PERFORMANCE WORK STATEMENT

"Attachment A"

DEPARTMENT OF VETERANS AFFAIRS

Veterans Health Administration

VA San Diego Health Care System (VASDHCS)

Project Title:
Research & Development (R&D) Facility Lease

Initial Outfitting, Transition, and Activation Services (IOTA) Contract

Date:
July 6, 2026

1.0 Objective

The purpose of this acquisition is to provide the Department of Veterans Affairs, Veterans Health Administration (VHA) with Initial Outfitting, Transition, and Activation (IOT&A) services for the VA San Diego Healthcare System Research & Development (R&D) Facility Lease. The objective is to have the IOTA project completed by the first day of Research & Development Services, which is projected for April 2029. North American Industry Classification System (NAICS) code for these services is 541614, Process, Physical Distribution, and Logistics Consulting Services.

2.0 Introduction

Activation is defined as the process of identifying, planning, managing, and executing the logistical and operational requirements to bring a new medical center into full planned operations. The medical center assigns VHA staff to an Activation Team which is responsible for managing the Activation Project and ensuring the Research & Development (R&D) Facility Lease is in full planned operations on 'Day One' (the first day of Research Services are scheduled to be in operations). IOTA Contractor services are often required to support the medical center's Activation Team.

3.0 Background

In Fiscal Year 2018, the United States Congress approved numerous major leases for the Department of Veterans Affairs to enhance services for Veterans. The parent facilities, such as VA San Diego Healthcare System, are working with VA Office of Real Property and other support offices to secure award of the leases to developers who want to create the site of care for VA use. VA San Diego Healthcare System has been approved for a major lease to create an expanded service opportunity for Veteran Healthcare Research & Development (R&D) Facility Lease. This project proposes to lease a new Research & Development facility in San Diego, CA. This project is approximately 44,000 net usable square feet (NUSF), and 100 parking spaces. The new R&D Facility Lease will allow an expansion to the current footprint as well as added new services.

4.0 Scope

Conduct all necessary Planning, and IOTA activities, in accordance with the PWS, in support of the project(s) identified in paragraph 3.0 above. The IOTA contractor shall provide professional services to include all labor, materials, transportation, and equipment to conduct and provide IOTA support services to accomplish the PWS tasks. The scope includes project support for planning, activating, outfitting, and transitioning the staff associated with the project that includes the Administration Support, Biomedical Laboratory, and Veterinary Medical Unit areas. The scope of services includes Comprehensive Project Management, Comprehensive Interior Design, FF&E, and Space Planning Support; CONOPS and Transitioning Planning; Acquisition Support Services to include package development, Activation, Delivery, Relocation and Installation, Training, and Turnover and Post Occupancy Support for the identified project.

5.0 Applicable Documents

Applicable documents are listed below. IOTA contractor shall use the most current versions of all applicable documents listed below.

- **A.** Entire Lease/Construction contract to include the L100 from the Lease, Lease Design Narrative Appendix A-F
- **B.** Research and Development (R&D) Design Guide, PG-18-12, dated June 1, 2022, Office of Construction and Facilities Management, U.S. Department of Veterans Affairs
- **C.** VHA Directive 1200.07, "VA Research with Animals," May 23, 2023
- **D.** VHA Directive 1200.08, "Safety of Personnel and Security of Laboratories Involved in VA Research," April 24, 2019, Amended January 8, 2021
- **E.** Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules"
- **F.** FIPS Pub 201-3, "Personal Identity Verification of Federal Employees and contractors," January 2022
- **G.** 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
- **H.** Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, title IX Information Security Matters
- **I.** 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"

