that serves to aggregate and display RTLS data from all VA facilities (the NDR). It is expected that NDR requirements will evolve over time as the facility-level RTLS implementations are completed. While VA does not anticipate necessarily storing

every time-stamped RTLS event in the NDR, it is anticipated that many national-level analytical questions can be solved through the aggregation and analysis of local RTLS data. This architecture shall detail the hardware, software, processing methodology, data flow, and integration points at a local (facility), regional (VISN or other Networks), and national level that supports the gathering, storage, reporting, and analysis of VA RTLS data. The following data will serve in part as basis for formulation of the architecture:

1. VHA has 21 VISNs (groups of hospitals, outpatient clinics, nursing homes, etc.) and the preference would be to deploy RTLS at a VISN level. The number of facilities in a VISN varies from 5 medical centers to 10, depending upon the region.
2. VHA also has 7 CMOPs that will deploy as standalone facilities.
3. Approximate number of tags to be deployed at the following:
 - a. VHA facility – average estimate is for 80,000 active (25%) and passive (75%) tags per facility. This will vary by facility and is for an initial deployment / procurement only. It is expected that additional tags will be added over time.
 - b. CMOP facility – average estimate is for 3,000 active and passive tags per facility. This will vary by facility and is for an initial deployment. It is expected that additional tags will be added over time.

5.1.1 Architecture Design Considerations

As with any national-level technology rollout, there are a number of additional design considerations and tradeoffs that need to be made. The Contractor shall provide an architecture that addresses the following considerations:

1. VA is in the process of consolidating local data centers into larger regional level or national data centers and VA cloud computing solutions. In the context of this move towards VA cloud-based solutions, the solution shall account for tradeoffs involved with locating the majority of the RTLS server infrastructure in VA cloud infrastructure (such as regional/national data centers) versus the need for real-time response at the local facility level. For example, some required applications (such as patient elopement) directly affect safety and security of staff and patients – potential system downtime or latency issues could affect architecture decisions. Local and regional capacity to support this effort will vary from region to region and must be defined accordingly at the TO level. VA cannot guarantee the availability of space for an RTLS-specific server at every local facility, so the solution shall be capable of running in a virtual server environment. Furthermore, the RTLS solution shall be capable of operating effectively from a remote location, to accommodate situations where no virtual server (or no virtual server capacity) is available at the local facility. VA will consider either a 2-tiered architecture (with Tier 1 being an instance of the RTLS database dedicated to each local facility, [regardless of the database's physical location] or an instance of the RTLS database dedicated to each VISN, and Tier 2 being the NDR) or a 3-tiered

architecture (with Tier 1 being an instance of the RTLS database dedicated to each local facility, Tier 2 being an instance of the RTLS database dedicated to each VISN, and Tier 3 being the NDR). Justification for the proposed architecture should be included in the proposal.

2. The solution shall account for network utilization tradeoffs in determining server location. The system architecture shall minimize bandwidth utilization while maximizing throughput of data. The data transfer rate shall take into account size, distance and time when operating across the VA nationwide network. Tradeoffs in database design, location, frequency of updates, time and frequency of queries and cost can all impact system architecture decisions.
3. End User support and daily application management of the RTLS at a facility will be managed by VA facility and regional staff. As such, the RTLS and architecture will not require dedicated on-site contractor support to maintain.
4. VA maintains numerous databases which may interface with the RTLS at the local, regional, and/or national level. In some instances, databases may contain data only from an individual facility, while in other cases, may contain data from multiple facilities. For example, AEMS/MERS is typically deployed as a separate instance at a facility level; however two VISNs deploy it at a VISN-wide level. Therefore, a mechanism must be in place to allow multiple RTLS databases to communicate with a single VistA database. The Contractor shall provide a flexible system architecture that can accommodate numerous interfaces at potentially multiple levels in the architecture.
5. The system shall be designed with built-in redundancy and fault tolerance commensurate with a mission-critical system where patient safety is at risk. Depending on the type of facility and use cases, the RTLSs must be available as designated in Section 5.10.3 of this document. The Contractor shall provide a system architecture that provides for a high level of availability, especially at the facility level.
6. The RTLS system is expected to grow over time, as new use cases are added. The Contractor shall provide a system architecture capable of supporting the increasing magnitude of data anticipated, without redesign or degradation of existing capabilities. The architecture shall also be expandable to accommodate new use cases, without requiring changes to the architecture or contractor intervention.
7. The VA has a number of strategic initiatives designed to move towards an integrated Electronic Health Care program with the Department of Defense. The integrated Electronic Health Record (iEHR) is one initiative that is providing an Enterprise Service Bus (ESB). The Contractor shall ensure interoperability between the iEHR ESB and its RTLS ESB.
8. VA is moving its information systems toward designs that utilize a service-oriented architecture (SOA). It is therefore desirable that the design of the RTLS system also utilize SOA principles.

5.1.2 Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP)

The Contractor shall develop an independent COOP and/or DRP for the RTLS. For architecture placed within VA regional data centers, the Contractor shall supply all needed information and assistance for the development of a COOP and/or DRP for the RTLS and associated data for those locations.

The Contractor shall work in partnership with the Enterprise Systems Engineering Staff on the design of the DR/COOP and ensure it meets Standard Adherence. The Contractor shall follow guidance from the Office of Information and Technology Continuity of Operations handbook 0320.1 dated July 22, 2009.

Activities associated with developing the RTLS continuity of operations plans include:

- a. Identification of critical tasks associated with each use case.
- b. Prioritization of identified tasks.
- c. Establishment of personnel requirements necessary to conduct these tasks.
- d. Identification of mission critical systems necessary to support these tasks.
- e. Deferment of tasks not deemed essential to immediate agency needs.

All vital records shall be protected from damage or destruction. Federal continuity plan guidance recommends compliance with the US National Archives and Records Administration (NARA) Code of Regulations, Subchapter B – Records Management, to ensure the protection and continuous availability of vital records.

5.1.3 Disaster Recovery Specifications

As an enterprise wide system, RTLS is going to require multiple levels of disaster recovery, dependent on the final architecture and placement of the various infrastructure components. At a minimum, the system will have two levels of disaster recovery. The facility level RTLS system is considered mission critical, and will require a short (12-hour) time window for disaster recovery. The NDR components are not considered mission critical, and they have a longer time window for disaster recovery. Requirements are defined below:

- In disaster recovery situations, RTLS-L shall be restored to full operation within 12 hours.
- In disaster recovery situations, the NDR shall be restored to full operation within 72 hours.
- The RTLS and NDR shall be designed to facilitate database backups within a corporate data center environment.
- The RTLS and NDR shall be designed to be easily reloaded from a backup image and placed back into service.
- The RTLS and NDR shall be designed to prevent the loss of critical data.

- The RTLS and NDR shall be designed to support periodic archiving of data.

5.2 Operating Environment

5.2.1 PC Client

The client software shall be browser based. Browser and desktop configuration shall be in accordance with Federal Desktop Core Configuration (FDCC). Custom browser configuration shall not be required. The Contractor shall specify any plug-ins required for client software and approved version numbers. The software solutions shall support the current VA standard browser client and plug-ins and the previous major release of the browser/ plug-ins.

The defined system shall be compatible with the current VA Operating System (currently Microsoft Windows XP Client SP3) and Web Browser (currently Internet Explorer 7) standards, and shall remain compatible with newer versions as they are implemented by the VA.

5.2.1.1 Non-PC Client (tablets, smart phones)

Non-PC clients may be offered but are not required.

5.2.2 System Software

The system shall be capable of running on a virtual server. The Contractor shall use VA enterprise software whenever possible, and provide software for which VA does not currently have enterprise software licenses. The Contractor shall discuss with the TO COR if enterprise software is available prior to purchasing new software. VA enterprise software includes, but is not limited to the following:

1. IBM BigFix
2. Guidance EnCase
3. McAfee ePO (e-Policy Orchestrator)
4. McAfee VirusScan Enterprise V8.7 & HIPS V7.0 (Host Intrusion Prevention System)
5. SecureWave Sanctuary

The Contractor shall run the above mentioned software on all RTLS servers and associated PCs, where appropriate.

5.3 Software

5.3.1 Application Capabilities

A key component of the RTLS capability is the functionality presented to the system users and stakeholders. The Contractor shall design all RTLS user-facing applications

in accordance with common user interface standards and conventions, preferably Microsoft Windows/Office design standards.

The software shall have an intuitive User Interface. The user interface should be easy and implicit in its design taking into consideration; colors, icons, graphs, pick lists, free form text, notes, forms, point and click, drop and drag, copy and paste and other normalized Word-type capabilities that are critical to reducing errors.

The contractor shall evaluate application designs, application prototypes and COTS applications with VA stakeholders, both novice and expert, to ensure usability requirements are defined, tested and met.

The following subsections detail specifics on the requested application capabilities.

5.3.1.1 Real Time Location

The Contractor shall provide a COTS RTLS which supports the collection and reporting of RTLS data from RTLS devices within and across facilities to address the following functional areas:

1. People
2. Assets
3. Supplies
4. Specimens
5. Implants

The Contractor shall provide a web-based, real-time, tracking application that tracks and displays the location of all of these items within the designated areas in each facility and their movements within the designated areas. Further applications and use cases have been defined for development to include high level workflow based upon relationships of these items in the processes. Many VHA facilities are “campus” locations, with multiple buildings. In such cases, there may be a need to track tagged items, (eventually to include staff or patients) between buildings. .

5.3.1.2 Localization Methodology

The Contractor’s proposed RTLS application shall be capable of providing tag location, using a location coordinate system, so position can be overlaid on a floor plan. In addition, the application shall also be able to provide zonal positioning for the tag. Most use cases will require room-level specificity, however certain functionality within these use cases may require finer spatial resolution to bay or workstation levels. Examples include:

1. SPD workflow will require localization of tags at numerous workstations and devices within a large, open room with multiple stainless steel surfaces at various orientations.
2. VA has multi-bed rooms that require bed-level specificity. Recovery rooms can have up to 12 beds in one area.
3. Inventory management can require the identification of a supply to the cabinet, shelf or bin level.

5.3.1.3 Position Reporting

The RTLS shall allow for the definition of an unlimited number of zones and allow assets to be tracked at varying levels of specificity (e.g., 3rd floor zone, Room 124 on 3rd floor, etc.). The Contractor's RTLS solution shall discriminate between indoor and outdoor locations. The RTLS shall manage the discrimination between designated location quadrants in the facility (floor, zone, room, etc.). Floor-to-floor discrimination is required in all zones except stairwells. The RTLS shall detect, record, and display tag travel direction (examples include the ability to discriminate between exiting versus entering specified egress points for patients, staff, visitors or critical assets) The Contractor shall be capable of preparing or updating facility CAD drawings, if required by the individual TO. The Contractor shall assist with the reconciliation of conflicting names for the same location as required.

5.3.1.4 Presentation Features

The Contractor's RTLS solution shall include a configurable, rule-based mapping application that can generate alerts and alarms based on VA-specified events, such as but not limited to: the movement of patients and assets into or out of a specified area, the state of a tag, etc. The system shall be capable of event history playback or look-up. The RTLS query/display software shall be capable of displaying at least two photographic images of each tagged item.

5.3.1.5 Customizable Views

The RTLS solution shall visually depict assets within a zone, several zones or within an entire building (i.e., graphical representation of assets on the 1st floor of building 99).

The system shall provide customizable viewing options for users (e.g., lists, maps, dashboard views, location of items on screen, favorite reports, other graphical views, etc.) The system shall have a customizable user interface based upon class of user (e.g., view of certain items, locations, etc.). The system shall remember the user's default view and their last view. The initial display at the initiation of a new session shall be user configurable based on the user's selection.

5.3.1.6 Play Back Routes

The application shall have a method for time-lapse location monitoring with a playback mode in real time or rapid mode for equipment movement (report and graphical views) The duration of location memory shall be selectable by the VA based on the category of the tagged item with a maximum play-back period of 48 hours. For asset tracking, the system shall provide a graphical map display with search capabilities based on asset type or Identification (ID) number. It shall be possible to tailor or limit users' map views based on their user group and its associated access privileges.

5.3.1.7 Patient and Staff Tracking Requirement for Mapping Display

The Contractor shall design and develop the patient elopement system so that if a patient has moved outside of a designated area (or is attempting to), a warning alert shall appear at the nurse station's computer monitor along with a floor plan of the relevant patient care area. This floor plan shall display an indicator pointing out the real-time location of the eloped patient. The system shall have the ability to post alerts or other notifications such as entry of patients into restricted areas or removal of items from an area in a dashboard-like display clearly indicating the priority of the event. The RTLS shall also have the capability of generating messages regarding these events and sending them to external notification systems, for delivery to devices such as pagers, cell phones, or in-house wireless communication devices, as well as to other computer systems.

5.3.1.8 Help

The software shall have a searchable help function accessible to all users.

5.3.2 Alerting

The following describes the spectrum of alerting and alarming capabilities that are expected of the RTLS. For the purpose of this document, an alert is defined as passive and an alarm is defined as active. Specific alerting requirements will be defined at the individual TO level. The capability should exist to run reports for all types of alerts and alarms.

5.3.2.1 Alert Rule Configuration

The system shall provide the capability to configure business rules for alerts and alarms. Alert notifications shall be customizable based on class or category of device (e.g. laptop passing through an exit door generates a different level of alert than a wheelchair). The alert notifications shall be configurable on a per-tag basis. The alert capabilities shall be programmable based on individual named users or designated user roles. User interface for alert configuration shall be easy to use, requiring no more than 1 hour of specific training on alerts for proper use.

The system shall be capable of designating one or more alert notification mechanisms based on the location or movement of a tag. The system shall send alert messages to communication and hospital systems, such as physical security systems. These interfaces shall be activated based on predefined alarm events (i.e., security camera is triggered upon detection of an asset exiting the building). Alarms and Alerts shall have the ability to be sent to the VA facility's unified communication system. The system shall notify users through various communication mechanisms, including but not limited to: email, telephone systems (all types), pager text message, and instant messaging. The system shall be able to direct alarms and alerts to specific users or user roles to the extent that these functions will be controlled by or integrated to the specified software at the TO level.

During system installation, a designated number of notifications will be pre-configured as defined by the user team. Authorized users shall be capable of modifying existing notifications and adding additional notifications after initial installation. Notifications shall be capable of registering a status of acknowledged or closed. It is desirable but not required that notifications shall be automatically forwarded to the next tier of responsibility if there is no closure of the alert within a specified time period.

5.3.2.2 Geo-Spatial and Time Based Alerting

The system shall provide the capability to designate geospatial areas for geo-fencing. The system shall be configurable to alert when a geo-fence region is entered, exited, or if a tag dwells within the region for a specified period of time. The system shall generate alerts when a tag enters, exists or dwells in a reader coverage area. The system shall alert if an object designated as stationary is moved. The system shall send alerts if tagged assets assigned to certain locations are removed from those approved locations. The system shall provide automatic, proactive area entrance and exit alerts for all designated zones.

The system shall generate an alert when a given tag signal has not been received for greater than a specified period of time. For assets that have been unloadable for more than the specified period of time, the system shall send an alert when the device reappears into the system. The system shall provide an alert when a previously active tag that has gone outside of a detection area for a specified period of time reenters a zone and becomes active. Detection delay shall be programmable.

5.3.2.3 Sensory Alerting

For tags with environmental monitoring capabilities, the system shall allow the user to program the environmental limits. The system shall alarm when tags with environmental monitoring capabilities are outside preprogrammed limits.

The system shall be capable of sending an alert from a tagged patient when he or she falls to the ground.

5.3.2.4 Status Alerting

The system shall provide the capability to associate a status with a tag, and to modify the status of a tag. The system shall provide the capability to configure business rules for alerts based on tag status being changed. The system shall notify appropriate systems or users when the tag status is changed.

5.3.2.5 Staff Panic Button Alerting

Staff tags shall have one or more programmable buttons. The button shall allow staff to activate a "panic" alarm from their tag so that an alert is sent from the RTLS to the facility's communication or security system. The alert shall detail time of alert, staff identification, location where alert was activated, and current location of staff member.

5.3.2.6 SPD Automation Requirement

The system shall immediately send an alert when the cleaning/sterilization process is not completed properly, as defined by standardized workflow/business rules developed from directives and guidance documents.

5.3.2.7 Patient Elopement / People tracking

Authorized VA staff shall be able to configure the security level of the system on patients, based on their degree of risk. For example, some patients may be confined to their room (high risk) while other patients may have a more relaxed restriction and only be confined to a specific ward/floor (low risk).

The system shall be capable of sending a signal to a door management system, if available at the individual facility, to allow the enabling/ disabling of locks and audible alarm systems when a specific patient has come within a defined distance of exiting the ward. Authorized VA users shall be allowed to override these instructions by using other VA life support/emergency systems. The system shall respond to a patient exiting the zone within 4 seconds for staff to respond to avoid elopement. Door alarm systems should be sent locking messages within 1 second. Medical staff shall be able to designate specific users to be able to activate/deactivate the patient elopement alarm feature for any given patient.

When the VA facility elevator system is capable, the RTLS shall be able to send a signal to the elevator system in order to lock out the elevators when an eloped patient is in the elevator/stairwell zone. For locked units, tags shall be configurable to unlock doors as authorized staff approaches.

VA staff shall be able to designate specific users' privileges to be able to activate/deactivate patient wander alerts for any given patient paired with a tag. Each identified zone for patient wander shall have sensors detecting patient movement in and out of designated area.

5.3.3 Process Management

The system shall allow for the creation of workflow rules, reports alarm triggers, etc. to be facility centric and customizable for each VA facility. The system shall also have a mechanism for nationally defined workflow/alerts that can be set to be un-editable at the local level. The system shall accept user status updates through some combination of tag buttons and direct input into the user interface. Configuration shall have the capability to be copied from facility to facility to ease in system setup, but each facility must also have the ability to create unique business rules.

5.3.3.1 Workflow Management

The system shall be designed to have tracking with alerts for specific, VA-defined workflows that require a predefined sequence of events. Specific examples of workflow management will be identified at the TO level.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

The process for creation of custom workflows and reports shall be simple and easy to understand, requiring minimal application training.

To achieve workflow in certain use case applications, the system must meet the following requirements:

1. Tags must have the ability to have defined relationships with one another, regardless of tag type (active, passive) or application from which tagged item is used.
Example: A patient record could be updated (based upon set business rules) when the following tagged items enter a surgical field during a procedure; patient, staff, surgical instrument, medical device, or supply item.
2. The system shall have the ability to define the status of a tagged item based on applicable business rules.
Example: A medical device could assumed to be dirty or clean based upon its location or activation of a programmed button on the tag
3. Tags shall have the ability to be linked or grouped with each other in the software
Example: Tagged Surgical Instruments can be linked together for use in a tagged surgical tray.
4. The system shall have the ability to assign short-term use tags
Example: Rented or Loaned equipment can be easily and quickly tagged for tracking purposes with a notification when rental period is over
Example: Tags can be assigned on a daily basis for contractors or visitors to a facility.

5.3.4 Data Management

5.3.4.1 Queries

The Contractor shall provide a RTLS that allows users to query any or all of the assets for a specific facility. Users shall have the ability to perform drill-down searching by multiple filters (i.e., VISN > campus > building > floor > area/zone > room > patient care vicinity). The mechanisms for querying results shall be forms-based or graphical. Search capability shall be provided to users for multiple options to include: current / past location, item demographics, time in a location, and relationship to other tagged items. The solution shall include a standard base set of queries for each installation. Base queries may be further defined, enhanced and or modified in accordance with the requirements of individual TOs. The RTLS solution shall provide users the ability to create and save their own queries as well as share queries with other VA sites without intervention from the Contractor and at no additional cost.

5.3.4.2 Reporting

The Contractor shall provide standard reporting capability that will be available upon installation. The system shall be capable of providing reporting at both a facility and regional level. Additional reports will be defined at the TO level. The Contractor's RTLS solution shall provide users with the ability to create and save ad-hoc reports. The Contractor shall provide training and support for user ad-hoc reporting features in

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

accordance with the requirements identified in each individual TO. Custom reports and report templates designed for VA will be the property of VA.

The system shall provide the following additional reporting capabilities:

1. Report generation and modification based on defined access level by user group/category
2. Prescheduled reporting and automated delivery to an e-mail distribution list
3. Reporting capable of both periodic and on-demand frequencies
4. Report generation based on defined access level by user group or category
5. Graphical reports to include: time based charts, bar charts, line charts, digital dashboards and other standard commercially available visualization capabilities
6. Report layout tool for designing data connections and report layout
7. Sharing of report templates between VA sites.
8. Exporting report data: It shall be possible to save report output in file formats compatible with Microsoft Office products (principally Word and Excel) and in PDF format.
9. Allow the ability to make report templates un-editable
10. Provide a status indicator of query and report generation and estimated time to complete (prior to submission of the task).
11. The proposed solution must offer customizable dashboards so that the end users can gain critical business intelligence data. These dashboards shall include metrics and measurements defined in each VA use case included in Attachment A of this PWS.

The Contractor shall provide various RTLS administrative system report templates consisting of, but not limited to, the following:

1. The number of users logging in, when, and for how long
2. The type of content that is accessed
3. Malfunctioning readers
4. Available disk space
5. System Status and/or Health
6. Other system management reports

The RTLS shall allow novice users to produce site-specific reports with no more than two hours of training. The RTLS solution shall allow expert users to produce tailored reports after 40 or less hours of training. The RTLS solution shall allow users to save tailored report templates for future use; saving a report should not require an expert user.

5.3.5 Virus and Attack Protection

The system shall have an integrated method of protecting the system firmware and software from viruses and other malware with the latest version of the VA's anti-virus and host intrusion protection software. The system shall conform to VA and HIPAA security standards for data transmission.

The system shall maintain an audit trail of who has accessed individual files and the time and date when those files were accessed, edited, or deleted. The Contractor shall complete VA's Pre-Procurement Assessment per Directive 6550. The Contractor shall provide VA with a list of all communication ports and protocols required for communication into and out of the system. The system shall also detect and track unauthorized attempts to access the system.

5.3.6 Role Based System Access

VA shall be able to assign users access to the client software, with no limit to the number of users granted access (e.g., enterprise license). The RTLS and NDR shall accommodate simultaneous access and simultaneous query for unlimited users.

5.3.6.1 Directory Services

The RTLS shall provide user authentication through the existing VA Active Directory infrastructure. This shall provide a "Single Sign-On (SSO), so that the user will not have to provide a second Account/Password log-in upon launching the RTLS application. User credentials stored within RTLS shall be encrypted using the latest NIST recommended algorithm (currently SHA-2 hashing algorithm, moving in near term to SHA-3).

Within the Active Directory application, the Contractor shall be capable of utilizing AD "Organizational Units" (OUs) and Security Groups in order to support distinctive groups as well as individual AD users. This will assist in the assignment of RTLS-access privileges based on the user's function and role within the RTLS application.

The RTLS shall assign privileges to the user based upon the active directory log-in data provided by the user. The rule-based algorithm shall be sufficiently flexible to address system application requirements that may change over time.

1. All valid user accounts shall have RTLS viewing access.
2. Power-user accounts shall have access to use-case report generation and to assign staff tracking tags to the appropriate personnel.
3. System Administrator accounts shall have access to system administration, diagnostic, maintenance, and upgrade capabilities.
4. Other rule-based system access privileges shall be assignable based on the particular needs of the use case as determined by post-implementation experiences. The RTLS rule-based system shall provide the VHA capability to control user viewing and reporting access down to the individual data field level.

5.3.6.2 Role-based Controls

The system shall provide hierarchical access for users. The access levels shall be configurable by VA through role-based group privileges. Access to information and creation of custom workflows and reports shall be limited to users with appropriate access based on their group. Roles shall be assigned by "least privileges" down to

"view only" configurations. The proposed system shall lock out a user who is not approved to perform a particular process based on user group membership, and will log the incident. The system shall have the capability of sending immediate alerts for certain security incidents, as specified by VA RTLS administrators.

5.3.7 RTLS Software Capability for Large Wall-Mounted Monitors

The Contractor shall provide a software capability to display selected RTLS data on large flat screen wall-mounted monitors and receive / display alerts on these monitors. RTLS software must be capable of a HIPAA compliant display. If touch-screen monitors are provided, the software should be optimized to utilize a touch-screen interface.

5.4 RTLS Hardware Acquisition and Delivery

The Contractor shall provide, deliver, and install all hardware components necessary to implement the solution as identified in each TO, including any incidental hardware or equipment necessary for completion of the initial facility installation, with the exception of wired or 802.11 wireless network infrastructure. VA will not be responsible for storage or other logistical support for hardware deliveries. Hardware required for sustainment will be requisitioned through contract modification or separate TOs. Installation TOs will not include sustainment spares, but may include them if identified. Hardware ordered after initial facility installation may exclude installation.

Whenever the VA states that a Wi-Fi infrastructure will not be installed in a facility deploying RTLS technology, the Contractor shall be capable of providing both an alternate infrastructure to support RTLS, and the RTLS tags, readers and other hardware compatible with that alternate technology.

5.4.1 RTLS Tags

The Contractor shall provide a variety of tag types and technologies that will be used for multiple applications. Each tag shall be able to accomplish all of the requirements of the specific use case for which it is intended. The Contractor shall provide tags that meet or exceed the minimum requirements, which are defined below. Active tags shall have an onboard battery voltage monitor and automatic signaling when battery life reaches a pre-defined threshold level. When battery-powered tags are used, the power level shall be read using the readers. The Contractor shall provide active tags that work in either beacon mode, or associate with the network. Contractor shall provide a set of active tags that shall be able to sense if it has been tampered with or removed from the object from which it was attached. Both active and passive tags shall be tamper resistant.

The Contractor shall provide a variety of tags capable of operating in multiple environments including, but not limited to: sterile storage, wet, oxygen rich, and indoor/outdoor. The Contractor shall provide environmental range capability specifications for all tag models provided.

5.4.1.1 Power

Battery powered tags shall have a battery life of at least 3 years at a 5min beacon rate. (The 5 minute beacon rate is an example for the sake of comparability. It is not a requirement for all active tags.)

5.4.1.2 Encoding

The Contractor shall provide unique tag numbers. The RTLS solution shall not allow duplicate tag numbers within the entire VA system. Passive tags shall have the ability to have VA's numerical nomenclature printed on the tag. VA currently utilizes an alphanumeric nomenclature to identify their assets and instruments (EE Numbers – example: 528A4-EE12345, where “528A4” is the station number and “12345” is the unique identification number in AEMS/MERS). All tags provided, should have the ability to display this identifying number on the tag for visual verification. A standard for physical identification of active tags with EE numbers will be created during the VISN 23 deployment and utilized for all future VISN Task Orders.

5.4.1.3 Communications

Tags shall be able to communicate using an unlicensed portion of United States of America (USA) spectrum.

5.4.1.4 Tags with Sensors

The Contractor shall provide tags with sensors. Tags with temperature and humidity monitoring capability shall have external probes and be NIST traceable.

The Contractor shall provide active temperature sensor tags and monitoring solutions. The temperature monitoring solution shall include tags with the ability to be mounted in the interior of assets that have a closed container (refrigerator and freezers, for example) without the use of an external probe and wire penetrating the insulation. Where appropriate, the solution shall provide mountable tags with external temperature probe and wire; in this application, the probe shall be NIST traceable and able to be calibrated. The temperature monitoring solution shall produce an alarm in the event of the following tag issues: a) High Temperature; b) Low Temperature, c) low battery capacity, b) tag failure, c) probe failure (for externally mounted tags), and d) tampering with, or removal of, tag.

5.4.1.5 Programmable Features

VA prefers that programmable tags shall be capable of being programmed remotely over the air. For example, when applicable, the active tag beacon rate shall be programmable over the air and the beacon rate shall be able to be set to multiple time intervals (minimum 2 seconds). The tags' beacon rate shall be adjustable based on configuration (i.e., tag will increase beacon rate when status changes from “idle” to “in motion”).

The Contractor may need to provide active tags with on-tag button(s) for information to be communicated back to the RTLS server. In the event that the Contractor is required

to provide active tags with buttons, it is preferred that the system logic shall be programmable. The tags shall be programmed to respond to sensors or be triggered by a command sent to the tag. The contractor shall be capable of providing tags with either an audible or a vibration alert capability. It is desirable, but not required, that the contractor is capable of providing tags with adjustable motion sensitivity thresholds and motion timeout settings. Where applicable, the tags shall be firmware upgradeable over the air.

5.4.1.6 Physical Design

The Contractor shall provide tags in a variety of shapes and sizes to fit a variety of assets. Tags shall be reusable whenever applicable to the requirements of the defined use case per individual TO. They shall be durable and properly sealed to guard against damage from exposure to liquids. Tags shall be placed on patient ID bracelets and staff badges. Tags that are mounted using adhesives shall be durable and properly sealed to guard against damage from exposure to liquid, dust, and debris. Tags shall be capable of being mounted on metal surfaces. Tags shall be capable of being read when affixed to metal assets. If technically feasible, tags shall be capable of being inserted inside desktop computers, laptops, and medical devices with no interference with equipment performance. If tags are to be affixed to existing surgical instrumentation, the method of adhering the tag to the device should mitigate the risk of becoming a retained foreign body within the patient.

5.4.1.7 Size

Both active and passive tags shall have a small footprint so as not to interfere with the operation of the equipment and shall be able to be attached in an inconspicuous location. Tags shall have the ability to be attached to surgical instruments in a variety of sizes from 1 to 12 inches.

5.4.1.8 Environmental

Tags used for surgical and other sterilizable devices shall be able to withstand cleaning and sterilization (liquid steam) using various techniques at temperatures of up to 275 degrees Fahrenheit for up to 30 minutes. The Contractor shall provide documentation on procedures for cleaning/maintaining tags.

Tags shall be resistant to chemical agents. Tags shall be able to endure multiple cleaning protocols; 1) low level disinfection (no claim for tuberculocidal activity), 2) intermediate level disinfection (disinfectant with tuberculocidal activity), 3) high level disinfection (sterilant / disinfectant with sporicidal chemical - short contact time), and 4) Sterilization (sterilant / disinfectant with sporicidal chemical - prolonged contact time).

Tags shall be resistant to high pressure fluids (e.g., water, steam, etc.). Tags shall operate in an oxygen-rich environment and not ignite combustible gases. The Contractor shall document conditions where tags could cause interference with other electronic devices or receive interference from other electronic devices. Tags shall be safe to use around electrical equipment items that are known sources of interference. Tags shall withstand a reasonable amount of electrostatic discharge in accordance with

industry standards. . Tags shall withstand shock and shear forces to the greatest extent possible. The Contractor shall provide a water-tight, hermetically sealed, autoclavable RTLS tag solution for instrument trays and other items. The RTLS tags for this purpose shall be resistant to ETO, H₂O₂, PA, and other sterilization methods in place at VA medical centers.

5.4.1.9 Passive Tags

Contractor shall provide standardized (one) passive tagging technology, but may provide tags in various shapes, sizes, and materials. Passive tags shall be capable of excitation and sensing with both mounted and hand held readers. Passive tags shall be capable of operating, and resistant to degradation, when exposed to certain conditions, such as exposure to disinfectant and cleansing agents.

The Contractor shall provide an exciter/reader, (mounted and mobile handheld), with a minimum scan distance, (under Contractor-defined conditions), capable of accurate scanning from a standoff distance of at least one meter. A larger functional scan distance is the desirable goal; given that the exciter/reader shall not interfere with medical and other care-critical device operation and communications.

5.4.1.10 Instrument Tagging

While VA prefers active and passive RFID tagging, if employed, two-dimensional (2D) data matrix barcodes (stencils) are required to be produced sequentially in number to create a unique identifier for surgical instruments in VA. The 2D stencils should employ not less than three (3), and allow for up to five (5) digit customizable prefixes that VA will utilize to enter facility-specific codes for future enterprise-wide tracking purposes. The instrument tracking software will remain flexible and scalable over time to allow seamless inter-facility transfers of items with traceability and full maintenance history. An example of this strategy is embedded below for review.



VA Facilities 2D
Stenciling Strategy.xl

The Contractor shall be capable of providing instrument etching services as required at the TO level.

5.4.1.11 CCX Compatibility

RFID tags shall be compatible with Cisco Compatibility Extension (CCX) specification version 4 or later.

5.4.1.12 Tagging and Commissioning Services

The Contractor shall include optional services for the tagging and/or commissioning of all items such as assets, supplies, and instruments. These services shall include

locating the item(s), researching said item(s) for necessary information, affixing tags/labels or etching as appropriate to the item, completing necessary data entry, and system configuration to fully activate these individual items within the RTLS and/or VA System of Record. All tagging and/or commissioning activities shall be communicated to VA inventory and equipment team(s) as defined by the individual station. The specific selection of tagging and/or commissioning service needs shall be defined in the Task Order.

5.4.2 RTLS Readers/ Interrogators Reader and Device Management

The system shall recognize both active and passive tags. The RTLS infrastructure shall accommodate new additions or changes to the coverage requirements inside the facility. The readers/receivers shall utilize or leverage the existing facility data network, and shall comply with VA security requirements. The Contractor shall specify the approximate quantity of additional LAN connections required at each facility. Whenever the existing facility wireless network is to be utilized, (Wi-Fi-based installations) the Contractor shall confirm coverage areas and notify the COR where the facility wireless network must be enhanced to support the desired operational performance. The Contractor shall also confirm whether or not existing services on those networks will be impacted by the increased traffic attributable to RTLS.

The Contractor shall provide fixed passive RFID readers that shall be powered via Power Over Ethernet (PoE). VA prefers that add-on / supplemental technology readers are battery powered. If non-battery powered add-on / supplemental technology readers are not provided, the contractor shall clearly state this and provide an explanation on why this solution is preferred.

5.4.2.1 Fixed Readers

The Contractor shall provide fixed readers powered by a standard 110V supply unless otherwise specified by the TO. The readers/receivers shall operate and communicate at a power level and frequency that does not interfere with any other devices in VA facilities. Contractor shall conduct testing of this capability prior to installation.

The Contractor shall provide readers that are capable of functioning in a dense asset identification environment such as a warehouse storage room or clean utility room. The readers shall be able to discretely identify all tagged items in such a location without false positive or false negative identification.

The readers shall be able to be dynamically monitored by the RTLS to ensure that all reader components are working properly. If the readers experience any loss in connectivity, the RTLS shall be alerted.

5.4.2.2 Handheld Readers

The Contractor shall provide handheld readers that download and upload (preferably wirelessly) current information from the RTLS database to better reconcile equipment assigned to various zones. These readers shall have the ability to determine location

and associate it to the tagged item that was scanned without having to scan a bar code when entering a location. All fixed reader requirements mentioned previously in section 5.4.2.1 shall apply to the handheld readers.

The readers and receivers shall operate and communicate at a power level and frequency that does not interfere with any other devices in the medical center. The Contractor shall test to verify compatibility prior to first use. Readers shall not operate within the Medical Telemetry Frequency Range.

The Contractor shall provide an exciter/reader, (mounted and mobile handheld), capable of accurate scanning from a standoff distance of at least one meter. A larger functional scan distance is the desirable goal; despite that, the exciter/reader shall not interfere with medical and other care-critical device operation and communications.

5.4.3 RTLS Display Monitors

The Contractor shall provide large, wall-mounted display monitors in each ward or other locations, as specified at the TO level. Per requirements specified at the TO level, the Contractor shall provide display monitors with touch screen capability. Examples of where this technology may be applicable would be included but not limited to patient elopement, surgical, and emergency department use cases. The size of the monitors will be determined at the TO level. Displays shall not cause electromagnetic interference (e.g. plasma display causing infra-red interference).

5.4.4 Passive Tag Printers

The Contractor shall be capable of supplying printers with the capability of printing human readable information and barcodes on passive tags.

5.4.5 Smart Cabinets

The Contractor shall be capable of supplying Smart Cabinets that can inventory and report on items entering or leaving the cabinet confines. Smart Cabinets shall be available as stationary or mobile devices.

5.5 System Administration

The storage system and database shall provide means for proactively notifying the system administrator in the event of a failure. The notification system shall include drive, disk, and tape failures, as well as failures of other hardware components. The system shall notify multiple phone/pager numbers through the VA facility's unified communication system in the event of such a failure.

The system shall allow VA to manage firmware/software/system configuration remotely for all components of the RTLS. The system shall dynamically monitor each component to ensure it is working properly. The system shall send alerts to a system administrator whenever there is a loss in connectivity or failure of any of the hardware and/or infrastructure components.

VA system administrators shall have full access to the hardware, software and programs that constitute the system, including any diagnostic software features, and full administrative rights. The Contractor shall brief VA system administrators regarding all software upgrades and changes; VA system administrators must agree to each software upgrade, prior to installation. A mutually agreed upon "Change Management Process" shall be developed prior to system installation.

The Contractor shall provide diagnostics software/tools and support for readers (i.e. RTLS Readers) and server software. The Contractor may be required to provide system administration services, software development, and database design, as defined at the individual TO level. The Contractor shall be capable of remotely accessing the RTLS by a VA-approved methodology. The Contractor shall complete a VA interim security agreement/memorandum of understanding (ISA/MOU). The Contractor's Remote Control Software shall be FIPS 140-2 Compliant.

5.6 Data Interfaces and Standards

5.6.1 General Interface Requirements for RTLS

The Contractor shall create all required interfaces, from end-to-end, in accordance with industry standards, to communicate with all VA information systems. This will include any M programming code (i.e., MUMPS - [Massachusetts General Hospital](#) Utility Multi-Programming System), that would need to be added/modified within the selected VA information system / database to allow for the exchange of data between the RTLS and NDR to and from that system. It is understood that VA will provide a conceptual data model for all data that must flow from VA information systems to the RTLS and NDR Solutions to allow for clarity and consistency of data. Contractors shall be required to map this data from local non-standard terms to nationally standardized terms as necessary. The contractor is required to provide a development and test environment for the RTLS solution. VA will provide access to VA test data and systems for Contractor verification of any interfaces developed to VA information systems.