J. Department of Veterans Affairs (VA) Directive 0710 Personnel Security and Suitability Program dated May 2, 2016
K. Department of Veterans Affairs (VA) Directive 6102 (Internet/Intranet Services)
L. Health Insurance Portability and Accountability Act (HIPAA); 45 CFR Part 160, 162, and 164; Health Insurance Reform: Security Standards; Final Rule dated February 20, 2003
M. VHA Security Handbook 1600.01, Business Associate Agreements
N. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2024
O. Office of Management and Budget Circular A-130, "Management of Federal Information Resources', November 28, 2000
P. U.S.C. Section 552a, as amended
Q. Title 32 CFR 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
R. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, February 2024
S. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. Section § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
T. Homeland Security Presidential Directive (12) (HSPD-12), March 27, 2024
U. Department of Veterans Affairs (VA) Directive 6500, "VA Cybersecurity Program," February 24, 2021
V. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," February 24, 2021
W. VA Handbook 6500.1, "Mobile Device Security Policy" February 15, 2018
X. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information", June 30, 2023
Y. VA Handbook 6500.3, "ASSESSMENT, AUTHORIZATION, AND CONTINUOUS MONITORING OF VA INFORMATION SYSTEMS," March 10, 2015
Z. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle," March 12, 2010
AA. VA Handbook 6500.6, "Contract Security," March 12, 2010
BB. Federal Travel Regulation (FTR) July 1, 2021
CC. VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014
DD. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
EE. VA Handbook 7002, Logistics Management Procedures, January 8, 2020
FF. VHA DIRECTIVE 1761(1)/Supply Chain Inventory Management
GG. VA Directive 6404, VA Systems Inventory (VASI)
HH. HISD Medical Device Protection Program (MDPP) National Cyber Security Risk Assessment for VHA Networked Medical Devices, Version 2.1
II. ANSI/EIA/TIA 568B Commercial Building Telecommunications Wiring Standard
JJ. VA Handbook, 0730/4, Security and Law Enforcement, August 11, 2000
KK. U.S. Department of Veterans Affairs, Office of Construction & Facilities Management, Physical Security Design Manual for Life-Safety Protected Facilities, January 2015
LL. U.S. Department of Veterans Affairs, Office of Construction & Facilities Management, Physical Security Design Manual for Mission Critical Facilities, October 1, 2020, Revised May 1, 2024
MM. MIL-STD-1691 Construction and Material Schedule for Military Medical, Dental, Veterinary and Medical Research Laboratories, June 1, 2022
NN. 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.
OO. Architectural Barriers Act Accessibility Standards (ABAAS) including VA supplement, PG-18-13 Barrier Free Design Standard
PP. VA PG-18-14 Room Finishes, Door, and Hardware Schedule
QQ. VA PG 18-4 Standard Details and CAD Standards
RR. VA H-18-8 Seismic Design Handbook August 3, 2017

SS. VA Signage Design Guide: PG-18-10 May 16, 2023, Revised February 19, 2025
TT. VA Directive 7531 Acquisition of Artwork, Decorative Furnishings, and Decorative Items March 1, 2017
UU. VA BIM Standard "BIM Manual V2.2" November 1, 2016, Revised November 1, 2023
VV. International Building Code (IBC)`
WW. NFPA 10: Standard for Portable Fire Extinguishers
XX. NFPA 70: National Electrical Code (NEC)
YY. NFPA 72: National Fire Alarm and Signaling Code
ZZ. NFPA 150 - Fire and Life Safety in Animal Housing Facilities Code
AAA. AAALAC – Guide for the Care and Use of Laboratory Animals
BBB. NFPA 101: Life Safety Code
CCC. International Plumbing code (IPC)
DDD. Occupational, Safety, and Health Administration (OSHA) Standards
EEE. Federal Acquisition Regulation (FAR)
FFF. Veterans Affairs Acquisition Regulation (VAAR)

6.0 Contract Type

This is a Firm-Fixed-Price (FFP) Contract. This Contract is a 100% Service-Disabled Veteran Owned Small Business (SDVOSB) set-aside under FAR Parts under 12 and 37.

7.0 Non-Personal Services

In accordance with FAR 37.201-2 and 5 U.S.C. 3109, this requirement has been determined to be a non-personal services contract. A non-personal services contract is a contract under which the contractor personnel providing the services are not subject to continuous Government supervision and or control, either by the contract's terms or by the manner of its administration.

8.0 Organizational Conflict of Interest

Per FAR Subpart 9.5, Organizational Conflict of Interest, due to the requirement of the contractor providing support services for Furniture, Fixtures, and Equipment (FF&E) and the possibility that any FF&E may be available through the prime contractor or its subcontractors, which may be regarded as a potential conflict of interest as seen by the Contracting Officer (CO), neither the prime contractor nor its subcontractors or consultants may participate as an offeror, subcontractor, or consultant on any procurement of FF&E conducted by the prime contractor or its subcontractors/consultants under this contract.

A. Contractor to provide a complete list as part of the quote submission of all proposed subcontractors in performance of this contract.
B. Contractor to provide notice to the contracting office immediately if any proposed subcontractors are changed during the course of the period of performance of this contract.
C. If procurement related tasks are divided by prime and sub, contractor to provide a list of which activities are performance by which contractor
D. Contractor to mitigate any risk associated with an OCI. Non-disclosure agreements may become necessary as part of Contract award.
E. Contractor to work will all subcontractors in reviewing subcontract terms and conditions associated with the awarded Contract.

9.0 Location and Hours of Work

The primary place of performance is at the Government's facility, with necessary work to be done off-site at the IOTA contractor's facility. All Face-to-Face meetings will be held at the Government's facility located at VA San Diego 3350 La Jolla Village Drive, San Diego California 92161. Normal workdays are Monday through Friday, except US Federal Holidays. Typical workdays are eight (8) hours per day, forty (40) hours per week. Core hours of work are from 0800 am to 1630 pm daily. Work shall not take place on Government site after normal working hours, on weekends, or on Federal holidays unless specified in the contract or approved by the Contracting Officer's Representative (COR). Some weekend hours are expected (i.e., inventory services, activation services).

There are eleven (11) Federal holidays set by law (USC Title 5 Section 6103) that the Department of Veterans Affairs follows:

- **A.** Six (6) Federal holidays are set by day of the week and month:
  - **A.** Martin Luther King's Birthday - Third Monday in January
  - **B.** Washington's Birthday - Third Monday in February
  - **C.** Memorial Day - Last Monday in May
  - **D.** Labor Day - First Monday in September
  - **E.** Columbus Day - Second Monday in October
  - **F.** Thanksgiving - Fourth Thursday in November
- **B.** Five (5) Federal holidays are set by date. If any of these dates fall on a Saturday, the Friday before shall be observed as a holiday. If any of these dates fall on a Sunday, the following Monday shall be observed as a holiday.
  - **A.** New Year's Day - January 1st
  - **B.** Juneteenth – June 19th
  - **C.** Independence Day - July 4th
  - **D.** Veterans Day - November 11th
  - **E.** Christmas Day - December 25th
- **C.** Any other Federal Holiday declared by the President of the United States

10.0 Reserved

11.0 Travel

Cost-reimbursable travel will be included in the final award based upon the Government's estimated need. The Government will not reimburse any living or relocation costs of IOTA contractor employees from other geographic areas. The purpose of staffing the contract is considered the cost of doing business and is not subject to reimbursement. It is the responsibility of the IOTA contractor to mobilize employees and pay living expenses for non-local employees, if it is necessary IOTA contractor personnel be located near project site.

Local travel, within a 50-mile radius from the place of performance will not be reimbursed. The Government will not pay travel charges for travel to and from the IOTA contractor employee's home and government office or from one Government facility to another. Travel beyond a 50-mile radius of the contractor's facility are authorized for reimbursement on a case-by-case basis and must be pre-approved by the Contracting Officer's Representative (COR) via the Travel Authorization Request (Attachment B). The IOTA contractor must obtain written approval from the VA COR **BEFORE** any travel begins, utilizing the Travel Authorization Request form. Other documents or e-mails will not be accepted as pre-approval. Travel that occurs without written pre-approval will not be reimbursed. Travel expenses will be reimbursed on an actual expenditure's basis in accordance with FTR and FAR 31.205-46. Per diem expenses will be paid per the GSA daily rates for the location of travel. To be reimbursed for travel, the IOTA contractor shall submit supporting documentation as required by FTR with invoices. FTR requires for any temporary travel destination you must provide a receipt to substantiate your claimed travel expenses for lodging and a receipt for any authorized expenses costing over $75 (FTR 301-11.25). Expenses for subsistence and lodging will be reimbursed to the IOTA contractor only to the extent where an overnight stay is necessary and authorized by FTR in effect at the time of the stay for the specific location. Approval for rental vehicles is discouraged and will be approved on an individual basis. Additional information can be found at GSA FTR.

12.0 Key Personnel

The IOTA contractor shall provide the necessary qualified personnel, materials, resources, and infrastructure to manage, perform, and administer the contract. The IOTA contractor shall accomplish the assigned work by employing and utilizing the identified key personnel with appropriate combinations of education, training, and experience as well other identified personnel with education and experience appropriate for the tasks assigned.

The personnel identified herein are considered essential to the work being performed. In the event changes to key personnel are required during the performance of this contract, replacement key personnel must meet the minimum requirements of the PWS. Prior to substituting, removing or replacing any key personnel, the IOTA contractor shall notify the CO and COR 10 working days in advance. The CO and COR will evaluate the replacing person's resume to determine the experience and qualifications of the replacement meet the requirements of the PWS. New IOTA personnel shall not commence work until all necessary security requirements have been fulfilled and résumé provided and accepted. The CO and COR will evaluate such requests and promptly notify the IOTA contractor, within 5 business days of approval or disapproval in writing

For the purposes of this contract, key personnel are listed below:

A. IOTA Activation Project Manager

- **A.** A minimum of seven (7) years' experience as a Project Manager, acting in a lead role over healthcare-related projects
- **B.** Demonstrated experience in scientific research infrastructure, operations, and/or practice and have direct experience in transition activities.

B. IOTA Senior Designer

- **A.** A minimum of five (5) years of experience in healthcare facility design
- **B.** National Council for Interior Design Qualification (NCIDQ) Certification or Certified Healthcare Interior Designer (CHID) certification
- **C.** Demonstrated experience in healthcare operations and related furniture, fixtures, casework/case goods and signage, and be able to translate requirements into design/construction/installation documents

C. IOTA Senior Transition Planner

- **A.** A minimum of three (3) years of experience in transition planning and relocation services on multi-phased scientific research building projects
- **B.** Experience in healthcare/research setting.
- **C.** Demonstrated experience in conceptual advance planning, identifying occupancy milestones, detailed implementation planning and move sequencing, preparation and setup, compiling documents of detailed move plans for each inter-departmental impact, and relocation execution.