The Contractor shall capture interface details through the creation of a formal Interface Control Document (ICD). The ICD shall become the intellectual property of VA. As a part of the ICD, the Contractor shall provide a chart indicating relevant factors for calculation of response time of data transfer rates between interface databases. The chart shall include parameters required to accomplish industry-standard response times.

The Contractor shall adhere to common industry standards designed to enable exchange of data amongst the RTLS, NDR and other VA information systems. As an initial guide, the Contractor shall ensure RTLS data is integrated through common industry standards for data transport, data transformation, and routing, to include: The methods for transferring data between VA information applications such as standard industry protocols (i.e., TCP/IP); Data transformation actions for converting RTLS data from one data format (source) to another (destination); and the real-time communication

of data (such as an RTLS location event) from one application to another (i.e., synchronously - pull model or asynchronously - push model).

The Contractor shall provide standard system architecture, data mapping support and both local and national database storage and reporting, thereby standardizing solutions for all facilities within each respective VA organization. The Contractor shall work with VA to establish a standardized naming convention for items within the RTLS database. Upon VA approval of the standard naming convention, the contractor shall implement and then map / translate data elements from existing VA databases to the RTLS standard term when necessary. To preserve data integrity, the Contractor shall provide a drop down list of standardized data elements in selected data entry screens and permissions to edit these lists will be restricted through hierarchical controls.

The Contractor shall provide data profiling to support data mapping from the multiple independently maintained VA databases. Data profiling shall include a metadata database and user friendly reports that analyze and describe the content and characteristics of all data sources. Data profiling shall support both initial data mapping and ongoing drift analysis. The contractor shall derive terminology sets from the data profiles that will form the basis of the translation tables. Profiling analysis shall include both statistical measures and distribution characteristics. Reports shall be user friendly and include graphics such as histograms and distribution graphs. Reports shall also include the ability to drill down to individual offending records that do not conform to the data nomenclature standard.

The Contractor shall track all interfaces developed at the TO level. Interface code shall be stored and maintained by the contractor to enable reuse of common interfaces under follow-on task orders with no additional development fee.

5.6.2 VA Application Interfaces

The Contractor shall provide Application Program Interfaces (APIs) to facilitate integration of the RTLS solution with other VA applications and third-party applications through open standards. The Contractor shall provide a language-independent service-oriented API, written so that it can be called from several programming languages and provided as remote procedure calls or web services. The Contractor shall provide a non-proprietary ICD with details on messaging, routing, and connectivity required to reliably integrate RTLS data into existing databases. Attachment C of this PWS includes a list of VA information systems / databases that may need to be interfaced with the RTLS and/or NDR.

The Contractor shall provide bi-directional interfaces to both the RTLS and NDR databases. Interfacing with identified COTS systems shall be completed between contractors, without VA assistance.

5.6.3 Mobile Device Application Interfaces

The RTLS shall accept data from portable data capture devices as well as fixed position readers. The RTLS shall provide for mobile viewing applications (e.g. laptops,

handhelds, smart phones). The RTLS shall be able to integrate with fixed and mobile output devices. (i.e. Barcode printers, RFID printers, mobile printers). The RTLS shall orchestrate RTLS-related end-to-end processes by: Supporting machine-to-machine communication in systems environment; and providing seamless integration with workflow, rules management, role management and UI (user-interface) tools.

5.6.4 Miscellaneous Hardware Interfaces

The RTLS shall interface with various other hardware systems for the associated use cases, such as security systems, elevators, door interlocks, energy management, contractor visitation system, or PIV access card. Individual interfaces will be determined at the TO level.

5.6.5 Communication Interfaces

The RTLS shall integrate with communication systems at each facility deployment based on the individual TO for the purposes of alerting / alarming and messaging. Types of communication systems include: SMTP Email Server (same for all VA), two-way paging systems, nurse call systems, Voice Over Internet Protocol communication systems, cell phones and pagers.

5.7 Database Design, Standardization and Management

5.7.1 RTLS Databases

The Contractor shall create a standard database schema that shall be used for all VA RTLS implementations. The schema shall become the intellectual property of VA. The database shall retain a minimum of 18 months of history for tagged items. For more consistently moving items, the amount of retained history will fluctuate and will be defined at the TO level. The database shall be able to store one or more images of a tagged asset, as well as a description (caption) for each image.

The Contractor shall integrate information from multiple tags and technologies into a single database per the defined architecture. The RTLS shall have the ability to establish relationships between tags and these will be listed in a single database (e.g., if instruments are 2D bar-coded and a person has an active tag and a sterilizer has a passive tag, all can have a relationship to each other for business process and work flow tracking purposes). The database shall also distinguish VA-owned versus rented tagged items.

The RTLS database shall incorporate information on all tagged items. This information may be imported from VA information systems, manually entered by facility personnel, or inputted by devices (e.g. scanners). The database shall maintain information on the sources of all data. Whether the RTLS solution consists of a single database at the facility level or multiple databases (i.e. one database for each niche use case or equipment type), the solution shall ultimately consolidate all facility-level RTLS data into a single facility-level database and present a single, unified user interface to the VA user, from which information about any tagged item at that facility may be obtained.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

Users should not be required to navigate from one RTLS subsystem database to another in order to effectively use the system.

There shall be a single, nationally standardized database schema that all instances of RTLS in VA will adhere to. The Contractor shall assist VA in maintaining the database schema and the data it contains clean. VA shall have access to the RTLS and NDR database schemas at no additional cost, such that VA will be able write its own queries of the database, should it so choose. RTLS databases shall be accessible from a standardized database management tool that allows System Administrators and select users the ability to administrate all aspects of the database and its container.

Ownership of all RTLS data remains with VA and the Contractor shall allow VA to migrate any and all RTLS data to another contractor's system at the end of this contract, should VA so choose. There shall be no fees associated with the right to export/copy VA data from Contractor's database and there shall be no requirement for this function to be performed by Contractor's staff (i.e., VA staff may export the data, if VA so chooses). Upon request, the Contractor shall provide VA staff with instructions on how to export the data, at no additional cost to the Government.

5.7.2 National Data Repository (NDR)

The Contractor shall provide a solution to enable the querying, viewing, and reporting of aggregate data from any or all VA RTLS databases. In other words, an authorized user at any VISN or Region, or at a National level, must be able to view selected VA RTLS data from any individual VA facility or aggregated RTLS data from any combination of VA facilities, in order to be able to get a VISN-wide, Region-wide, national, or custom view of the data. (VISN-wide aggregation may be unnecessary if the Contractor's RTLS solution specifies a VISN-level RTLS database rather than a facility-level database.)

The Contractor shall utilize COTS and/or industry standard components and applications to develop, customize, integrate, test, train, deploy, and maintain NDR capability. VA's desire is to employ COTS and industry standard components wherever and whenever possible. NDR shall provide extensive business intelligence and predictive analytics capabilities, preferably through a web-based interface. Where possible, existing VA Business Intelligence and Predictive Analytics software shall be utilized. If this is not possible, the Contractor shall supply the appropriate Business Intelligence and Predictive Analytics software. The NDR shall also include application software to perform queries and display results in a manner conducive to analysis of RTLS data, which may include a map-based representation of tag location data over time.

Data retention time frames will vary by data type. However, the government expects the vast majority of data in NDR to be long term storage.

The Contractor shall develop the data interface between the VA RTLS databases and the NDR. The Contractor may use a data architecture other than one which transmits RTLS data from the RTLS servers to the NDR and stores a copy at the NDR.

The Business Intelligence tool(s) shall have the following capabilities:

1. Define workflows and workflow rules
2. A graphical user interface that enables an end-user to easily create, update, and delete workflows. Use of this interface shall require no more than one (1) hour of training for proficient use.
3. Associate workflow rules with the NDR
4. Run the workflows against the data within the NDR
5. Produce queries for records that do not conform to the workflow rules. Data and reports shall be visible to the NDR query/reporting functionality
6. Allow end user to publish new or updated workflows for use by other users
7. Execute workflow analysis and reporting at recurring times or on demand

If the Business Intelligence software is supplied by the Contractor, it shall allow the user to become proficient with eight (8) hours or less of instructor-led training.

If the Contractor is unable to utilize existing VA predictive analytics tools, the Contractor shall provide a COTS predictive analytics tool for data mining and predictive modeling.

The predictive analytics tool shall have the following capabilities:

1. A simple interface with which to build data sets for modeling
2. Save mining "Sets" (data plus formulas run) as individual files.
3. Auto schedule or auto run a pre-defined set of inquiries on a recurring basis.
4. No aspect of running the predictive analytics system will in any way impact the business intelligence tools or any other aspect of the RTLS
5. Design, build and implementation of any business rule based on any data element or combination of data elements from the Data Model

If the predictive analytics software is supplied by the Contractor, it shall allow the user to become proficient with sixteen (16) hours or less of instructor-led training.

5.8 Installation / Configuration / Acceptance

5.8.1 Pre-Installation site assessment

5.8.1.1 Radio Frequency Survey

Utilizing Radio Frequency (RF) spectrum analyzers, the Contractor shall analyze the RF activity in the desired frequency range that the RTLS solution will operate in to assess the current activity and potential interference. The Contractor shall analyze RF interference from the network and environment such as the current wireless RF LAN and WAN infrastructure (i.e., Wi-Fi networks, Walkie-Talkies & other types of radio transceivers, Microwave communications, satellite, etc.).

5.8.1.2 Infrastructure Survey

The Contractor shall determine the adequacy of data network connectivity that exists at the potential read points and provide detailed requirements regarding LAN drop, Wi-Fi

access, etc. The Contractor shall determine the adequacy of power that is available at the potential read points; and if no power exists, provide requirements. The Contractor shall assess the IT infrastructure available to support the RTLS solution and/or identify the additional infrastructure needed. The Contractor shall provide a visual layout of the RTLS infrastructure for each facility. The visual layout shall include, at a minimum, the following over facility blueprints: types of readers, location of readers, zonal coverage of readers, power requirements for readers, networking requirements of readers, and cabling requirements of readers.

The infrastructure survey shall consist of a full equipment/hardware list with specifications, a full software list with all specifications, compatibility and licensing requirements, interface network plans for the different RTLSs being used in the area/facility, interface network plans for the assets that will be tracked throughout the facility (in some instances area location may suffice whereas in other instances finer spatial resolution will be required with tracking to a specific room location). The Contractor shall clearly delineate any unknown VA responsibilities for acquisition and installation of items required for the facility infrastructure to successfully support RTLS applications.

5.8.1.3 Business Process Survey

At the TO level, the Contractor, in conjunction with VA, shall determine the point(s) in the business processes where RTLS will be introduced (i.e., at what points in the process should tags be read, etc.). The Contractor shall determine the physical location where reader interrogation zones should be located. The Contractor shall determine the installation points of the RTLS readers with sufficient detail to develop a construction / installation plan. The Contractor shall conduct an analysis of the points in the business processes where data must be transferred to and from the RTLS and other designated VA IT Systems. The Contractor shall provide input on how best to revise existing business processes to maximize the benefit of RTLS technology.

VA will analyze 'as is' and 'to be' business flows for each use case on each TO. The Contractor shall work with VA to finalize the 'to be' processes in order to best integrate revised business processes with the RTLS system.

5.8.1.4 Documentation

The Contractor shall provide a detailed report of the RF Survey findings and recommendations, Infrastructure Survey findings, and the Business Process Survey findings. Ultimately, the Contractor shall provide VA with Final As-Built Drawings (CADD) of the RTLS in all specified locations.

5.8.2 Site Assessment

After each TO award, the Contractor shall provide a site assessment report that includes a detailed narrative and diagrams. At minimum, the site assessment shall include a complete diagram of the entire area that shows the entire deployment of the RTLS. Site assessment scheduling shall be coordinated with the TO COR.

When a TO is awarded, the VA facility will provide the Contractor with floor plan drawings, designating distinct areas on each of the floors where RTLS coverage is required. Each area will indicate the floor number, coverage area, number of rooms, type of unit and area IDs, as well as the desired RTLS spatial resolution. The Contractor shall submit a preliminary design showing how the facility's desired RTLS spatial resolution in each given location will be achieved. The preliminary design shall include the quantity of readers required for each area and the scheme for reader connectivity with the RTLS database. All deliverables associated with this section will be identified at the TO level and will be subject to review and acceptance by the TO COR. The Contractor shall *update* facility drawings and Engineering Space Files as defined by individual TO requirements.

5.8.3 RTLS and National Data Repository Customization

The Contractor shall provide technical services to configure the RTLS to the individual local and national requirements of each installation, and NDR to national requirements, as defined in the individual TO:

1. The Contractor shall configure RTLS software to include facility-specific location identifiers, organizational identifiers and any changes required to fit the generic software to the specific installation.
2. The Contractor shall import existing inventory records and establish the association between RTLS tags and existing inventory records. The Contractor shall create an RTLS database line item for the entire inventory of tagged items, including items to be tagged that are not currently in the existing inventory system. The Contractor shall augment imported data to include data elements that are required for local RTLS reporting that are not included in the inventory management system.
3. The Contractor shall configure RTLS software and NDR to support local and national role-based access and security requirements.
4. The Contractor shall develop individualized reports and queries to support local and national reporting needs as specified in each TO. Report templates and queries shall be transportable from one RTLS installation to the next if they can meet the requirements of more than one facility. The Contractor shall create online views, maps and dashboards displaying RTLS data to meet local and national implementation requirements as defined by each TO. The Contractor shall develop modeling and analytic capabilities, as required, for local and national implementations. These capabilities shall be transportable from one facility to another if requested.
5. The Contractor shall develop additional RTLS processing modules to support emerging RTLS technologies and analysis techniques as defined by each TO.

5.8.4 Installation

The Contractor shall provide each site with a coordination activity plan, which shall include at a minimum: a description of VA responsibilities to provide utilities, networks, and any other infrastructure support required for installation and operation. The

Contractor shall submit a logistics plan for how material will be delivered to each site and stored at each facility. The Contractor shall provide a schedule, including the major milestones and durations of installation for the RTLS specified for each area/floor for concurrence by the RTLS engineer at each site. The Contractor shall provide documentation on all wiring connections between readers and the facility infrastructure. The Contractor shall install all system wiring necessary to interconnect system components (up to the point of interfacing with the VA network). Connections to the hospital data network shall be identified and quantified. The Contractor shall identify the quantity and location of data network connections at the individual TO level and shall be responsible for working with VA Staff to ensure installation of the appropriate number of network connections in the required locations. The Contractor shall install all readers as appropriate to achieve required coverage. The Contractor shall verify proper operation of the system.

5.8.4.1 Cable Installation

It is not anticipated that a significant amount of cabling will be required in support of the RTLS deployments. But whenever cabling is required, the standards below shall be followed.

The cabling installation shall adhere to the standards outlined by the National Fire Protection Association (NFPA-101 Life Safety Code). Horizontal runs are the responsibility of the contractor, to include a drop with the appropriate closet terminations, rack, patch panel terminations, and patch cord. Cable run color, AP patch cable color, and closet patch cable color will be supplied by the Facility.

The cabling installation shall follow the facility wiring standards for termination T568A or T568B (commonly referred to as 568-A or 568-B) which are specified in the current EIA/TIA – 568-B wiring standard. All Ethernet cable used to connect access points to the local area network shall be in accordance with Section 300-22(C) of the National Electrical Code (NEC). A cable drop is defined as a single Category 5E cable run from the telecommunications closet, punched down in the closet on existing patch panels to an RJ45 jack within 6 feet of the AP's designed location. In case where insufficient space is available on existing patch panels, the cabling project shall provide a patch panel that matches (to the extent possible) the existing patch panels in use at the facility.

The cable installation will follow these standards:

1. All existing cable pathways and hardware including cable trays, raceways, j hooks, conduit, other suspension media, penetrations, and openings shall be used to the fullest extent possible.
2. Cable runs shall be suspended from or attached to the structural ceiling or walls with hardware or other installation aids specifically designed to hold their weight and shall not lay directly on ceiling tiles. Cables shall not be secured to any electrical lines or conduit containing electrical wiring or any fire sprinkler system components. Cables may be attached to existing low voltage cable as long as it is not part of the fire alarm system. When no other suitable method is available

ceiling stringers may be used to support cable runs, but they must be attached using caddy clips.

3. Cables and all cable runs shall maintain a six inch (6") clearance from ceiling systems, conduits, lights and any other obstructions - when physically possible. It shall be understood that many ceilings at VA locations do not have sufficient space for a six inch (6") clearance; in those cases the cable contractor shall make their best effort to make sure the cables do not come in contact with any other obstructions
4. When a drop cable (or a number of drop cables) leaves the existing cable pathway, it/they shall be suspended by the appropriate sized j hooks or other approved suspension method (such as caddy clips on ceiling stringers) spaced at most every five feet (5').
5. A six foot (6') service loop shall be installed at the biscuit end of the cable run, unless those six feet would cause a cable length test failure. This service loop shall also be properly secured.
6. Cables leaving the existing pathways shall be run (as much as possible) parallel or perpendicular to the walls.
7. Cable labeling shall be in accordance with the TIA/EIA 606 labeling standard, using the information provided after award.
8. A Cat5e jack in a 'biscuit' shall be installed in the ceiling within six feet (6') of the device.
9. The Contractor shall punch down to either existing or new patch panels in the specified telecommunications closet.
10. The Contractor shall test the drop to normal Cat5e standards and provide test results of all drops electronically to VA in Adobe Acrobat® .pdf format. Include a separate test sheet for each cable. Paper copies are not required. Test results shall include the length of each drop and verification that the drop meets the IEEE specifications for Ethernet 802.3 communications over category 5e cabling.
11. In mental health wards, the installation shall follow the instructions in the Mental Health Areas Installation Guide.
12. The facility may specify a specific color of cable to properly identify RTLS cables.

5.8.4.2 Mounting Workstation Brackets

The Contractor shall perform the physical installation of mounting brackets at the VISN locations identified by the VA TO COR.

5.8.5 Acceptance

Inspection/Acceptance shall be conducted in accordance with FAR 52.212-4(a), Contract Terms and Conditions --Commercial Items, Inspection/Acceptance. Additional VA requirements for Inspection/Acceptance shall be defined on each subsequent task order.

5.8.5.1 Integration / Interface Testing

The Contractor shall verify that all system interfaces are operational and all data is transferred to and from the appropriate system according to the business requirement. The Contractor shall also ensure that it complies with all VA security protocols. The

Contractor shall provide VA with a copy of the integration test plan methodology, scenarios, test data, and test results.

5.8.5.2 Performance Testing

During the system testing the Contractor shall verify that the system is fully operational and meets all the performance requirements. The Contractor shall test and verify that all system functions and specification requirements are met and operational, and no unwanted effects, such as signal distortion, interference with other facility devices, etc. are present. The Contractor shall provide VA with a copy of the performance test plan methodology and test results.