13.0 Employee Identification

All IOTA contractor employees working at a Government facility shall wear company Identification and Government issued identification to distinguish themselves as contractor personnel. When conversing with Government personnel during business meetings and over the telephone, IOTA contractor employees shall identify themselves as such. Where practicable, IOTA contractor employees occupying space within a government facility should identify their workspace area with their name and company affiliation.

14.0 Conduct of Personnel

The CO may require the contractor to remove from the job site any IOTA employee working under this contract for reasons of misconduct, security violations, or found to be or suspected to be under the influence of alcohol, drugs, or other incapacitating agents. IOTA contractor employees shall be subject to dismissal from the premises upon determination by the CO that such action is in the best interests of the Government. Such removal from the job site or dismissal from the premises shall not relieve the IOTA contractor of the requirement to provide sufficient personnel to perform the services as required by this contract.

15.0 Contract Kick-Off Meeting

The Government activation team will schedule telephonic IOTA Kick-Off meeting for this contract after award. Attendees shall include the general contractor, key stakeholders including representatives of the Research Department, site activation team, IOTA Contractor, subject matter experts, Regional Activation Support, COR, CFM Resident Engineer, and the CO. The IOTA contractor, in collaboration with the COR and CO, shall coordinate dates and an agenda. The COR will include the Resident Engineer to complete a roles and responsibilities review of the construction project and activation project during the kick-off. The IOTA contractor is to provide meeting minutes within three (3) business days after the Kick-Off meeting. At the Kick-Off meeting, the Government will discuss administrative functions (i.e., security background process, reporting, COR responsibilities, invoicing, deliverable submission process), and contractual expectations. The IOTA contractor shall be prepared to present the details of the intended approach, work plan, and project schedule, as well as make IOTA personnel introductions. IOTA contractor will be given the opportunity to clarify contract requirements and expectations. The Government may elect to do a telephonic contract administrative kick-off meeting immediately following contract award, and an on-site programmatic kick-off meeting separately.

16.0 Tasks and Deliverables

This contract includes base contract tasks and optional tasks. Optional tasks are those tasks the Government may elect to award via contract modification at a future time if a need is identified during various phases of the construction and activation schedule. Optional tasks are pre-priced on a firm-fixed-price basis; however, optional tasks will be funded at the time they are exercised. The Government may elect to exercise none, some, or all of the optional tasks defined below, at any phase during of the activation project.

16.1 Comprehensive Project Management Services

Provide comprehensive Pre-planning and Activation Project Management Services integral to the execution of tasks ensuring effective, efficient, and timely completion of contracted services. The IOTA Activation Project Manager shall not be reassigned without notification to the CO. The IOTA Activation Project Manager may be required to be onsite as required per contract and lead user group and Integrated Project Team (IPT) meetings, installation activities, and project closeout. The IOTA Activation Project Manager will ensure close coordination with the design and construction efforts of the building contractor

Project Plans, Schedules, and Reports:

The IOTA contractor shall support the VHA Activation Team's planning, scheduling, and reporting requirements.

The IOTA contractor shall support the Facility Activation Project Manager in establishing a local level Integrated Project Team (IPT). The purpose of the IPT is to provide timely input to concept and design development, identification, planning, and execution of procurement functions, and logistical and operational requirements in order to bring the project into operation. Stakeholder engagement is vital to a successful outcome. IPT members should include, at a minimum: Research Department, local OI&T, Infection Control, Emergency Safety & Preparedness, Logistics, Patient Safety, facility Fiscal office, Privacy, Lock Shop, Police, Environmental Management, project Resident Engineer, local Union representation, Biomedical Engineering, Interior Design, local Contracting, public affairs, and others as required depending on project type and scope.

The IOTA contractor is also responsible for developing an Activation Integrated Master Schedule (AIMS) which integrates activation activities, Construction Project/Schedule, and the VA Information Technology Project Schedule, etc. The AIMS shall be coordinated with the CFM contract dates and the Lessor/building contractor's construction schedule.

In managing the AIMS, the IOTA contractor shall advise the Government of suspense dates that need to be met by the Government and/or Government contractors to ensure on-time execution such as, but not limited to, delivery dates for items purchased by the Government, information that the contractor needs from the Government to complete the requirements of this PWS, and certain IMS milestone dates. The IOTA contractor is responsible for tracking these dates and keeping the parties informed. However, the IOTA contractor is not responsible for

enforcing dates or ensuring work is completed on schedule to the extent the dates and/or work are not a requirement of the IOTA contractor as described herein. The IOTA contractor shall report in a timely manner any schedule deviations to the Activation Team, CO and COR. Upon the Government's acceptance of the schedule deviation, the IOTA contractor shall prepare and submit for approval a revised AIMS.

In the event a schedule deviation impacts the period of performance of this contract, the IOTA contractor shall provide in writing to the CO the reason for the delay, associated points of contact, and a request for extension. Extension requests must detail the amount of additional time required and are not automatically granted. The IOTA contractor shall document lessons learned throughout the project in the monthly status report.

#	Deliverable Name	Deliverable Description
16.1.1	Monthly Project Status Report	The Monthly Project Status report shall give an overview of the progression of the project and describe the work completed during the reporting/billing period. The report shall include status of milestone items in the Master Project Schedule, discuss moderate to high-risk items, and a summary of meetings attended. The report shall discuss any “lessons learned” during the reporting/billing period. If there are any changes to staff (prime or sub), or Key Personnel change during the month, and updated Attachment C, Contract Staff Roster shall be included. The Monthly Project Status Report shall correlate to and be submitted with the monthly invoice. The report shall cover the same time period as the invoice. During the months of acquisition support, the report shall provide a graph of equipment purchased, remaining, pending market research, approval or deferred to include percentages complete and dollar amounts.
16.1.2	Activation Integrated Master Schedule (AIMS)	The AIMS shall be a color coded, time-lined graphic which marks the start and end dates of major element or sub-element milestones/gateway of construction which may impact the start, duration, or completion date of scheduled IOTA tasks, shows major start and end dates of milestone/gateway events for purchased items, shows scheduled activities in activating or approving building systems and support contracts, and shows IOTA events which may be impacted by schedule acceleration or slippage by others. A complete AIMS will include and demonstrate all construction milestone/gateway dependencies with both Government and contractor IOTA-related processes from contract award to the completion of the contract itself. The schedule shall track all major milestones to demonstrate effective management and execution of the project by the IOTA contractor, illustrate timely performance, and identify delays or potential delays to the project. The schedule shall be coordinated with the lessor/building contractor’s IMS to ensure IOTA contractor’s deliverables, reviews, submittals, and milestones do not delay or conflict with the lessor/building contractor’s schedule. The lessor/building contractor’s schedule shall be given priority. The schedule shall include dates from the construction schedule through Day One (commencement of R&D facility services) and project closeout. The schedule shall identify key tasks, start and completion dates, and the duration of tasks to be completed by the contractor to satisfy the requirements of the PWS. The IOTA contractor shall annotate any schedule deviations in monthly updates. Milestones must include Activations FY2026-Term of the Lease budget requests, Activation Management Plan complete, construction contractor need by date for VC items, Order VC items, construction contractor need by date for High-Cost High Tech (HCHT) equipment, funds to the NAC by date for HCHT equipment, Equipment testing, First Use.

16.1.3	Individual Service Project Schedules	IOTA contractor shall develop a detailed Individual Service Project Schedule created from the Activation Project Schedule to provide individual reports to specific services. The details included in the Activation Project Schedule shall also be included in the Individual Service Project Schedules
16.1.4	Risk Management Plan and Log (Attachment D is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool Note: Contractor shall utilize SharePoint to enter data directly into system)	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION TOOL BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE The IOTA contractor shall update and maintain the Risk Management Plan. The plan shall include an itemized listing of project-specific risks, challenges and perceived problems that are anticipated to threaten the project. Risks identified shall include probability of occurrence, and level of impact. With each issue specified, the contractor shall list their proposed solution to mitigate or resolve the risk/challenge/problem. The plan shall cover all phases of the work. When identifying risks/solutions the contractor should consider items in areas that may cause the project to: **A.** Not be completed on time. Proposed execution schedule will be evaluated as part of the technical factor **B.** Not finish within budget **C.** Generate change orders **D.** Result in owner dissatisfaction **E.** Result in poor quality of services; and/or **F.** Any other areas identified by the IOTA contractor. Risk Management shall be a regular coordination meeting agenda item to ensure Risks are being managed per the RMP. The existing Risk Register on the Government SharePoint site shall be updated as additional risks are identified through coordination meetings or day-to-day project execution.
16.1.5	Change Management Plan and Log (Attachment E is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool Note: contractor shall utilize SharePoint to enter data directly into system)	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION TOOL BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE Change Management applies to requests from user/user groups for changes to equipment lists resulting in impact to infrastructure requirements, and equipment and building layouts. The contractor shall coordinate with the SRE (or R/E) through the COR to identify cost, schedule, and scope impacts. The IOTA contractor shall work with the COR to identify appropriate members for a Change Management Committee, which will include key VA personnel and contractor personnel, and may include participation by representatives of the non-VA contributors to this project. The Change Management Plan shall develop processes for submitting, reviewing, and approving or disapproving change requests. The Change Management Committee will review all change requests and make recommendations to the Medical Center Director or their designee, who is the final approval authority for all proposed changes. The IOTA contractor shall provide a monthly report of the Change Management Committees activities, including minutes from any meetings, and maintain a running tally via the VA provided SharePoint site of all change requests, their status, and their impact on project cost and schedule. The IOTA contractor shall document requested and approved changes to the FF&E in a change management log. IOTA contractor shall not direct changes. Any

		changes with infrastructure or space impacts will need coordination with the RE to determine any scope, schedule, or cost impacts prior to submitting for approval.
16.1.6	WBS (Attachment F)	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION TOOL BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE The IOTA contractor shall maintain/update/track the Government provided WBS on the SharePoint site. The WBS is to be updated to reflect the current project, current status, and changes as they occur throughout the life of the project. IOTA contractor can utilize the provided file by changing and updating as needed or can create a new file with consideration of tasks on the VA provided file, using software which can be opened by VA team members.
16.1.7	Integrated Project Team (IPT)	IOTA contractor shall draft an IPT Charter, to include IPT roles and responsibilities of stakeholders and the identification of individual members, and IPT member nominations letters. The IOTA contractor shall update the IPT letters and charter throughout the requirement accounting for any changes.