5.8.5.3 User Acceptance Testing

The Contractor shall submit the test results and certification to the TO COR. The Contractor shall schedule an acceptance test date and provide VA 30 days written notice prior to the date the acceptance test is expected to begin. The System shall be tested to certify Proof of Performance. Testing shall verify that the total system meets all requirements of this specification. The notification of the acceptance test shall include the expected length (in time) of the test(s). The Contractor shall provide certified/qualified personnel to assist VA with performing this testing. The Contractor shall provide VA with a copy of the acceptance test plan methodology and test results with each TO. All warranties, as defined in paragraph 5.10.4 shall become effective upon acceptance by VA.

5.8.5.4 Documentation

The Contractor shall submit all documents as required by each subsequent task order to the COR within a timeframe that allows for proper review and acceptance of the deliverable in accordance with the due date(s) identified in the task order. For all documents, the COR will provide comment and revisions within ten (10) business days. The Contractor shall provide the COR the final updates and revisions within ten (10) business days after Government comment.

5.8.6 Standards

The standards listed in this section shall be applied when applicable--using the most recent version, respectively. If the application of more than one standard might be in conflict, the Contractor shall identify the potential issue and offer an alternative that is in the best interests of VA.

5.8.6.1 International Organization of Standardization

1. RTLS
 - a. The RTLS shall be compliant with ISO/IEC Standards for RTLS: 24730-1, 2, 3, and 5.
2. RFID

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- a. The RTLS shall be compliant with the following ISO/IEC Standards; 1800:1,3-7, 1801, 15961:1-4, 15962:1, 15963:1, 24710, 24729:3,4, 24752, 24753, 29158.
3. Bar Codes
 - a. For systems that utilize barcodes, the system shall be compliant with the following ISO/IEC Standards for testing and quality control; 15960, 15415, 15416, 15421, 15423, and 24720. The system shall be compliant with the following ISO/IEC Standards for data carrying related to bar codes; 15417, 15424, 15438, 16022, 16023, 16388, 16390, 24724, 24728, and 24778.
4. Interoperability
 - a. The proposed RTLS aligns with industry standards for interoperability ISO/IEC 24730.
5. Security
 - a. The proposed RTLS aligns with industry standards for security ISO 15693.
6. Quality
 - a. The proposed RTLS aligns with industry standards for quality. ISO/IEC TR 18046-18047.

5.8.6.2 GS1 Standard

VA recognizes the need to be compliant with the Food and Drug Administration (FDA) standards for securing the supply chain, including two unique identifiers the Standardized Numerical Identifier (SNI) for pharmaceuticals and the Unique Device Identifier (UDI) for medical supplies and devices. The only global standards noted by the FDA (footnote this link <http://www.fda.gov/RegulatoryInformation/Guidances/ucm125505.htm>) as a path to achieving this unique identification is through the standards documented in the consensus-based, not-for-profit, Global Standard (GS1) effort and utilization of Global Trade Identification Number (GTIN) that can be used for all commodities from pharmaceuticals to retail products such as food and hardware.

In an effort to support global standardization and provide a framework that allows products, services and information effective exchange, traceability and interoperability within VA and the organizations with which it interacts, the proposed RTLS system will be compliant with all applicable healthcare GS1 global standards to include:

- a. Global Location Number (GLN).
- b. Global Trade Identification Number (GTIN) allocation rules.
- c. Global Traceability Standards for Healthcare.
- d. EPCglobal Pedigree Messaging Standard.
- e. Global Data Synchronization Network (GDSN) Trade Item Extension: Healthcare.
- f. Automatic Identification and Data Capture (AIDC) Application Standard.
- g. Automatic Identification and Data Capture (AIDC) Application Standards for Small Instruments.

5.8.6.3 EPC Global

For passive RFID systems, the system shall meet the passive RFID standards defined by EPC Global.

1. Tags - For systems that utilize passive RFID, the system shall be compliant with:
 - a. EPC Global Tag Data Standards v1.5,
 - b. EPC Global Tag Data Translation v1.4,
 - c. EPC Global UHF Class 1 Gen 2 Standard v. 1.2.0
2. Reader - For systems that utilize passive RFID, the system shall be compliant with:
 - a. LLRP Standard v. 1.0.1
 - b. DCI Standard v1.0
 - c. RM Standard v. 1.0.1
3. Middleware - For systems that utilize passive RFID, the system shall be compliant with:
 - a. EPCIS Standard v. 1.0.1
 - b. ALE 1.1.1

5.9 Documentation and Training

5.9.1 Reference Documentation

The Contractor shall provide, at no additional cost to VA, updated documentation and service bulletins for all system components through the system's lifecycle. The Contractor shall provide an electronic set of user manuals and technical manuals to VA for all components of the system.

The Contractor shall provide commercial user manuals for each piece of equipment delivered. The commercial user manuals shall provide step-by-step procedures for each function performed by the equipment and shall identify all preventive maintenance tasks and troubleshooting procedures. The original commercial user manuals shall be included with each delivered piece of equipment and shall not be separately priced.

The Contractor shall provide software reference documentation to be used by software developers creating RTLS applications. The documentation shall contain specific details for the integration of RTLS equipment. The documentation shall be at a level of detail sufficient to fully define the operator interface and application operations. The original software reference documentation shall be included with each delivered piece of equipment and shall not be separately priced.

The Contractor shall document the workflows, business rules, queries and reports in the Use Case Usage Document. The Use Case Usage Document shall contain detailed instructions on how to modify or add workflows and business rules for this use case in RTLS. The Contractor shall review the Use Case Usage Documents with the COR. The Contractor shall update the Use Case Usage Document and the design based on feedback provided by the COR.

The Contractor shall also document the installation and configuration of the RTLS and NDR Systems in the VA Environment.

5.9.2 Training

The Contractor shall identify training requirements, obtain or develop training programs and conduct training for systems, applications and products throughout the life of the contract. This includes, but is not limited to, newly developed systems as well as existing deployed systems, current systems, and any updates or changes to migrated systems. The Contractor shall develop or procure training plans, manuals and other training documentation or training aids. Electronic training tools such as video conferencing and computer-based training shall be employed to enhance the effectiveness of training materials and courses. All training materials shall be available to VA staff members for the life of the contract, at no additional cost. The Contractor shall conduct training (upon installation, closure of warranty, and as purchased for ad-hock training after acceptance) for VA personnel to ensure proper operation, maintenance and testing of systems, applications and products. The Contractor shall provide training and knowledge transfer to VA technicians and other staff with regard to services and associated products delivered under any functional and or technical areas described herein. The training allows VA personnel the ability to operate, maintain, and train new staff on the product or process in the future. The Contractor shall identify and provide any additional training required by end-users, technicians, or any other VA staff for implementation, maintenance and use of deliverables specified in individual TOs.

5.9.2.1 System User Training

The Contractor shall provide training to all users on system application and use. Initial training shall be on-site. Thereafter, VA shall have unlimited access to web or computer-based training, tailored to VA configuration, at no additional cost. Education curriculum must include, but is not limited to, the following:

1. Operations and set-up
2. Report and query generation
3. User maintenance
4. User troubleshooting
5. User tips

5.9.2.2 Technical Maintenance and Repair

The Contractor shall train designated VA staff on technical maintenance and repair. The Contractor shall provide each trained VA staff member with all service tools, service keys and other diagnostic software, technical documentation, and accessories necessary to service the RTLS prior to the warranty expiration.

The Contractor shall furnish any devices required or recommended to test, calibrate, and operate / maintain / configure the system for proper operation. The Contractor shall provide service/maintenance/diagnostic software and associated security keys for in-

house service of the equipment. Where applicable, the contractor shall renew the software license or security key for the duration of the contract at a VA facility. At a minimum, the service software shall include system diagnostics down to the board or module level, error codes and definitions, and system setup capabilities to include networking, and peripheral connectivity.

5.9.2.3 System Administrator Training

The Contractor shall train designated selected VA staff for the purposes of supporting the application as a system administrator. The Contractor shall provide each trained VA staff member with all application and support tools necessary to configure and use the system. In addition, the system administrator is expected to have the knowledge after training to provide first level application support to VA users.

5.10 Support and Maintenance of RTLS

5.10.1 Help Desk

It is anticipated that VA staff members will handle initial trouble calls from end users. Issues which cannot be resolved by VA staff will be referred to the Contractor by VA technical support staff. Methods for requesting technical support from the Contractor shall include all of the following: telephone, e-mail, and web portal.

5.10.1.1 Toll-Free Customer Support Help Desk

The Contractor shall provide toll-free telephonic support for a Customer Support Help Desk. The Help Desk shall be staffed 24 hours per day, 7 days per week, 365 days per year. The Help Desk shall respond to all calls from VA technical support staff no later than 2 hours after receiving a call, at least 95% of the time. Recorded answering services are not acceptable to VA; however, the Contractor may use an on-line knowledge base, and an on-line Return Merchandise Authorization (RMA) input functionality to assist Contractor Help Desk staff in meeting the workload. Contractor personnel staffing the Customer Support Help Desk shall possess sufficient expertise to recommend troubleshooting procedures and possible corrective actions for the RTLS equipment and software. Contractor personnel staffing the Help Desk shall understand and speak fluent English. An incident/trouble ticket number shall be routinely provided to all VA callers. The Contractor shall maintain a database of calls received, action taken, and track user calls for troubleshooting assistance, capturing the following information: incident/trouble ticket number, failed component, Point-of-Contact, VA facility affected, date, problem, and resolution. This information shall be available to authorized VA staff members on-line, and provided to VA upon request.

5.10.1.2 Tier 1 Support

When VA technical support staff member submits an incident via e-mail, telephone, or web portal, the Contractor shall acknowledge the incident by providing an incident/trouble ticket number to the requestor. Help desk support via telephone call must be available in one minute on average over every one-month period. For all Tier 1 issues submitted via telephone, the call abandonment rate of shall not be greater than

3% after 30 seconds, for every one month period. All Tier 1 issues submitted via email or web portal should be responded to within 1 hour. The Contractor shall resolve all Tier 1 VA issues within 2 hours or refer to the appropriate functional or technical personnel for resolution.

It is the expectation that VA would be sufficiently trained to handle Tier 1 Support issues upon acceptance of the system.

5.10.1.3 Tier 2 Support

The Contractor shall resolve all Tier 2 incidents within eight (8) hours or escalate the incidents to Tier 3. All other requirements for Tier 1 shall apply.

5.10.1.4 Tier 3 Support

The Contractor shall provide a service report to the user/requestor within twenty-four (24) hours of all performed service for Tier 3 incidents. All other requirements for Tier 1 and Tier 2 shall apply.

5.10.1.5 Web Site

The Contractor shall establish and maintain a World Wide Web site for VA users no later than 60 calendar days after contract award. The web site shall be available daily on a 24-hour basis, for the life of the contract. The web site shall not be password protected and shall allow access to all users accessing the web site from “.gov” internet domains. At a minimum, the Web site shall include, or provide hotlinks to:

1. Warranty and maintenance support
2. Warranty maintenance tracking using the RMA number
3. Exchange technical information between the Contractor and individual users and groups
4. Point-of-Contact, telephone and facsimile number, email address and mailing address for each RC
5. Technical troubleshooting support
6. Database of all VA service calls and associated information with the ability to conduct queries and run ad hoc reports
7. Product and Services Ordering Catalog
8. Reference and user manuals (i.e. commercial manuals, technical manuals, software manuals, Frequently Asked Questions (FAQs))
9. Other data as mutually agreed to by the Government and the Contractor;
10. RTLS device drivers
 - a. Monthly Equipment and Service Report, Status Report, and Warranty Status Report

The Contractor shall ensure that all hardware device drivers for the RTLS hardware are available on the web site. At a minimum, the Contractor shall post to the web site those drivers that were developed by the Contractor for use under this Contract. Any initial drivers shall be posted to the web site no later than 60 calendar days after Notice to

Proceed. New and updated drivers shall be posted to the web site no later than 48 hours after Contractor validation. In the event that drivers are updated, the original version shall also be maintained on the web site.

5.10.2 Technical Engineering Services and Products

Technical Engineering Services (TES) shall be ordered by a TO. The Contractor shall provide TES on-site at the place of performance specified in the TO. TES shall include those services required for RTLS implementation, equipment integration, site analysis, installation, de-installation, relocation, problem-solving, user unique training, software development; communications, interfaces with other Government systems, equipment and systems engineering services and systems integration.

5.10.2.1 Software Programming, Development, Testing and Installation

The Contractor shall program, develop, test, and install RTLS software to address additional requirements on an ad-hoc basis as defined by individual TOs. When VA elects to develop reports itself, the Contractor shall provide the appropriate unlimited telephonic and email or on-line technical programming support to assist the customer software engineer or programmer during the development of RTLS and NDR applications. This support will be defined at the TO level.

5.10.3 Service Level Agreements

The Contractor shall provide the following uptime guarantees: 99.5% for business critical, 99.9% for mission essential and 99.99% for mission critical.

Business critical is defined as: A system that is necessary for the accomplishment of VA's day-to-day operations. Examples include, but are not limited to: locating of tagged items for inventory purposes, theft deterrence of assets, hand washing validation, and validation of remains.

Mission essential is defined as: A system that is basic and necessary for the accomplishment of VA's organizational mission. Examples include, but are not limited to: automated temperature monitoring, and supply tracking.

Mission critical is defined as: Vital to the operation of the VHA. A system or application that has immediate impact on the safe, effective delivery of patient care or on the safety of staff. Examples include, but are not limited to: surgical instrument tracking, SPD workflow, patient and staff safety, and patient elopement.

5.10.4 Maintenance (Warranty and after Warranty)

The Contractor shall oversee all sub-Contractor support, maintenance and warranties. The Contractor shall develop and provide on-site a list of commonly replaced spare parts in accordance with requirements of each TO. Any other parts needed for repair, shall be available and provided to the site. The Contractor shall provide documentation (service report) to the customer within 24 hours of all performed service. The Contractor shall furnish any devices required or recommended to test, calibrate, and

operate / maintain / configure the system for proper operation while under the current level of support. The Contractor shall provide Field Service Engineers (FSEs) to meet on-site support needs or field level support to provide VA with an onsite response time as per level of support, once determined that virtual support (phone or remote) cannot resolve problems. The Contractor shall sponsor an RTLS user group, consisting of all VA customers, that meets at least annually and also provide a method for the users to interact with each other on an ad-hoc basis.

5.10.4.1Warranty

The RTLS equipment, hardware, software and services shall be covered under the manufacturer's warranty and shall include all parts and labor and technical support for a minimum of one (1) year following acceptance by VA. Acceptance of any deliverables will be defined at the TO level. All warranties shall be included in the item (hardware/software/service) price and not priced separately. The Contractor shall either perform or manage all maintenance during the warranty period.

Before warranty expiration, the Contractor shall review all service-related work / failures and trending with VA for agreement to warranty conclusion. Any commercial warranties still in effect at the end of the reporting period of performance of this contract shall be transferred to the Government. The type of warranty and extent of coverage shall be determined on an individual TO basis.

5.10.4.2 Service Contract

The Contractor shall provide all maintenance, emergency service, updates and upgrades as defined at the individual TO level. The Contractor shall provide options for three levels of Service Contracts (Gold, Silver, and Share Service). Varying levels of support between the Contractor and VA shall be noted, along with response time for onsite service, turnaround time for part delivery, or any other service that can be tiered.

5.10.4.2.1 Software

Software maintenance shall be provided for all commercial software provided under this Contract in accordance with customary commercial software maintenance terms and conditions offered to the general public, to include all fixes, updates and changes necessary to maintain the software in an operational state.

The Contractor shall supply software updates, excluding VA-provided software, to the equipment at no additional charge for the life of this contract. Updates are defined as all modifications to correct or improve system operation and current functions including known remedies for safety and security vulnerabilities.

Updates to the operating system, RTLS application or NDR, which remedy bugs or defects in system function, shall be provided for the entire system for the life of this contract. If the updates are embedded with system upgrades that add additional functionality and the Contractor is unable to provide the update as a distinct deliverable separate from the upgrade, VA will not be liable for the cost.

The Contractor shall provide, coordinate, and install manufacturer recommended software upgrades and changes, at no additional charge, during the warranty term.

5.10.4.2.2 Hardware

The Contractor shall provide all parts and components needed for maintenance.. These updates shall include any circuit boards or other parts required.

5.10.4.2.3 Agreements

The Contractor shall comply with the terms and conditions of the standard VA Business Associate Agreement (BAA). The Contractor shall complete security and patient confidentiality training per VA requirements

5.11 Project Management

5.11.1 Implementation Manager

The Contractor shall provide a dedicated, experienced single point of contact (implementation manager) for the VISN, or facility (as designated in the TO), that will be responsible for the overall RTLS implementation. The Contractor implementation manager shall:

1. Develop the master project plan including project deliverables and milestones
2. Effectively communicate the project schedule and milestones to VA and Contractor team members
3. Ensure proper documentation is delivered to VA
4. Coordinate, escalate and resolve Contractor-related project issues
5. Represent the Contractor in status meetings and provide status reports
6. Be on-site during the implementation for a portion of the time during normal working hours to coordinate and manage Contractor personnel

5.11.2 Project Management Plan

The Contractor shall draft a Project Management Plan (PMP) following ProPath guidelines which will include the approach, timeline and tools to be used in execution of the contract. The PMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline PMP shall be concurred upon and updated semiannually thereafter. The Contractor shall

update and maintain the VA PM's approved PMP throughout the period of performance. In addition the PMP shall contain:

1. RTLS Configuration Management Plan
2. Risk Management
3. Product Support Plan – including methodology for supporting RTLS devices no longer available in the marketplace
4. Helpdesk Support Approach
5. Training Development and Support Management and Reporting Methodology for Gathering, Validating and Generating Reports
6. Life-cycle Management Plan
7. End of Contract Transition Plan
8. Change management plan to facilitate acceptance of business Process Workflow changes in conjunction with local RTLS Manager.

Deliverable:

Project Management Plan

5.12 Contract Management

5.12.1 Government Support

5.12.1.1 Contracting Officer's Representative (COR)

For this contract, a COR shall be designated and shall reside within the VHA RTLS PMO. The COR shall be appointed by the Contracting Officer and duties delegated in an appointment letter. Contract surveillance duties shall be defined and be in accordance with the Quality Assurance Surveillance Plan (QASP).

5.12.1.2 COR – Task Orders

For each TO a COR shall be designated and shall reside within the Requiring Activity. The COR shall be appointed by the ordering CO and duties delegated in an appointment letter. The COR is the Requiring Activity's designated representative. The COR designated for each TO shall provide the Contractor access to all available Government furnished information, facilities, material, equipment, services, among others as required to accomplish each TO. Contract surveillance duties shall be defined and accomplished in accordance with the TO QASP.