Government Provided Share Site for Information Sharing:
The IOTA Contractor shall use the Government-provided SharePoint site for project documentation and information sharing through the provided SharePoint lists and subsites. The VA SharePoint can only be accessed by individuals with a VA email address and network access. Project deliverables, schedules, reports, and management plans (all versions and final as applicable) shall be shared with the Government by posting on the Government-provided SharePoint site document libraries, lists, and subsites. IOTA Contractor shall complete, update and maintain all versions of project deliverables as required per the deliverable schedule and posted on the Government SharePoint site. All project documentation shall be compatible with systems utilized by the medical facility with files downloadable by all parties.

Project deliverables, schedules, reports, and management plans shall be shared with the Government by posting on the Government provided SharePoint site. IOTA Contractor shall update and maintain all versions of project deliverables as required per the deliverable schedule and posted on the SharePoint site, unless otherwise agreed upon by the COR, CO and VHA Activation Program Manager. Revisions to schedules and plans since the last update shall be tracked and clearly identified. The project SharePoint site is the official Activation Project Management site for all project working documents and deliverables, as well as the location for lists and subsites for all data sets to be worked throughout the lifecycle of the Activation project. At the end of the contract, all deliverables are to be turned over and/or coordinated for download between the IOTA contractor and the COR.

Where SharePoint tools are available, the IOTA contractor must utilize the tool and complete and update as necessary, all fields. Data shall be input directly into the SharePoint tool, in lieu of other formats (i.e. excel). Contract attachments provided are representations of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool. Tools shall be completed and updated as the project works through the Activation process. The SharePoint tools are intended to be live databases, where the actual work is done. As a result, periodic bulk updates from other formats such as excel, should not be necessary.

#	Deliverable Name	Deliverable Description
16.1.8	SharePoint Site	IOTA contractor shall update and maintain all versions of project deliverables as required per the deliverable schedule and posted on the Government SharePoint site. The SharePoint site is the official Activation Project Management site for all project documents/information.

Meeting Facilitation Services:

The IOTA contractor shall provide group facilitation services to key stakeholders, Integrated Project Team (IPT) and work groups for meetings required to perform contract PWS tasks. Key stakeholders include, but not limited to, Representatives of the Research Department, Activation Team Members, Integrated Project Team members, and Program Support Staff from Facilities, Medical Maintenance, and other project-related Government and Medical Staff as necessary. The IOTA contractor may identify additional ad hoc groups as approved by the COR. The IOTA contractor shall guide groups to consensus by identifying requirements, facilitating group discussions, and documenting decisions. The IOTA contractor shall coordinate meetings, and facilitate the groups to assess, analyze, recommend, and document solutions as developed jointly by the contractor and the stakeholders and/or group members.

The IOTA contractor shall be responsible for coordinating and planning. The IOTA contractor shall coordinate the meeting locations and audio/visual support as needed for these meetings with the COR. The COR will finalize arrangements with the facility for rooms and audio/visual support. For meetings requiring teleconferencing capability, the IOTA contractor shall provide the teleconferencing service and call-in numbers and host the meetings. The IOTA contractor shall not meet with any end users, the A/E firm, the construction contractor, etc. without first coordinating with the CFM RE, COR, and VA PM. The IOTA contractor shall participate in design/construction meetings as determined by the COR.

It should be noted that prior to award of this contract, CFM worked diligently with the VAMC to produce the Lease Contract and its corresponding appendices. This includes workflows, the program for design (PFD), floor layouts, room contents list (i.e. general equipment list Attachment Q), agency specific requirements, IT requirements, security requirements, and janitorial requirements produced in the awarded Lessor contract. The Lessor is the only party that is allowed to make changes to the items above (with the exception of the room contents list). All Lessor changes must be discussed with Research Department and approved by the CFM Administrative Contracting Officer (ACO). Otherwise, it is the Lessor's responsibility to ensure contract compliance regarding these items.

The IOTA contractor may not make changes to the items above (with the exception of the room contents list – provided there is no impact to infrastructure requirements). Any changes resulting from such an instance without the approval of the CFM RE will be borne on the IOTA contractor. In regard to changes to the room contents list, the IOTA contractor is allowed to make changes only within the lease/building contract parameters, with approval of user groups, including Research Department leadership. This would entail further defining equipment listed in the room contents list in Attachment Q. The IOTA contractor will also be responsible for scrubbing the equipment list via user group meetings, to identify any equipment that is to be deleted or added.