5.12.2 Contractor Support

5.12.2.1 Contractor Program Management

The contractor shall provide a Program Manager who shall serve as the manager of the contract and shall be the Contractor's single point of contact for the VA COR. The Program Manager shall be responsible for formulating and enforcing work standards, assigning schedules, and reviewing work discrepancies, communicating policies, purposes, and goals of the organization to the assigned Contractor personnel for all

projects. The Program Manager shall manage all TO performance. The Contractor shall be available to meet with the Government at the Government facilities within 24 hours notice, without added cost to the Government. This Contractor function shall handle RTLS programmatic issues, facilitate information exchange, and enhance management coordination.

The Contractor shall provide the following Program Management activities and services.

1. Timely and sustained response to program issues and problems that occur during the execution of the contract as identified by the VA RTLS PMO
2. Conduct Project Progress Reviews (PPR)
3. Provide Monthly Contract Status Report
4. Provide a Monthly Warranty Status Reports
5. Provide Monthly Equipment and Service Reports (MESR)
6. Perform risk management activities

5.12.2.2 Points of Contact

The Contractor shall provide a list of Contractor points-of-contact to the COR no later than ten calendar days after the effective date of the Notice to Proceed. The list shall include names, telephone numbers, facsimile numbers, and areas of responsibility for the Contract, addresses, and e-mail addresses. When a key point-of-contact is replaced, the Contractor shall notify the COR no later than five workdays afterward.

5.12.2.3 Work Control

All program requirements to include deliverables, contract actions and data interchange shall be conducted in a digital environment using electronic and web-based applications. At minimum, such data shall be compatible with the Microsoft Office 2003® family of products, and Microsoft Windows XP® network protocols. The Government will designate a standard naming convention for all electronic submissions within 60 days after contract award. Electronic methods for the interchange of data/documents (to include deliverables and invoices) shall be required for the duration this contract.

5.12.3 Government Rights

The Government shall have full and unrestricted rights, in accordance with copyright laws and regulations, to use and reproduce for its own use, all documentation provided under this contract. The Contractor shall provide the VA RTLS user community with online access to, including the rights to download, all user manuals and software reference documentation for any piece of equipment that interfaces with a host computer system. User manuals and software documentation shall be submitted using Portable Document Format (PDF).

5.13 Technology Refresh

The Contractor shall monitor the hardware products provided under this Contract and notify the Contracting Officer (CO) if any products are required to be refreshed. If any of

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

the products are approaching the end of their product lifetime (EOL) (e.g. if a Manufacturer will no longer be marketing, selling, or promoting a particular product and may also be limiting or ending support for said product) the Contractor shall provide notification and an Engineering Change Proposal (ECP) to the COR and CO at least 180 days prior to the EOL date. Notification can be either via email or overnight mail.

In performing technology refresh, the Contractor shall maintain the same brand name items as identified within the original Contract to the maximum extent practical.

The following conditions shall be met in performing a technology refresh:

1. The product(s) refreshed shall be fully compatible/backwards compatible with the originally provided product.
2. The product(s) refreshed shall meet or exceed the mandatory technical requirements as stated in the specifications.
3. The product(s) refreshed shall be off the shelf configurations.
4. The price of the product(s) refreshed, including support services, shall be equal to or lower than the current contract pricing for the same product. The Contractor shall agree to all terms and conditions, equal to or more favorable to VA for the refreshed item(s).

All refreshed products shall comply with VA Acceptance testing defined in this RTLS IDIQ PWS.

5.14 Technology Insertion

As new technologies are developed and used by the commercial industry or the Government, VA and/or Contractor may identify these technologies, and propose necessary additions, modifications, upgrades, enhancements, and improvements to the current Contract hardware scope. The Contractor shall translate the technology insertion recommendation into a formal ECP as directed by the CO.

All inserted products shall comply with VA Acceptance testing defined in this RTLS IDIQ PWS.

The Contractor shall inform VA in advance of any known, or potential changes, in cost of ownership pursuant to technology refreshments, insertions, or other changes to the RTLS. The Cost of Ownership change shall be quantified and communicated to VA at the earliest possible date.

5.15 Engineering Change Proposals (ECP)

Technological changes over time may result in the need to update the Hardware being provided to VA. To ensure that these changes are properly documented and managed the contractor shall submit a Configuration Management Plan for Government approval as part of its proposal. As part of this plan the Contractor shall be required to submit Engineering Change Proposals (ECPs) for Technology Refreshing and/or Technology Insertion to the COR and Contracting Officer (CO). Application of ECPs applies to

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

future equipment deliveries. That is, the Contractor shall not be required to retrofit already installed equipment unless the proposed change corrects a problem or hazard with the existing installed equipment.

An ECP is a proposed engineering change and the documentation by which the change is described, justified, and submitted to VA for approval or disapproval.

There are two (2) classifications of ECPs as defined below.

Major ECP

Major ECPs apply to:

1. Products introduced by VA or the Contractor that result from the requirement for Technology Insertion
2. Products provided by the Contractor that have undergone major component, configuration, and/or system changes
3. Any introduced product or product change that MAY impact the ability to meet performance specifications, the connectivity and/or interoperability with current VA systems
4. Any product change that will result in a change in price or negatively impact delivery schedule.

The CO may ask the Contractor to prepare a Major ECP for Hardware within scope of this contract. Upon receipt of a written request from the CO, the Contractor shall prepare and submit an ECP in accordance with the information provided below.

The Contractor may also initiate a Major ECP. Any Major ECP submitted to the CO shall include "not-to-exceed" (price or estimated cost and delivery or period of performance) adjustments, if any, prior to issuing an order for implementation of the change.

After submission of a Contractor-initiated Major ECP, the CO may require the Contractor to submit the following information:

1. Cost or pricing data in accordance with FAR 15.403-5 if the proposed change meets the criteria for its submission under FAR 15.403-4
2. Information other than cost or pricing data adequate for CO determination of price reasonableness or cost realism. The CO reserves the right to request additional information if that provided by the Contractor is considered inadequate for that purpose. If the Contractor claims applicability of one of the exceptions to submission of cost or pricing data, it shall cite the exception and provide rationale for its applicability.

A Major ECP submitted to VA for approval shall contain information as required at section C.6.10 of this contract and the following information:

1. Title
2. Originator Information
3. Hardware Identification

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

4. Description of Problem/Deficiency
5. Justification for Change
6. Description of Proposed Solution / Alternative
7. Supporting Information
8. Prepared By
9. POC Information

Minor ECP

Minor ECPs apply to:

1. Any minor component, configuration, and/or system change that DOES NOT impact the ability to meet performance specifications, connectivity and/or interoperability with current VA systems
2. Model Number Changes

The Contractor may initiate a Minor ECP. All Minor ECPs shall be submitted to the CO as a notice that a minor change has taken effect and does not require CO approval.

A Minor ECP provided to VA shall contain information as required at section C.6.10 and the following information:

10. Title
11. Originator Information
12. Hardware Identification
13. Description of Problem/Deficiency
14. Justification for Change
15. Description of Proposed Solution / Alternative
16. Supporting Information
17. Prepared By
18. POC Information

5.16 Certification and Accreditation

The Contractor shall develop a system certification and accreditation plan in accordance to the agency's security policies, procedures and regulations. VA 6500 Handbook, the agency's Information Security Program, should be the primary source for certification and accreditation compliance. This shall be done with cooperation and approval from an assigned agency Information Security Officer (ISO) and an agency OI&T Service, Delivery, and Engineering (SD&E) representative. The Contractor shall also execute and provide all necessary data, files, documents to the agency with the goal of attaining both a security and an operational system certification as well as meeting all operational readiness requirements. The Contractor shall ensure that all hardware and software meets all VA certification requirements needed to deploy them within the VA network. Final documentation from VA certifying that the project has authority to operate shall be the major output of this task. A Certificate of Authority to Operate is issued by VA.

6.0 REPORTING REQUIREMENTS

The deliverables defined below are required for the base contract and each TO and shall be provided in accordance with paragraph 5.12.2.3 (Work Control). The base contract report shall be a rollup of each TO and shall be delivered to the CO and the COR. Each individual task order report shall be delivered to the COTR/COR for that Task Order. Any differences between the requirements for the overall basic contract report versus the task order report are noted below. Each deliverable is required by the 15th day of each month. The deliverables shall also be forwarded electronically to the VA TAC website, once established.

6.1 Monthly Contract Status Report

The Contractor shall prepare and submit a Status Report in Microsoft Office Excel format not less than once a month. VA may request reports more frequently, as needed. This report shall convey the status of all TOs awarded as of contract inception as well as cumulative contract performance. All relevant billing information shall be posted to the VA TAC website. TOs that are completed shall be listed as such. A standard format shall be utilized for submission of the below required information. This report is required at the basic contract level and shall be a rollup/summary of each TO. In addition, the Contractor shall provide a monthly individual TO report. The TO report shall be unique to that TO only.

A. For Each TO, indicate/discuss:

1. TO summary
2. Performance metrics
3. TO schedule
4. PMAS Compliancy (as applicable)
5. Critical items for Government review
6. Accomplishments
7. Significant open issues, risk and mitigation action
8. Summary of issues closed
9. Meetings completed
10. Projected meetings
11. Subcontractor performance – discuss 1st tier Subcontractors and Contractor performance
12. Projected activities for next reporting period
13. Explanation if the reporting period is over one month
14. Receiving report submitted
15. Milestone payment schedule
16. Automated bill of materials in data base format

B. General and Cumulative Performance. Indicate the following:

1. Any general meetings that occurred with Government representatives during the reporting period
2. Total dollars awarded to date (ceiling)
3. Total dollars invoiced to date, by fiscal year, and since contract award

C. Performance Metrics

1. Schedule Performance to Plan

Deliverable:

Monthly Contract Status Report

6.2 Status of GFE Report

This report is required at the base contract and shall be a rollup/summary of each TO. The overall base contract report shall show the detail for each TO with a summary column for the entire program. In addition, the Contractor shall provide a monthly individual TO report. The TO report shall be unique to that TO only. This report shall include:

1. TO Number
2. Project Name
3. Type of Equipment
4. Tracking Number
5. Location
6. Value
7. Total Number of Pieces
8. Total Value of Equipment
9. Anticipated Transfer Date to Government
10. Anticipated Transfer Location
11. The Government Furnished Equipment Report

Deliverable:

Status of GFE Report

6.3 Personnel Contractor Manpower Report

This report is required at the base contract and shall be a rollup/summary of each TO. The Contractor shall provide a Personnel Report (MS Excel), on a monthly basis listing all personnel working at a VA facility or accessing VA networks under each Task Order. As personnel changes occur, a revised report is required only for the individual Task Order affected for Background Investigations. The overall basic contract report should only be updated on the monthly basis. The overall basic contract report shall show the detail for each task order with a summary column for the entire program. The individual task order report will be unique to that task order. The information required is as follows:

1. Task Order
2. Name
3. Clearance level and/or Status

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

4. Company name
5. Prime/Subcontractor
6. Labor Category
7. Facility location
8. Tour of Duty Schedules (e.g. Monday through Friday, 9:00 am to 5:00 pm)
9. Project supporting
10. Contractor Rules of Behavior
11. VA Cyber Security Awareness and Rules of Behavior Training
12. Annual VA Privacy Training
13. The Personnel Contractor Manpower Report as set forth in Section D, Attachment 012(basic) and 013 (task order), shall be submitted monthly via the VA TAC website or the CO.

Deliverable:

Personnel Contractor Manpower Report – Basic
Personnel Contractor Manpower Report – Task Order

6.4 Monthly Equipment and Service Report

The Contractor shall provide the TO COR with a Monthly Equipment and Service Report (MESR) in Microsoft Excel format via electronic mail. The initial MESR shall be submitted covering the month the first RTLS item is received by the Contractor for repair (warranty or maintenance), and shall be provided no later than 10 calendar days after the end of each subsequent month i.e., January report is due by 10 February. The Contractor shall provide, as part of the MESR, a consolidated list of service user calls for troubleshooting assistance. This detailed information on warranty and maintenance repairs will be used to identify trends and compliance with equipment turn-around requirements. The MESR shall include a separate line item of description for each of the RTLS item service incident and, as a minimum, shall include the following:

1. RMA number and date assigned to user Category of service action: Per-incident maintenance, Monthly Maintenance, On-call maintenance or Warranty
2. Parts breakout: nomenclature; National Stock Number (NSN), when available; part numbers; model number, CLIN; and serial number
3. Quantity of each type of component repaired or replaced by CLIN under the Contract to date
4. Equipment warranty expiration date
5. Equipment maintenance start date and expiration date for monthly maintenance;
6. Date field engineer arrival on-site, or receipt of the failed RTLS equipment at the repair facility
7. Date repair action was completed, or equipment was sent back to the user, shipper or carrier
8. Remarks section providing information outside of the items listed above, which gives a brief, non-technical description of equipment problems identified, repair action accomplished, parts replaced, serial numbers of replacement items

(when the item was replaced by the Contractor), problems identified but causes not isolated, or a statement of no evidence of failure

Deliverable:

Monthly Equipment and Status Report – Task Order

6.5 Warranty Status Report

The Contractor shall provide a Warranty Status Report in Microsoft Excel format to the TO COR, at the end of the warranty period, to include but not limited to, a list of all equipment due to leave warranty status within the next twelve months with serial number, model number, acceptance date, warranty end date, point of contact and telephone number. The initial report format shall be provided by the Contractor for VA review and approval no later than 30 calendar days after issuance of the Contract effective date specified in the Notice to Proceed. The Warranty Status Report shall include a separate line item of description for each of the RTLS item service incident and, as a minimum, shall include the following:

1. RMA number and date assigned to user Category of service action: Per-incident maintenance, Monthly Maintenance, On-call maintenance or Warranty
2. Parts breakout: nomenclature; National Stock Number (NSN), when available; part numbers; model number, CLIN; and serial number
3. Quantity of each type of component repaired or replaced by CLIN under the Contract to date
4. Equipment warranty expiration date
5. Equipment maintenance start date and expiration date for monthly maintenance;
6. Date field engineer arrival on-site, or receipt of the failed RTLS equipment at the repair facility
7. Date repair action was completed, or equipment was sent back to the user, shipper or carrier
8. Remarks section providing information outside of the items listed above, which gives a brief, non-technical description of equipment problems identified, repair action accomplished, parts replaced, serial numbers of replacement items (when the item was replaced by the Contractor), problems identified but causes not isolated, or a statement of no evidence of failure

Deliverable:

Warranty Status Report – Task Order

6.6 Small Business Participation Report

This report is required at the base contract and shall be a rollup/summary of each TO. In accordance with Small Business Participation Requirements (reference section C, clause C.6.6), The Contractor shall submit the Small Business Participation Report on a quarterly basis to the CO.

Deliverable:

Small Business Participation Report

6.7 MEETINGS AND REVIEWS

For successful management and contract surveillance, the following meetings and reviews are required.

6.7.1 Post Award Conferences

The Government intends to convene a Post-Award Conference within 40 days after contract award to review the PWS, business policies, and procedures, and introduce personnel. The CO shall notify the Contractor of a specific date, location and agenda within 7 days after contract award.

6.7.2 Task Order Kickoff Meetings

As required by the designated COR, and CO, a kickoff meeting may be held on the TO level after award. Dates, locations, and agenda shall be specified at least five (5) calendar days prior to the meeting.

6.7.3 Project Progress Reviews

The Contractor shall conduct Project Progress Reviews (PPRs) for Government personnel at a mutually agreeable facility. The CO or the COR will schedule the initial PPR. It is anticipated the first PPR will occur no later than 90 calendar days after date of contract award. Thereafter, PPRs shall occur quarterly, for the life of the Contract. During each PPR, the Contractor shall present material that addresses:

1. Status of current technological substitutions and additions
2. Status of configuration and risk management activities
3. Status of TOs, to include but not limited to, received and processed dates (listed by Requiring Activity), scheduled delivery date, and shipped date and period of performance for services
4. Actions under warranty and maintenance
5. Significant trends (quantities by CLINs, component reliability safety issues, problems, and recommended solutions)
6. Minutes from the previous PPR
7. Activities determined to be of importance to VA, such as unanticipated problems, and high visibility issues identified by VA;
8. Status of significant program events
9. Customer feedback
10. VA organizations contacted and initiatives with each; and
11. Reasons for delinquent TOs

6.7.4 Organizational Chart

The Contractor shall include in each review, a current organizational chart that includes the names and telephone numbers of all key Contractor personnel, and any key personnel changes highlighted. The Contractor shall prepare and coordinate with the COR, an agenda for all PPRs at least five workdays before a scheduled PPR. The

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

Contractor shall provide the briefing charts to the COR electronically at least three workdays prior to the day of the PPR. The Contractor shall prepare and coordinate minutes of the PPRs with COR no later than five workdays after the PPR. Coordination shall be done through electronic mail. Upon COR approval, the Contractor shall, have no more than five workdays to distribute electronic copy of the minutes to COR and CO.

Deliverable:

Organization Chart
Agenda and Minutes of the PPR

7.0 SECURITY

7.1 Systems Security

The Contractor(s) shall comply with all the physical and data security policies of the ordering activity. Copies shall be made available as part of the RTEP process.

7.2 Personnel Security

The Contractor(s) shall comply with all personnel security requirements included in this contract and any unique organization security requirements described in each TO.

7.2.1 Position Risk Level and Contractor Personnel Security Requirements

1. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access will be determined at the TO level. It is anticipated there may be requirements at the Low, Moderate, and High levels for this contract. The levels of access are:

- ☐ Low/NACI
- ☐ Moderate/MBI
- ☐ High/BI

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.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Moderate	Minimum 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.

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. For a Low Risk designation the following forms are required: 1.OF-306 and either 2. DVA Memorandum – Electronic Fingerprints or FD-258 Fingerprint card. For Moderate or High Risk the following forms are required: 1. VA Form 0710 and either 2. DVA Memorandum – Electronic Fingerprints or FD-258 Fingerprint card. These should be submitted to the CO or COTR after award has been made.
- d. Within 3 days after award, the Contractor shall provide a staff roster to the CO and COTR to enable the initiation of the Electronics Questionnaire for Investigations Processes (e-QIP) to begin their background investigations.
- e. The Contractor personnel will receive an email notification from the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85 or SF85P). 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).

- f. The Contractor is to sign the signature page and send to the COTR and CO for electronic submission to the Security and Investigations Center (SIC).
- g. 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.
- h. If the background investigation is not completed prior to the start date of the contract, the Contractor employee may work on the contract once the investigation has been initiated and sent to the OPM. 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 databases of either the OPM or the Defense Industrial Security Clearance Organization (DISCO).
- i. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration in working under the contract.
- j. Failure to comply with the Contractor personnel investigative requirements may result in termination of the contract for default.

7.2.2 Security Requirements

The following security requirement must be addressed regarding Contractor-supplied computer equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. (i.e. any device capable of processing or storing digital data) for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) Equipment will meet all sanitization requirements and procedures before disposal as per VA policy (hard drives will not be returned). The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

- 2. Information made available to the Contractor/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).
- 3. 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.
4. 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 CO within 30 days of termination of the contract.
 5. 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 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.
 6. 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.
 7. 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 FAR part 12.
 8. 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.
 9. 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 CO for response.
10. 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 CO for response.
 11. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is to be determined at the TO level.

7.2.3 Organizational Conflict of Interest

All functions related to Acquisition Support shall be on an advisory basis only. Please be advised that since the awardee of this contract will provide systems engineering, technical direction, specifications, work statements, and evaluation services, some restrictions on future activities of the awardee may be required in accordance with FAR 9.5 and the clause entitled, Organizational Conflict of Interest. The Contractor and its employees, as appropriate, shall be required to sign Non-Disclosure Agreements (Attachment E)

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.¹ 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 and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

The following security requirement must be addressed regarding Contractor supplied equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COTR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates the security clause VAAR 852.273-75 by reference as though fully set forth therein, as well as the VA Handbook 6500.6, "Contract Security," March 12, 2010, in its entirety. Both the security clause VAAR 852.273-75 and the VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses identified on the current external VA training site, the Employee Education System (EES), and will be tracked therein. The EES may be accessed at <https://www.ees-learning.net/librix/loginhtml.asp?v=librix>. If the decision is made by the local Program Office to provide the Contractor a VA Talent Management System (TMS) account, the Contractor shall use the VA TMS to complete their mandatory training, accessed at <http://www.insidetms.va.gov/>

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.

A2.0 VA Enterprise Architecture Compliance

¹ See VAAR 852.273-75 referenced *infra*.

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). The VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1 VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

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.

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.access-board.gov/sec508/standards.htm>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

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

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The Contractor and their 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 and their personnel shall wear visible identification at all times while they are on the premises.
2. The VA does not provide parking spaces 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. The 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 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.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of the VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by the VA.
7. Contractor must adhere to the following:

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
 - h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

ADDENDUM B

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

B1. 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.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

1. 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.
2. 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.
3. 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.
4. 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, 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.
5. 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.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. 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 the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.
4. 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.
5. 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.
6. 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.
 7. 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 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
 8. 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.
 9. 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.
 10. 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.
 11. 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.
 12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service 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.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

1. 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, *VA Information Security Program*). 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, *VA Privacy Impact Assessment*.
2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.
3. 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.
4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
5. 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*.
6. 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.
7. The Contractor/Subcontractor agrees to:
 - a. 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:
 - i. The Systems of Records (SOR); and

- ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;
 - b. 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
 - c. 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
8. 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.
- a. "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.
 - b. "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.
 - c. "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.
9. The Contractor 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 Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that Security Fixes shall not negatively impact the Systems.
10. The Contractor 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.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the Contractor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.
12. 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.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

1. 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.
2. 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.
3. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* 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 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.

4. 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. 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 C&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 C&A would be necessary.
5. 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.
6. 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.
7. 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 the 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.

8. 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 Contractor at the end of lease, for trade-in, or other purposes. The options are:
 - a. Contractor must accept the system without the drive;
 - b. 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
 - c. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
 - d. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;
 - i. The equipment Contractor 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
 - ii. 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.
 - iii. 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.

B6. SECURITY INCIDENT INVESTIGATION

1. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security 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.
2. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information

involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

3. 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.
4. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA 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.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.
2. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.
3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
 - a. Nature of the event (loss, theft, unauthorized access);
 - b. Description of the event, including:

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- i. date of occurrence;
 - ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
 - c. Number of individuals affected or potentially affected;
 - d. Names of individuals or groups affected or potentially affected;
 - e. 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;
 - f. Amount of time the data has been out of VA control;
 - g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - h. Known misuses of data containing sensitive personal information, if any;
 - i. Assessment of the potential harm to the affected individuals;
 - j. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
 - k. 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.
4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of \$37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
- a. Notification;
 - b. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
 - c. Data breach analysis;
 - d. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
 - e. One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
 - f. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. 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.

B9. TRAINING

1. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
 - b. Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
 - c. Successfully complete *VHA Privacy Policy Training* if Contractor will have access to PHI;
 - d. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
 - e. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access
2. 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 1 week of the initiation of the contract and annually thereafter, as required.
3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

ADDENDUM C

Acronyms

AAA	Authentication, Authorization, and Accounting
AEMS/MERS	Automated Engineering Management System/ Medical Equipment Reporting System
AITC	Austin Information Technology Center
ALE	Application Level Events
API	Application Program Interface
ARRO	Acquisition Rapid Response Office
BAA	Business Associate Agreement
BCMA	Barcode Medication Administration
BI	Background Investigation
CADD	Computer Aided Design and Drafting
CATH	Cardiac Catheterization
CLIN	Contract Line Item
CMOP	Consolidated Mail Outpatient Pharmacies
CO	Contracting Officer
CONUS	Continental United States
COOP	Continuity Of Operations Plan
COR	Contracting Officer's Representative
COR	Contracting Officer's Technical Representative
COTS	Commercial Off The Shelf
CPR	Contract Performance Report
CPRS	Computerized Patient Records System
CPU	Central Processing Unit
DCI	Display Control Interface
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
EIL	Electronic Inventory List
EIT	Electronic and Information Technology
EMR	Electronic Medical Records
EPC	Electronic Product Code
EPHI	Electronic Protected Health Information
ERP	Enterprise Resource Planning
ESPPP	Enterprise Strategy, Policy, Plans & Programs
EST	Eastern Standard Time
EVMS	Earned Value Management System
FAR	Federal Acquisition Regulations
FAQ	Frequently Asked Question
FCC	Federal Communications Commission
FDCC	Federal Desktop Core Configuration
FFP	Firm Fixed Price

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

FOUO	For Official Use Only
FIPS	Federal Information Processing Standards
FSE	Field Service Engineer
FTR	Federal Travel Regulations
FY	Fiscal Year
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GOE	Government Owned Equipment
GOTS	Government Off The Shelf
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
IAW	In Accordance With
ICD	Interface Control Document
ID	Identification
IDIQ	Indefinite-Delivery/Indefinite-Quantity
IEC	International Electrotechnical Commission
IFCAP	Integrated Funds Control, Accounting and Procurement
IP	Intellectual Property
ISA	Interim Security Agreement
ISO	Information Security Officer
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LLRP	Low-Level Reader Protocol
LMS	Learning Management System
LOE	Level of Effort
MATO	Multiple Award Task Order
MBI	Moderate Background Investigation
MCSR	Monthly Contract Status Report
MESR	Monthly Equipment and Service Report
MWSR	Monthly Warranty Status Report
MOU	Memorandum of Understanding
MRI	Magnetic Resonance Imaging
MUMPS	Massachusetts General Hospital Utility Multi-Programming System
NACI	National Agency Check Inquiry
NARA	National Archives and Records Administration
NDI	Non-Developmental Item
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NMDR	National Middleware and Data Repository
NSN	National Stock Number

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

OA&M	Operations, Administration, and Maintenance
OCONUS	Outside the Continental United States
ODC	Other Direct Cost
PO	Purchase Order
PC	Personal Computer
PDF	Portable Document Format
PHI	Protected Health Information
PII	Personally Identifiable Information
PMAS	Program Management Accountability System
PMO	Project Management Office
PMP	Project Management Plan
PPR	Project Progress Review
PWS	Performance Work Statement
RF	Radio Frequency
RFID	Radio Frequency Identification
RM	Release Management
RMA	Return Merchandise Authorization
RSD	Requirements Specification Document
RTEP	Request for Task Execution Plan
RTLS	Real Time Location System
SCM	Supply Chain Management
SDD	System Design Document
SP	Special Publication
SPD	Sterilization, Processing, and Decontamination
SQL	Structured Query Language
TAC	Technology Acquisition Center
TCP/IP	Transmission Control Protocol/Internet Protocol
TEP	Task Execution Plan
TES	Technical Engineering Services
TO	Task Order
TRM	Technical Reference Model
TRMSP	Technical Reference Model/Standards Profile
UHF	Ultra-High Frequency
USA	United States of America
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VISN	Veteran Integrated Service Networks
VistA	Veterans Health Information Systems and Technology Architecture (VA hospital information system)
VAMC	Veterans Affairs Medical Center
VPN	Virtual Private Network
WAN	Wide Area Network

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

Wi-Fi	Wireless Fidelity (conforming to the IEEE 802.11 standard)
WIP	Work In Progress
WMS	Warehouse Management Systems
XML	Extensible Markup Language

ADDENDUM D

Specific Functional and Non-Functional Requirements

The attached Requirements Specification Document contains the Functional and Non-Functional Requirements for the RTLS software. Hardware requirements are found throughout this PWS and other Task Orders.



RTLS RSD
2-16-12.doc

ATTACHMENT A: RTLS USE CASES

1.0 VHA SPECIFIC USE CASES

The solution(s) for all Use Cases listed below shall have the capability to incorporate aspects of patient and staff tagging. When patient or staff tagging is required, the following integrated capabilities shall be provided:

- *VA Database Interfaces Required*
 - VistA
 - PIV
 - iMed Consent
 - *Technology Considerations*
 - Passive tagging - Staff
 - Active tagging - Staff
 - *System Functionality*
 - Room or bay level coverage to track staff/patient movement
 - Ability to associate staff with other tagged items or performed tasks
 - Ability to be tracked throughout facility
 - Ability to alerting for patient/staff safety
1. System shall have the ability to locate staff/ patient in real-time with the individual's explicit knowledge. The goal of the technology will be to identify bottlenecks in the treatment/administrative processes such that process improvements can occur.
 2. Patients shall be tracked to allow for capture their progression from point of admission to discharge while simultaneously alerting family and staff of their status and location
 3. Reports generated by selected system shall also be used to improve communications, scheduling of activities/resources, and facilitation of patient flow.
 4. Time accounting for contract staff - the system shall assist in validation of contract staffing invoices by tracking when staff enter and exit facilities.
 5. The system shall have the capability of producing "spaghetti diagrams" for time analysis studies (graphical and time series positions).
 6. During a declared emergency, the system should rapidly detect staff and patient locations and monitor their movement to a safe location. System shall monitor progress of staff/patient movement and provide an alert if specific staff/patient location criteria are not met within a defined time period.
 7. The system shall have the capability to enable real time and retrospective analysis of an infectious patient's contacts with other patients and staff.
 8. The system will assist in identifying patients who are not in their rooms and experience urgent medical assistance
 9. System shall link into other areas of RTLS to provide updates to expendable products or equipment used on the patient where applicable.

1.1 Cardiac Catheterization Lab Supplies Use Case

1.1.1 Consumables Tracking

- VA Database Interfaces Required
 - GIP
 - Cart-CL
- Technology Considerations
 - Passive tagging
 - Active tagging
- System Functionality
 - Room level coverage to track supply room assets
 - Cabinet based inventory tracking with interface to above mentioned systems
 - Server based inventory management

Tracking of consumables is seen as a complex environment with multiple system interfaces and capabilities. The effective end goal is to implement a system that automates the inventory management process therefore reducing the effective level of effort exerted by facility staff, enhancing the granularity of consumables tracking and reducing the amount of errors with respect to patient-consumable/implant interaction. Functionality of said ideality is achieved through implementation of a wide range of possible technologies. The combination of technologies required to obtain the desired environment is acceptable when considering possible solutions. Expected outcomes from implementing RTLS in the Cardiac Catheterization Lab are expected to allow for the following benefits:

Benefit Name	Metric #	Metric Name
Improve Staff Efficiency	2.1	Reduce Level of Effort to perform supply inventory
Improve Managerial Decision Support	3.1	Reduce Turn over time of room between patients
	3.2	Number of instances in which supplies fell below a predetermined par level
Reduce Inventory and Equipment Costs	4.1	Track and reduce Supply Expiration Expenses
Improve Staff Satisfaction	5.1	Improve Staff Satisfaction
Improve Data Quality	6.1	Automate and improve Data Entry Compliance into CART
	6.2	Improve Door to Balloon Time measurement accuracy and reduce time.
	6.3	Automate and Improve time to complete FDA MedWatch Reporting Compliance

Implementation of a system shall be designed in the following fashion in order to enable the ability to track defined metrics.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

1. Tracking of consumables/implants (*biological and nonbiological*) begins at the cath lab storage area where hospital staff enters new consumables/implants into the installed RTLS hardware. Application of passive RFID tags is completed on the packaging of all consumables/implants not pre-equipped with passive tags by manufacturers.
2. Use of passive technology is required. Passive tags will be required to maintain at a minimum, manufacturer, model, serial number, batch or lot number, Unique Device Identifier (UDI) cost and expiration date. All electronic information will be interfaced with GIP.
3. Storage areas in all Cath and EP labs will be equipped with RTLS, providing capability of tracking consumables/implants exiting and entering the area, and interfaced to hospital GIP for inventory management and cabinet level RTLS components.
4. At the cabinet level components systems will require interface capability with Clinical Procedures, VistA/CPRS, Cart-CL and GIP. Patient procedural information will be used from Clinical Procedures to generate a work list for initiating patient exams. Once an exam is started, all consumables removed and not returned to the cabinet will be electronically tied to that patient's medical record in VistA/CPRS. The same information from used consumables/implants will also interface with Cart-CL for physician generated reports.
5. Cabinets will require user authentication to remove supplies.
6. Power failures will be logged as events in the system and upon power restoration update the inventory system.
7. Active management of consumables/implants expirations will be an additional functionality of the provided hardware/software.
8. Alert management will be interfaced with the hospital's email system and/or other communication systems.
9. The system shall allow hospital staff to generate reports that identify patients associated with recall notices on medical inventory such as pacemakers, defibrillators and stents.
10. The system shall allow hospital staff to generate reports that identify recalled items by patient name, address, patient status, attending physician, date of procedure, part number.
11. The system shall support medical procedure preparation by allowing hospital staff to generate reports that compare the Cath/EP Lab actual inventory to the operating procedure required inventory.
12. The system shall allow hospital staff to generate reports that identify all instances in which there was a reported device failure.
13. The system shall allow hospital staff to generate reports that identify the nearest location of required inventory for a procedure that is missing from the Cath/EP Lab.
14. The system shall allow hospital staff to generate reports that provide inventory delivery date, use date, expiration date, ID of the patient the inventory was used on, remaining inventory levels, inventory order status, and inventory replenishment alerts.

15. The System shall track data for all disposable inventory used for Catheterization and EP procedures (e.g. stents, catheters, pacemakers, balloons, guide wires). Information shall include:

- a. Current available inventory by type, manufacturer and location
- b. Inventory status reflecting if it is owned, consigned, leased, or rented.
- c. Inventory status reflecting where inventory was purchased, acquired, leased or rented from
- d. Dollar value of current available inventory by type, location, category, and in total
- e. Inventory used by location, patient, medical team.
- f. Inventory disposed of due to defects, contamination, expiration, etc.
- g. Inventory lost or stolen
- h. Inventory with a recall notice associated with it

1.1.2 Environment Workflow Enhancement

- Interfaces Required
 - Hospitals electronic paging system
 - Hospitals email system
 - Hospital Cath/EP scheduling system
- Technologies Considered
 - Active tagging
 - Passive tagging
 - Customizable asset tags with multiple alert buttons/indicators
- System Functionality
 - Tag to Tag association
 - Electronic alert functionality from tag through above mentioned interfaces
 - Server based database with automated report functionality, customizable by user

The ability to streamline communication between multiple service lines requires an active RTLS environment with the ability to track thousands of assets and people throughout the hospital. By enabling the ability to accurately track events through use of activity based time stamps, workflow analysis will be greatly enhanced. Further reduction in the necessary human process steps to make an order to facilitate the transitional periods of daily procedures will reduce the amount of time need to prepare exam rooms for patient procedures and reduce errors.

1. An effective system will provide capability of actively tracking hospital staff, inpatients and outpatients while providing interfaces with the hospitals electronic paging system, hospital email system and hospital Cath/EP scheduling system.
2. Provided system will allow for tag to tag associations, accuracy at minimum guaranteed to within 5 feet, and automated alerting capability, interfaced with hospital electronic paging system, email system and Cath/EP scheduling system.

3. Through the use of active or passive asset tags, preset alerts will be enabled to automate notifications to facility staff to indicate when and where transport staff and transport equipment are needed and when and where environmental staff and equipment are needed. The system shall track the time a patient or multiple patients enters a medical procedure area, starting from patient preparation and ending with patient readmission to ICU or nursing ward.
4. The system shall allow hospital staff to generate reports that track the time a patient or multiple patients enters a medical procedure area, starting from patient preparation and ending with patient readmission to ICU or nursing ward.
5. The system shall allow hospital staff to generate reports that provide device picture or icon, building, floor, and room location, device sterilization status, maintenance and recall status, manufacturer, model, vendor, and age.
6. The system shall allow hospital staff to generate reports that identify the number of events where procedures were delayed due to inventory issues in the Cath/EP room.
 - a. The report shall include the following information; Cath/EP room, items missing, medical team, patient, time elapsed until procedure occurs.

1.2 SPD Workflow Use Case



VHA SPD Business
Use Cases_103111.p

- VA Database Interfaces Required
 - AEMS/MERS
 - VistA/CPRS
- Technology Considerations
 - Passive tagging
 - Active tagging
 - 2D Bar-coding
- System Functionality
 - Workstation level coverage to track processes with an open environment (will need to track tags at individual workstations within 1 room)
 - System must work within a large open environment with multiple stainless steel surfaces with various orientations (walls, floors, tables, equipment, ceilings, etc.)
 - System will allow for consolidated ad-hoc and pre-defined reporting packages from RTLS systems and compatibility with common business intelligence tools for further analysis, like SAS, Microsoft Business Intelligence, etc.
 - SQL/ORACLE database interoperability and interfacing with other SQL/ORACLE systems

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- Ability to interface with HL7-based information systems from medical device host systems
- System should interface with medical center-based reusable medical equipment (RME) Reprocessors, washer/disinfectors, as well as with Steam, Ethylene Oxide, Ozone, Paracetic Acid, and Hydrogen Peroxide Plasma Sterilizers.
 - This data should be stored locally and not required to be exported outside of VA and returned through firewalls, etc.
 - Data should remain in the custody of VA and not subject to subscription fees, etc. for accessibility.
 - System should provide every effort to facilitate VA's goals aligned with achieving a paperless environment.

Use case goal is to ensure the safety of staff and patients by providing a reasonable assurance that all processes were followed according to manufacturer instructions for individual instruments and other Critical and Semi-Critical (CDC – Spaulding Classification) reusable medical equipment (RME). In addition, this application should help an SPD department automate, and improve processes, documentation, and efficiencies. Slight to significant variances to SPD processes will be present at each site due to physical layout and current work flow practices. VHA intends to standardize these processes enterprise-wide as much as possible throughout implementation via systems redesign efforts in collaboration with the Contractor.