The IOTA contractor will be responsible for the equipment planning within the contractual boundary of the CFM Contract Room Content List and defined floor layouts. Any deviations will have to be routed through the COR and approved through the CFM RE and CFM CO and in discussion with Research Department leadership.

The IOTA contractor shall assure that all appropriate personnel are invited to attend each meeting either telephonically or in person. The IOTA contractor's PM shall be available to attend requested meetings in person, as determined by the COR prior to the meeting. Beyond the IOTA contractor's Project Manager, the total number of personnel required to attend meetings to support successful execution of the work for any given meeting is to be determined by the IOTA contractor and must be approved by the COR.

#	Deliverable Name	Deliverable Description
16.1.9	Meeting Minutes and Meeting Agendas	Agendas shall be distributed no less than 3 Days prior to the meeting. IOTA contractor to work with COR or designee in creating the agendas. VA meeting agenda template to be used if available Minutes shall be distributed no more than 5 Days post meeting. Minutes of all meetings shall include agenda, attendees, action items and who is responsible

		for completion of the action items. If the facility has a standardized template, that template must be used.

PWS Deliverable Updates:
After initial acceptance of any developed deliverable under any of the task(s) identified in the PWS, those deliverables will be updated and maintained as part of the Comprehensive Project Management Services Task.

#	Deliverable Name	Deliverable Description
16.1.10	PWS Deliverable Updates	Updates must be completed no later than 10 business days after identification of need by either the Government or the IOTA contractor. Note: all updates shall reference this deliverable and the original deliverable numbers (i.e 15.1.11 update for 15.2.1)

16.2 Comprehensive Interior Design, FF&E, and Space Planning Services

Provide and coordinate comprehensive interior design (CID) services or coordination of CID services, ensuring incorporation of Research & Development Design Guide and laboratory safety concepts. FF&E must complement any interior packages developed by the Architect/Engineer firm associated with the construction project and/or the healthcare/Research facility's standards as provided by the Government. The IOTA contractor may be required to identify FF&E to purchase, receive and install FF&E and visual arts and/or inventory, uninstall, pack, transport and reinstall existing FF&E and visual arts in the health care facility's current inventory identified for reuse in the new facility following approval by the COR. Design support services include preparing cut sheets for FF&E and artwork, updating the room's content list on the Government's SharePoint site, including updating spaces to be consistent with A/E drawings. IOTA contractor is to work closely with the VA Interior Designer on all furnishings, space planning, and selections. IOTA contractor shall ensure all selections are in accordance with the CD's to avoid conflict resulting in either design or construction modifications.

IOTA Contractor may provide their own system for tracking, managing and validating FF&E, however the Government provided SharePoint site must also be updated and maintained at all times. It is the official repository for all project information and is utilized by outside bodies for budgetary and tracking purposes. The IOTA Contractor is responsible for promptly transferring and/or updating to the Government provided SharePoint, all information tracked and managed using any other contractor provided system. The IOTA contractor will be validating all FF&E and defining all salient characteristics. "Validating" in the sense means a generic item has been identified by a specific manufacturer and model has not yet been identified. The IOTA contractor shall then develop the list to the "Approved" phase. "Approve" in this sense means the manufacturer and model has been selected, to include the salient characteristics of the item. The IOTA contractor will be responsible for finalizing furniture, fixtures, and artwork with the appropriate VA IPT representative to sign off on the final cut sheets and specifications. The COR (or other designated representative decision authority) will direct the IOTA contractor to the appropriate stakeholder for approval.

The IOTA contractor will be responsible for identifying salient characteristics for all FF&E with end users and the VA Interior Designer for recording in the FF&E tracking system. This also ties into the acquisition support services required under this PWS as the identified salient characteristics will be included in "brand name or equal" procurement packages. A completed Justification and Approval (J&A) form will be required to be included in any procurement packages for any items that require a specific manufacturer or model.

The IOTA contractor is to ensure all identified FF&E or significant architectural items are in accordance with the Design Documents to minimize any need to change the Mechanical, Electrical, Plumbing or Architectural support systems and locations. Any impact to MEP resulting from equipment changes must go through the Change Request process. The IOTA contractor shall utilize Space, Equipment, and Planning System (VA-SEPS) Joint Service Number

(JSN) nomenclature in accordance with the VA BIM Guide (available at VA BIM GUIDE, https://www.cfm.va.gov/til/bim/VA-BIM-Guide.pdf) for all unique ID numbering. The cut sheets shall identify the basis of design item and shall show appropriate VA-SEPS JSNs. New JSN requests and JSN searches can be conducted at https://dha.max.gov/milstd1691. The IOTA contractor shall develop a Rough Order of Magnitude (ROM) to include estimated costs for storage, delivery, and installation.