Expected outcomes from implementing RTLS in the SPD workflow are expected to allow for the following benefits:

Benefit Name	Metric #	Metric Name
Improve Patient Care	2.1	Number of Negative Outcomes (Safe and Effective RME use) from SOARS Inspections reduced or negated
Improve Staff Efficiency	3.1	Call Volume to SPD for Equipment Requests are reduced or negated
Improve Managerial Decisions Support	3.2	Length of time RME/instruments are waiting to be cleaned/processed
	4.2	Instrument Processing Time is able to be tracked, standardized, and reduced.
Reduce Inventory and Equipment Costs	4.3	Reusable Medical Equipment Utilization Rate is increased.

Additional assurances should include:

1. Solution(s) provides set and item (RME/instrument) tracking as a result of RFID, or similar technology for scanning at various checkpoints.
 - a. A hands-free RFID solution is preferred over existing 2D data matrices and will be scored accordingly (See 1.2 “Technology Considerations”)

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

2. Any staff badges required to measure workflow shall be predominantly hands free. Workflow processes are attached, and shall be measurable at all sites in real time.
3. Ergonomics of solution(s) should be considered to reduce the possibilities of repetitive motion injuries to staff to the greatest extent possible.
 - a. Repetitive button pushing or trigger pulling are seen by VA as a liability that the Contractor should mitigate within their proposed solution.
4. RME Inventory Control/Management:
 - a. The system shall allow hospital staff to generate reports identifying reusable medical equipment that is assigned to ward storage. Reports at minimum shall include par levels, equipment ID, equipment type, ward, location, time in ward storage.
 - b. Par level inventory management shall also be provided within the solution.
 - c. Solution will provide the ability to provide inventory management and tracking capabilities (i.e. recall) for implantable items from receipt, storage, implantation, and reordering.
 - d. Solution shall be able to track expiration date of item that has been processed to ensure it is not used on a patient after it has expired.
 - o This will include the ability for alerts and alarms relative to expiration date tracking or FDA recalls.
 - e. The system shall allow hospital staff to generate customizable reports tracking the expiration dates for all emergency equipment. At a minimum, reports should include emergency equipment expected to expire within 6 months, 3 months, 1 month and already expired.
5. RME JIT (Just in Time) Request Data (call data):
 - a. The system shall allow hospital personnel to create standardized as well as facility-customizable reports that identify equipment sterilized following specific sterilization parameters and equipment sterilized outside specified sterilization parameters. The report shall include the recommended parameters as well as the actual parameters followed, equipment ID, equipment type, equipment location, sterilization staff, and sterilization status.
 - b. The system shall allow hospital staff to generate reports to identify equipment associated with recall notices. The RTLS shall at a minimum provide a report per recall item by equipment id, equipment type, location, maintenance status, time from recall notice to start of repair, and time to repair.
6. RME Process Control (Staff compliance data)
 - a. Ability to track specific RME, surgical instrument, or implantable item(s) to a specific patient in the event of a FDA recall or look back.
 - b. Ability to track specific RME and/or instrument of implantable item(s) to a specific SPD staff member that processed the RME and/or instrument.
 - c. The system shall allow hospital staff to track the number of events where procedures were delayed due to lack of instruments at the ready in the operating room. The report shall include at a minimum operating

room/procedure room, type of procedure, items missing, medical team, patient, time elapsed until procedure occurs.

- d. The system shall allow hospital staff to generate reports identifying the percentage of reusable medical equipment tagged for RTLS tracking. Reports shall include the percent of total items tagged per month, the percent of items tagged vs. the total number of items to be tagged, and time to complete the tagging process.
7. RME Process Control (Manufacturer IFU Document management - SOP):
 - a. Strict adherence to manufacturer's instructions for use regarding cleaning/sterilization parameters will be monitored by the solutions with alerts/alarms for data outside of established parameters.
 - b. Solution(s) shall be user friendly and offer integration of video clips, pictures, diagrams, or sketches of individual instruments for ease of identification of components that must be disassembled for cleaning/maintenance and reassembled prior to sterilization.
 - c. Solution shall also provide tray count sheets with identification of critical instruments required before a tray can be closed for use, versus non-critical instruments that can be closed with an identifier (i.e. sticker/label) indicating that a non-critical item is missing.
 - d. Items with required cycle counts will be tracked with an alert/alarm when the appropriate number or reprocessing cycles is close to occurring, or has been exceeded so that it may be removed from service.
 - e. To the greatest extent possible, instruments should be actively tracked throughout the entire workflow process.
 - f. Solution will interface with cleaning and sterilization equipment to correlate processes to items as part of quality assurance and facilitate VA's paperless documentation strategies.
8. RME Process Control (Process time expectations):
 - a. Reports shall include average time, maximum time, minimum time for equipment to get to the sterilization room after use as well as the average, maximum and minimum time by type of equipment.
 - b. The workflow shall measure time intervals to indicate the length of time instruments sit waiting to be cleaned, as well as a means to measure service productivity.
9. RME Utilization Rates (may fall under inventory management):
 - a. The system shall allow hospital staff to generate reports identifying all purchased equipment. Reports shall include at a minimum inventory ID, purchase date, location, cost, time in storage, time in use, time in maintenance and expiration/replacement date.
 - b. Solution(s) provides ability to document set and individual items for maintenance, repair, and replacement costs monitoring.
 - c. Tracking software will enable determination of Utilization Rates as well as a Return on Investment (ROI) for all RME, instrument sets, and individual instruments based upon generally accepted industry standard calculations.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- d. The system shall allow hospital staff to create reports showing annual aged equipment rates by equipment id, equipment type, dollar value, and location. The report should include a report on annual aged equipment by type, location and dollar value.
 - e. The system shall allow hospital staff to create reports/alerts showing equipment still in use after its anticipated replacement date as entered upon receipt within AEMS/MERS by equipment id, equipment type, dollar value, and location.
 - f. The system shall allow hospital staff to print reports identifying the utilization rate of all equipment moving through the sterilization process. Utilization should take into account time waiting to be sterilized, time in sterilization, time sterilized but waiting to be used (e.g. quarantine, storage) and time in use.
 - g. The system shall allow hospital staff to generate reports identifying the amount of time reusable medical equipment is out for repair/upgrade. Reports at a minimum shall include equipment ID, equipment type, date delivered for repair, date returned from repair, repair location, repair vendor, total time to repair, repair history.
10. SPD Staffing level management (accumulated from above to establish):
- a. The system shall track the number of times an employee has performed a competency based task. When annual evaluation is required the supervisor/trainer can use that information to tailor the re-competency validation. The supervisor/trainer shall be required to hand-enter an electronic validation code to endorse competency assessment.
 - b. Work history reports will provide scheduling and work data for supervisors or work leaders to allow equitable staffing assignments ensuring that staff can function in all roles within SPD operations.
 - c. Solution provides department management personnel with customizable statistical reports and data storage.
 - d. Track whether staff is taking appropriate precautions for their own safety, by wearing the appropriate personal protection equipment (PPE).
 - e. The system shall allow hospital staff to generate reports on the time it took to sterilize equipment from arrival at the sterilization location through sterilization completion. Reports shall include equipment id, equipment type, arrival time at the sterilization location, time at start of the sterilization process and time at completion of the sterilization process. Reports shall identify hospital staff performing the sterilization process.
 - f. The system shall allow hospital staff to generate reports on the time it takes to retrieve equipment (e.g., Level 1, Level 2, and instrument sets) for the sterilization process after use to the equipment's arrival at the sterilization location. Reports shall include average time, maximum time, minimum time for equipment to get to the sterilization room after use as well as the average, max and min time by type of equipment.

1.3 Asset Management Workflow Use Case

- VA Database Interfaces Required

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- AEMS/MERS
- Technology Considerations
 - Passive tagging (tags, readers, exciters)
 - Active tagging
- System Functionality
 - Room level coverage to track assets (required)
 - Egress coverage for theft notification
 - Bed/Bay level coverage for patient care activities

Use case goal is to track all equipment for purposes of conducting inventory, preventing theft, finding the assets when needed, accessing asset utilization, and monitoring asset related workflows when needed in VHA (medical facilities and CMOP's).

1. Stationary administrative and IT equipment, and stationary medical equipment shall be tracked through the use of passive technology that will prevent theft and allow users to locate equipment for purposes of inventory on a periodic basis. Passive Inventory Capabilities of this stationary equipment must be accurate enough for a reader to pick up room level location when the reader enters that room regardless of where the asset is located within the room.
2. For the passively tagged equipment the system shall have the ability to trigger an audible, silent alarm, security cameras, or other warning alert when an asset is leaving the building or unauthorized location, based on assigned rules. Location will be updated when it re-enters the assigned building, or enters another building. System shall have the capability to integrate with CCTV/IP security cameras if available.
3. Mobile Medical Equipment (Vital signs monitors, infusion pumps, etc.), computers/workstations on wheels (C/WOWs), and other high theft/loss equipment (including wheelchairs and stretchers) shall be tracked through the use of active technology that will prevent theft, and allow the users to locate equipment at any time that equipment is needed. System shall have the ability to automatically request service on a tag if/when the battery reaches a critical level to ensure continuous monitoring of assets. System shall also have a rules engine which provides users the ability to set par levels in defined rooms (clean equipment, soiled equipment, etc.), based on configurable rules. Tags must be made available that have the ability to send an alert when/if it is tampered with. Further, the system must have the ability to set "out of bounds" locations, which are capable of triggering an alert when a tagged asset enters that area (e.g. – leaves a building) based on assigned rules. Further, the system must be capable of achieving room level or better granularity—the resolution of the system must recognize the difference between adjacent rooms, and floors above or below.
4. Chokepoints shall not resemble department store or high security chokepoints. They shall be aesthetically appealing and blend in with the general décor of the facility.
5. System should have the ability to run reports verifying asset locations / status and provide asset location history at any time necessary.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

6. Movement of tagged assets shall be accessed to alert users when assets travel in along a path that is not permitted, e.g. patient soiled utility, back to patient.

Expected outcomes from implementing an asset tracking system are expected to allow for the following benefits:

Benefit Name	Metric #	Metric Name
Improve Patient Care	1.1	Sequestered Emergency Equipment Expiration Rate
Improve Staff Efficiency	2.1	Improve Recall Turnaround Time
	2.2	Biomedical Equipment Preventative Maintenance Completion Rate improved related to equipment that cannot be located.
	2.3	Level of Effort to complete an annual inventory is decreased.
	2.4	Number of Reports of Survey decreased to zero.
Improve Managerial Decision Support	3.1	Accuracy Rate for Non-Expendable Assets is improved.
	3.2	Percentage of Assets Tagged is increased
	3.3	Number of instances in which equipment fell below predetermined par level
Reduce Inventory and Equipment Costs	4.1	Biomedical Equipment Utilization Rate increases.
	4.2	Length of time Biomedical Equipment is in maintenance decreases.
	4.3	Length of time Facility Related Equipment is in maintenance decreases.
	4.4	Inventory Expenses reduced.
	4.5	Total Rental Equipment Use Rate is decreased.
	4.6	Biomedical Rental Equipment Use Rate is decreased
	4.7	IT Rental Equipment Use Rate is decreased.
	4.8	Service Down-Time for Biomedical Equipment is reduced.
	4.9	Amount of Equipment that is Lost or Stolen is reduced
	4.10	Value of Lost or Stolen Assets is reduced.
Improve Staff Satisfaction	5.1	Increased Staff Satisfaction.

Implementation of asset tracking should assist with managerial decision making and information gathering under the following requirements:

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

1. The system shall allow users the capability to run reports showing historical and current utility status of all equipment. (NOTE: Zones shall be set at a facility level RTLS with automated status settings.) Utilization Reports shall include queries for In Use equipment, equipment that is cleaned and available for use, equipment that has been soiled and requires cleaning, and equipment that requires maintenance or is being repaired.
2. The system shall allow users the capability to run reports that show events indicating equipment was stolen, attempted theft, or lost (e.g. has not communicated with server in set timeframe).
3. The system shall allow users the capability to run reports that identify the location prior to equipment loss, theft, or attempted theft.
4. The system shall allow users the capability to run reports to identify sites prior to most frequent and least frequent equipment loss, theft, or attempted theft.
5. The system shall allow users the capability to run a report to ascertain inventory counts of any combination of equipment categories (e.g. infusion pumps, bariatric beds, suction units, PCA pumps, Barcode Medication Administration (BCMA) Carts, wheelchairs, portable imagining equipment, beds, defibrillators, etc.).
6. The system will provide an option to report by Category Stock Number/USMDNS, Equipment Category, model, serial number, location, ownership status (purchased or rented), or PO number.
7. The system shall be able to run a report that denotes equipment in need of preventative maintenance and corrective service (i.e. broken equipment or infusion pumps with outdated drug libraries) sorted by the date scheduled for the individual device.
8. The system shall provide a means of alerting the Chief Biomedical Engineer or Biomedical Supervisor via e-mail of the location of devices that are currently due and overdue for preventative maintenance.
9. The system shall be able to run a report that documents par levels for actively tagged assets in equipment supply rooms (e.g. infusion pumps).
10. The system will have the ability to trigger an alarm for an un-authorized removal from facility of an asset.
11. The system shall allow staff to generate reports to identify equipment associated with recall notices The RTLS-L shall at a minimum provide a report per recall item by equipment ID, equipment type, location, maintenance status, time from recall notice to start of repair, and time to repair completion.
12. The system shall allow staff to generate reports tracking the expiration dates for all emergency equipment. At a minimum, reports should include emergency equipment expected to expire within 6 months, 3 months, 1 month and already expired.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

13. The system shall allow staff to generate reports identifying all leased or rented equipment. Reports shall include at a minimum equipment ID, equipment type, rental date, location, cost, time in storage, time in use, time in maintenance, and expiration date.
14. The system shall allow staff to generate reports identifying all leased or rented equipment. Reports shall include at a minimum equipment ID, manufacturer, equipment type, rental date, location, cost, time in storage, time in use, time in maintenance, time returned, and rental expiration date.
15. The system shall allow staff to generate reports identifying all known lost or stolen equipment. The report at a minimum shall include manufacturer, equipment IDs, lost or stolen item last known location, equipment age, and equipment value.
16. Items that are overdue for PM or which are part of a Hazard recall event shall be visible to all users.

1.4 Temperature and Humidity Monitoring Use Case

- *VA Database Interfaces Required*
 - AEMS/MERS
- *Technology Considerations*
 - Active tagging

Use case is to monitor temperature and humidity of refrigerators, freezers, some temperature dependent assets, and storage room locations to ensure compliance with governing regulations, to reduce the labor required to manually document temperatures, and to generate alarms when temperatures are out of range.

Expected outcomes from implementing an automated temperature monitoring system are expected to allow for the following benefits:

Benefit Name	Metric #	Metric Name
Improve Consistency of Services	1.1	Increase in percentage of Temperature Monitoring Logs that are Automated to 100%
	1.2	Increase in percentage of Assets that are Monitored Automatically
	1.4	Temperature Recording Compliance met at 100%
	1.5	Percentage of Incomplete Logs reduced to 0%.
	1.6	Number of Negative Findings (Temperature & Humidity) Found in SOARS Inspections to 0%.
Improve Staff and Customer Satisfaction	6.1	Improve Staff Satisfaction.

Additional assurances should include:

1. The system should have the capability to remotely monitor the temperature and humidity (if necessary) and issue alerts if the temperature goes out of range.
2. Alert system should escalate as the temperature nears a limiting temperature.
3. Data collection events (frequency of record) should be set by the user for each sensor and data should be rolled up to the server at user defined times.
4. The system should have the capability of recording discrete temperatures, mean, and event logging (e.g. when temperature goes out of acceptable range).
5. Minimal Alarms and Alerts should exist based on whether action needs to occur. They include, but are not limited to; 15 minutes temp out of range, low battery, battery failure, probe failure, and tag removed.
6. Reports to be provided include but not limited to;
 - a. Daily Reading Log - to include a daily reading of defined tags over a set period of time and display the following: Tag ID, Device Name, EE number, Location, Reading, Time of Reading
 - b. Alarm - to include all alarms and alerts in a specified time period and display the following:
<Tag ID, Device Name, EE Number, Location, Reason for Alert, Corrective Action, Time of Alert, Time Corrected, Responding Individual, WO number, Comment>
 - c. Temp Graph by Item - to include a graphical display of all temps and humidity over a period of time for a select tag(s) and also display any alerts that occurred
7. Temp Tags should provide a NIST Traceable Probe that can be calibrated.
8. Some assets (such as blood bank refrigerators) require monitoring on two (2) shelves. Temp tags should be provided that support multiple thermistors.
9. Temp tags will meet AABA (American Blood Bank Association) requirements for glycol media simulation.
10. Tags have the capability to measure temperature ranges from -80 degrees Celsius to 30 degrees Celsius.
11. Tags should have ability to be mounted in the interior of assets that have a closed container (refrigerators and freezers, for example).
12. Data collection must continue during network / power outages. 24 hour memory is required on temp tags.
13. Probes should reside in wells.
14. The maximum diameter for wired temperature probes are:
 - a. 0.8cm (-20C & -200C)
 - 1cm (-100C)

1.5 Patient Elopement Use Case

- *VA Database Interfaces Required*
 - VISTA/CPRS
- *Technology Considerations*
 - Active tagging
 - Display monitors to show real time viewing of patient movement
- *System Functionality*

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- Room level coverage
- Egress coverage for elopement notification
- Bed/Bay level coverage for patient care activities
- Active play back modes for retracing patient movement and interactions

The goal of the elopement system is mission critical to patient safety and should provide a fault tolerant design with minimal latency requirements. Delays beyond 2-3 seconds for communication and alarming within the System and to external sources are maximum requirement.

The elopement system should have the flexibility to have rules based on individual patients to freely move within the boundaries set for them. System integration with elevators, door locks, and security cameras should be patient specific and provide a fault tolerant design promoting patient safety. As patients approach doors or elevators an escalating system of alerts and security measures should prevent elopement including disabling of elevators and locking of doors; escalation should be transparent to the patient. Again the goal of the elopement system should be patient specific and provide freedom of movement within specified boundaries while maintaining a fault tolerant design and promoting the safety of the patient. In addition, the sensor shall have the capability of detecting falls.

Potential expected outcomes from implementing the patient elopement system is

Benefit Name	Metric #	Metric Name
Improve Patient Care	1.1	Number of missing patients in the facility is reduced
	1.2	Unexpected patient movement – number of alerts triggered
	1.3	Unexpected patient movement – number of alarms triggered
	1.4	Number of instances in which a patient fall is detected
	1.5	Unexpected patient movement – number of unauthorized entries
	1.6	Number of elopement cases that resulted in medical treatment is reduced
	1.7	Number of elopement cases that resulted in death is reduced
Improve Staff Efficiency	2.1	Staff to patient ratio – 1 to 1 observation is reduced
	2.2	Staff to patient ratio – close observation is reduced
Improve Staff and Customer Satisfaction	3.1	Staff Satisfaction is increased

expected to allow for the following benefits:

Specific capabilities and information management should include the following:

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

1. The system shall allow users the capability to run reports that show events indicating frequency of patient elopement.
2. The system shall allow users to be able run reports that identify the location prior to patient elopement.
3. The system shall provide active play back modes for retracing patient movement and interactions.
4. The system shall allow users the capability to run reports to identify sites prior to most frequent and least frequent patient elopement.
5. The system shall allow hospital staff to generate reports identifying the number of eloped patients stopped because of the RTLS device outside their designated area but still in the safety of the building. Reports shall include at a minimum, patient id, location, staff, distance from designated area, total time of elopement.
6. The system shall allow hospital staff to generate reports identify the number of eloped patients stopped because of the RTLS device outside their designated area but still on the hospital grounds. Reports shall include at a minimum, patient id, location, staff, distance from designated are, root cause of elopement, total time of elopement, locations eloped patient entered (e.g. male patient in female patient room).
7. The system shall allow hospital staff to generate reports identify the number of eloped patients making it outside the facility or its grounds. Reports shall include at a minimum, patient id, location staff, distance from designated are, root cause of elopement, total time of elopement.
8. The system shall allow hospital staff to generate reports identifying the number of eloped patients injured as a result of an elopement. Reports shall include at a minimum, patient id, location staff, distance from designated are, root cause of elopement, elopement injuries, and total time of elopement.
9. The system shall allow hospital staff to generate reports identifying the number of eloped patients dying as a result of an elopement. Reports shall include at a minimum, patient id, location, staff, distance from designated are, root cause of elopement, elopement cause of death, and total time of elopement.
10. The system shall be capable of generating reports quantify the number alarms, warning, alerts generated by the system and categorizing them (e.g. nurse response, police called).
11. The system shall allow hospital staff to generate reports providing a Pareto chart of the causes of elopements.

1.6 Hand Washing Use Case

- *VA Database Interfaces Required*
 - PIV
 - Active Directory
- *Technology Considerations*
 - Active tagging
 - Passive tagging
- *System Functionality*
 - Bay level coverage – at the hand washing station
 - Validation based on activity at station, not proximity

Use case goal is to validate staff hand sanitizing rates. VA deploys hand washing stations at all sinks and also at stationary locations throughout the facility via a sanitizing dispensing station or a sink. It is expected that hand washing rates can be monitored as a staff member approaches a sanitizing station and activates a dispensing container. The system would have the capability to monitor the sanitizing compliance, i.e., hand hygiene sensing device detects the dispensing of the sanitizing product and would communicate via employee badge to record the event. System would monitor the hand sanitizing after rest room use, after scheduled breaks, and entering or exiting occupied patient care area. Functionality for a system that has the capability of alerting or reminding staff to wash their hands is also desired.

1. The system should detect if the employee sanitized their hands and for how long.
2. The system should detect and report if the employee had not sanitizing their hands sufficiently.
3. The system shall allow users the capability to run reports that show contact between patients and staff by means of room/bed-level proximity. This shall allow for better management and prevention of the spread of contagious diseases.
4. The system shall allow users the capability to run reports that show caregiver hand-hygiene compliance.

1.7 Emergency Department Work-Flow Use Case

- *VA Database Interfaces Required*
 - VistA CPRS
 - EDIS – Emergency Department Information System
- *Technology Considerations*
 - Patient tags
 - Staff tags
 - OR Department Wall Display monitors
- *System Functionality*
 - Bay level coverage – near field resolution
 - Capability to track patient flow in ED supporting department, such as X-ray.
- *Performance Metrics*
 - Percent of ED Stays over 6 hours (quarterly report)
 - Patient divert hours per quarter
 - Patient elopements per quarter

The Emergency Department (ED) Work-Flow Use Case is to define the effective application of RTLS technologies to ED functions. The RTLS will track patients, necessary equipment, instruments, supplies, and (potentially) caregivers. The RTLS will facilitate continuous process improvement of ED patient treatment services. This is achieved not only by locating the patient at the appropriate ED bedside and diagnostic test station (such as X-ray Department or Clinical Lab), but also by associating the patient with the appropriate ED staff, medical equipment, supplies, and other

necessities. The RTLS and associated software package will reduce time and the risk of mistakes by replacing many of the tasks performed manually.

Process steps performed automatically through RTLS will reduce the time necessary to provide emergency care. As a result, patient throughput and utilization increases and the cost of ED services can be contained or reduced. There is a consequent potential to reduce the number of cases that must be referred to outside hospitals with their related costs and management issues.

1.7.1 Emergency Department RTLS Technology Application

1. Transmitter/receiver hardware technology
 - a. The RTLS shall apply 802.11 Wi-Fi-based RFID with auxiliary technologies, as needed, to achieve sub-room (near-field) level location resolution in order associate the patient with the waiting room, a distinct bedside in the ED, the X-ray department, Clinical Laboratory, or other diagnostic location. The transmitter (“tag”) will be associated with a patient upon registration at the ED reception desk. In areas requiring near-field resolution, receivers (“sensors”) shall be placed in every location that the patient will occupy as he/she progresses through the emergency treatment process.
 - b. The RTLS shall include a staff RFID tag option to locate patient care staff and track patient contact time.
 - c. Tag/sensor technologies will be placed for the purpose of Environmental Service staff to electronically notify the ED patient care staff that bedsides and related treatment areas have been cleaned and are ready to accept a new emergency case.
 - d. The RTLS rules-engine will detect ED patient elopement and alert ED staff of the situation.
 - e. The tag will be disassociated from the patient upon discharge or transfer from the ED.
2. Computer Software and Network Technologies
 - a. The computer software, network, and display functions are paramount to the RTLS performance. The RTLS shall be able to interface with CPRS/VistA to be able to receive the daily surgical schedule and to automatically populate the RTLS patient ID fields. The software will be designed so that it is easy for nursing and support staff to associate the unique tag with the unique patient.
 - b. The RTLS system shall be operated and viewed from Clinical PC workstations within the ED as well as VA-managed office PC's. This will enable ED staff to assess unit preparation, patient location, and other significant elements from more remote locations.
 - c. The tag/sensor technology will indicate the exact location of the patient as the patient progresses from ED admission through discharge or admission to inpatient or ambulatory treatment. The information will be viewable in an easily comprehensible format on a video monitor. The display will also

be capable of associating the patient RTLS ID tag with the ID tag of medical equipment, caregivers, and other assets currently being applied to the patient.

- d. The RTLS display software shall be configurable so that tabular and graphic displays of the ED patient and asset locations can be viewed at the earliest practicable time (frequent video display refresh). That way, the ED staff can assign resources and coordinate activities efficiently and without delays due to miscommunication. Upon viewing the display, managers can prioritize and make decisions to redirect or call in additional staff when necessary.
- e. The software must be flexible so as to accept and display text and color coded messages regarding the completion of X-rays, laboratory, and other diagnostic tests, and other important elements of optimal emergency care. It should also be able to alert the users when an emergency treatment process is about to be initiated without the necessary elements are in place (for example equipment, instruments, or appropriate caregivers are not present at the patient site).
- f. The RTLS shall have network capabilities to send outgoing messages to physicians and managers cellular communications devices to alert them to significant issues and events in the real time ED operation.

1.7.2 RTLS Workflow Process Improvement Application

1. The RTLS software shall be capable of quantifying the amount of patient time spent at each location of the ED treatment process, including waiting room, triage, ED treatment rooms, X-ray department, laboratory, etc. The data will be aggregated, sorted, and analyzed to identify delays, bottlenecks, inefficiencies, risks, and other impediments to optimal ED treatment.

1.8 Surgical Work Flow Use Case

- *VA Database Interfaces Required*
 - VistA CPRS
 - SQWM – Surgical Quality Workflow Manager (in development)
- *Technology Considerations*
 - Patient tags
 - Staff tags
 - Wall-Mounted display monitors
 - System control, viewing, and reporting from VA Managed Workstations
- *System Functionality*
 - Bay level coverage – near field resolution
- *Performance Metrics*
 - OR First Case Starts on Time
 - Volume of telephone call to OR desk reduce

The Surgical Work-Flow Use Case is to apply RTLS technologies to facilitate continuous process improvement of Surgery services. This is achieved not only by

locating the patient at every point of the care continuum, but also by associating the patient with the appropriate (and clean) room, surgeons, anesthesiologists, nurses, instruments, supplies, pre-screening diagnostic tests, blood products, and other necessities. The RTLS and associated software package will reduce time and the risk of mistakes by replacing many of the tasks performed manually. Patient risk will be reduced by RTLS automatically alerting the surgical staff when a vital step has been missed.

Process steps performed automatically through RTLS will reduce the time necessary to complete surgical procedures. As a result, patient throughput and utilization increases and the cost of Surgical and Clinical services can be contained or reduced. There is a consequent potential to reduce the number of cases that must be referred to outside hospitals with their related costs and management issues.

The RTLS will be able to improve the patient and family experience by keeping the family automatically informed as to where their loved one is in the process and allowing them personal access to the patient at the earliest feasible time.

1.8.1 Surgical RTLS Technology Application

1. Transmitter/sensor hardware technology
 - a. The RTLS solution shall begin with of a transmitter/receiver technology that is capable of sub-room (near-field) level location detection in order to associate the patient with a distinct room within a treatment area. The system must accurately locate patients in pre-op holding and recovery areas that do not have an individual room for each patient bedside. The transmitter ("tag") will be associated with a patient upon being admitted to the Out-patient or In-patient preoperative area. Receivers ("sensors") will be placed in every room and location that the patient will occupy as he/she progresses through the surgical process. Sensors will also be located at appropriate hallway locations along the treatment path.
 - b. Tag/sensor technologies will be placed in clean and sterile environments, such as the OR's, for the purpose of Environmental Service staff to electronically notify the OR patient care staff that rooms have been cleaned and are ready for the patient.
 - c. The tag/sensor technology will indicate the exact room location of the patient as the patient progresses from pre-op through discharge. The information will be viewable in an easily comprehensible format on a video monitor. The display will also be capable of informing the caregivers that the appropriate pre-operative lab tests have been performed, the necessary volume and type of blood product available, the room is clean, and the sterile instruments and supplies are in place. The facility is now ready for surgery, the surgeon is to be notified, and the patient can progress through the surgery.
2. Computer Software and Network Technologies

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

- a. The computer software, network, and display functions are paramount to the RTLS performance. The RTLS will be able to interface with CPRS/VistA to be able to receive the daily surgical schedule and to automatically populate the RTLS patient ID fields. The software will be designed so that it is easy for nursing staff to associate the unique tag with the unique patient.
- b. The video display will be programmed and configured so that the day's scheduled operations, room assignments, and room status can be viewed at significant locations throughout the surgical department and at the earliest practicable time. This enables the surgical, clinical laboratory, blood bank, support, and environmental staff can assign resources and coordinate activities efficiently and without delays due to miscommunication. Upon viewing the display, managers can prioritize and make decisions to call in additional staff when necessary.
- c. The software must be flexible so as to accept and display text and color coded messages regarding the completion of pre-surgical lab tests, available blood products, and other important elements of a successful operation. It should also be able to alert the users when a process step is about to be initiated, but not all of the necessary elements are in order.
- d. The RTLS information should be capable of being displayed and operated from managed office PC's as well as dedicated workstations and monitors in the surgical environment. This will enable managers and surgeons to assess the status of the OR preparations from more remote locations.
- e. The RTLS must have network capabilities to send outgoing messages to physicians and managers cellular communications devices to inform them that everything is ready and the patient is in the correct location to proceed with the surgical procedure. There should be capability to provide a remote display device with HIPAA masking capability so patients' family members are kept informed of the patient's current location in the process.

1.8.2 RTLS Workflow Process Improvement Application

1. The RTLS software shall be capable of quantifying the amount of patient time at each location of each unique the surgical process. The data will be aggregated, sorted, analyzed, and otherwise acted upon to determine the time utilization in OR location within and across surgical specialties. This will result in the most effective configurations of different surgical blocks and OR designations as well as identifications of nodes that are introducing delay or otherwise undesirable variation in process and procedure.

ATTACHMENT B: WIFI TECHNICAL PERFORMANCE PARAMETERS SUMMARY

The information cited herein summarizes the Wi-Fi technical performance parameters that were deployed under the National Wireless Infrastructure contract.

The Wi-Fi installation site survey was executed using Cisco Access Point model number AIR-LAP1131AG-A-K9.

Radio Frequency surveys were conducted at each VA Facility to provide site specific design for the deployment of the 2.4 GHz and 5 GHz network. The survey was conducted across all buildings and floors that received coverage. Areas where construction was ongoing or immediately planned at the time of the RF Survey were skipped and not completed through this process. Any work in this area after the RF Survey will be the responsibility of the Facility.

The survey methodology was based on a set of industry best practices for the survey of facilities for wireless networks. The survey methodology and resulting Wi-Fi network design / configuration conforms to guidance published in Cisco's Wi-Fi Location-Based Services—4.1 Design Guide, May 2008, (Addendum C.1), as well as to other equipment Contractor guidelines such as Radio Resource Management Under Unified Wireless Networks (Cisco Doc 71113).

The coverage levels granted to spaces are defined as enhanced, standard, and limited. Enhanced services are defined as areas where location based services are available where at least three access points can hear devices. The vast majority of coverage areas are enhanced services.

However, there are areas where it is not physically possible to provide enhanced services. In these cases, standard services or limited service is provided. Standard services are defined as areas where location based services are available where less than three access points can hear devices. Voice grade and redundant coverage is available. Ancillary administrative buildings with floors smaller than 5,500 square feet are typical candidates for this level of coverage.

Limited services are defined as areas where location based services are available where only one access point can locate devices. Basic wireless coverage only is provided due to excessive interference (i.e. maintenance areas such as electrical mechanical spaces and boiler rooms). Redundant coverage is not available. If an access point fails, all coverage may be lost. This will be used in a limited fashion, and agreed to in writing by the region team and VA PMO.

The Wi-Fi network configuration developed through the site survey process supports achievement of the technical performance specified in the National Wireless contract in 100% of the interior space within each facility.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

The following Wi-Fi network architecture and configuration notes were executed when performing the site surveys and developing the design / configuration packages.

- IEEE 802.11b/g (2.4 GHz) and IEEE 802.11a (5 GHz) frequency bands are used. Within each of the radio frequency bands, only non-overlapping FCC licensed channels are used.
- The Wi-Fi solution supports 802.11i Enterprise connections as the primary form of connectivity. It was configured with the WPA2 protocol with AES encryption and 802.1x EAP-TLS authentication. It also supports 802.11i Personal with WAP2 and PSKs. The 802.11i implementation is in accordance with NIST Special Publication 800-97 “Establishing Wireless Robust Security Networks (RSN): A Guide to IEEE 802.11i.”
- Mental Health Wards: Access points are not permitted in patient rooms (sleeping areas) or bathrooms. Tamper-resistant covers are required over all access points in mental health wards.
- Redundancy = The basic level of redundancy provides at least one adjacent device capable of increasing output levels to “heal” the wireless hole in coverage caused by a wireless radio failure.
- Interference (EMI) = All 802.11 solutions are covered under FCC Part15 D and limited to 1 W of effective transmit power. FCC Part15 compliance requires no system will cause harmful interference to another Part15 system. Contractors provided survey and analysis to identify and avoid potential areas of EMI interference.

The quantity and location of Wi-Fi access points are predicated on providing the following performance parameters at the access point boundaries:

- Minimum Signal Strength = -67dBm
- Minimum Signal To Noise (SNR) = 25 dB
- Each wireless device must be heard at better than -75 dBm by no fewer than 3 access points to support location based services.

Heat map drawings of all completed sites were developed to verify the required signal strength was obtained in the required coverage areas.

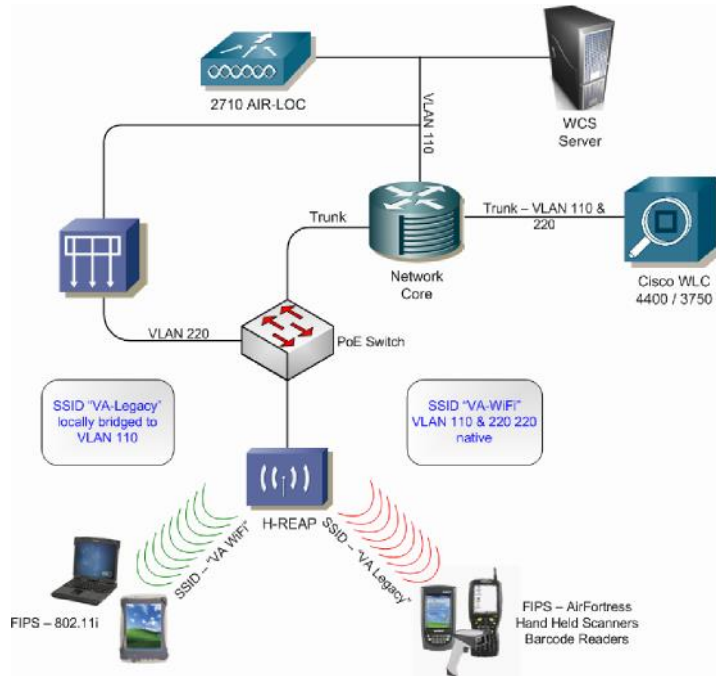
HIPAA Compliance strategies must be implemented to protect the security and privacy of information in a WLAN environment. Deployments of wireless networking solutions, when combined with other security controls and mechanisms within the context of an effective risk management strategy and policy, can effectively meet the security standards as proposed under HIPAA. The main requirements for compliance with HIPAA security standards for electronic patient medical data are:

1. Confidentiality. Ensure that patient medical information is not made available or disclosed to unauthorized individuals.
2. Integrity. Ensure that data has not been tampered with en route or in storage.
3. Authentication. Verify that only authorized users can access the network and that the person transmitting data is who he or she claims to be.

RTLS Performance Work Statement - ATTACHMENT 001
VA118A-12-RP-0118

4. Authorization. Allow authenticated users access to network resources and data based on defined permissions.

The figure below provides a notional representation of the Wi-Fi solution architecture.



ATTACHMENT C: RTLS INTERFACES TO VA SYSTEMS

VISTA SYSTEMS

1. AEMS-MERS: The official asset management system of record for the VA
2. Generic Inventory Package (GIP): VA system maintaining supply inventories, such as those typically stored in cabinets and used in clinical procedures.
3. Clinical Procedures: VA system listing the supplies required to support specific clinical procedures.
4. Integrated Billing: VistA software package which links patients and procedures to consumable supply records for billing purposes.
5. Patient File: VA system containing patient information
6. Prosthetic Inventory Package (PIP): VA system linking patients and implant devices.
7. Scheduling Package: VA system containing operating and procedure room schedules.
8. New Person file: List of all people authorized for VistA login.

OTHER VA SYSTEMS

1. Clinical Assessment, Reporting, and Tracking – Cath Lab (CART-CL): Non-VistA system tracking inventory in RTLS enabled cabinets.

ATTACHMENT D: VHA VISN RTLS SITE INFORMATION

The following attachment contains general VHA VISN site-specific information. All information provided herein is current as of the date indicated on the document and is subject to change at any time. The data is provided as general information only.



VHA Facility List.pdf

ATTACHMENT E: Non Disclosure Agreement



General HCE
Non-Disclosure Agree