The general contractor will be required to identify all Mechanical Electrical Plumbing (MEP) information necessary, and timelines needed. The IOTA contractor is to develop the make and model of all equipment with the Design Documents. The VA will be responsible for providing the correct POC's as designees to the IPT, for the user group meetings who have the authority to make equipment decisions, such as identification of make and model of equipment, locations for all equipment, and any J&As planned for the procurement of specified equipment. The IOTA contractor is to ensure all identified FF&E or significant architectural items are in accordance with the Design Documents to minimize any need to change the Mechanical, Electrical, Plumbing or Architectural support systems and locations.

Contractor to provide mock-ups via 3D modeling (Latest versions Revit, AutoCAD, and Bluebeam) of Research facility identified spaces which can include potentially room, procedure spaces, laboratories, research and other complicated research environments.

#	Deliverable Name	Deliverable Description
16.2.1	FF&E Cut Sheets	Cut Sheets shall include a photo of the item, finishes, specifications, instructions, dimensions, etc., that apply to that specific item. Cut sheet information shall be specific enough to convey information to the VA as they will need to purchase and install the product, but general enough to allow competition across multiple manufacturers. IOTA contractor shall prioritize cut sheets for long lead time items.
16.2.2	Master Key Plan	Develop Master Key plan to include door/furniture cores and electronic and mechanical access control devices. The plan should include an assessment of compliance with applicable Homeland Security and VA security requirements. **A.** Provide a list of new cores and staff assignment to assist VA Locksmith in making the cores and keys required and PIV access **B.** Develop Key plan and access control plan should be based on security design requirements for access control
16.2.3	Room-by-Room Master Equipment and Furniture List (MEL) (Attachment G is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool	The Room-by-Room MEL (captured using the SharePoint list, identifies all items listed by room. The MEL shall include reuse when applicable. The IOTA contractor shall provide a complete and finalized room by room activation SharePoint list for each service/area throughout the R&D facility. The IOTA contractor shall perform QA against the Design Documents to avoid conflict. Initial Data collected, updated, and maintained in the SharePoint list includes space identification that matches construction drawings, VV vs VC vs CC, item cost to include any purchased install and/or training, contracting and vendor lead and install times, funding appropriation, recurring vs non-recurring expense.

	Note: IOTA contractor shall utilize SharePoint to enter data directly into system)	
16.2.4	FF&E Layouts	Space plans showing FF&E furniture and equipment placement. FF&E layouts are to be used for end-user/VA designer group meetings, to assist in the validation of the FF&E, and to facilitate outfitting as an installation guide. Items shall be color-coded on the drawings for easy identification (i.e. red for reuse, black for construction contractor provided and installed, green for manufacturer installed). The initial layouts will be for the typical rooms in the concept drawings for the VHA Research & Development Facility. Updated drawings will be provided to update FF&E placement using basis of design dimensions using Revit. The IOTA contractor is to ensure all identified FF&E or significant architectural items are in accordance with the Design Documents to minimize any need to change the Mechanical, Electrical, Plumbing or Architectural support systems and locations. The IOTA contractor will work closely with VA Interior Designer. Hard copies and digital copies shall be available to the VA as soon as an update is completed. Floor plans and elevations to be printed on half-size sheets (15”x21”). All others may be printed on 11”x17” or 8.5”x11” paper with a 1/4" scale.
16.2.5	3-Dimensional Design Renditions	3D design renditions of FF&E items within planned spaces using SketchUp, AutoCAD, or another similar program. (End users to develop and provide a list of expected room types being sought for 3D rendition to the IOTA).
16.2.6	Rough Order of Magnitude (ROM)	The ROM is the total estimated cost by item to purchase, warehouse, delivery, install, test, and train (as applicable) for the project. The ROM should be provided at DD1, DD2, CD2, and final acquisition packages.
16.2.7	Mock-up services and Mock-up Report	Provide mock-ups via 3D modeling (Lastest versions Revit, AutoCAD, and Bluebeam) of Research facility identified spaces which can include potentially room, procedure spaces, laboratories, research and other complicated research environments. Facility shall provide an exact list of room required for physical mock-up. Mock-up report to include a report on all mock-up services completed and recommendations and finding that resulted from the mock-ups, to include user-feedback.
16.2.8	Design Submittal 1	IOTA contractor must deliver to the COR, used by the A/E all latest project information such as specific design requests as a result of user group meetings that occur prior to the delivery of DD1. Site activation team to provide due date of information to the A/E contractor to the activation contractor so to ensure A/E has time to include. Note: IOTA contractor shall upload directly into the SharePoint) Design submittal 1 shall include:

		A. Generic Cut Sheets for all JSNs for the equipment on the drawings if selected by the VA prior to activation contractor on-board. **B.** Room by room should match drawings and be reflected in the Contents Acquisition plan located on the Government SharePoint site. **C.** All Rooms Contents List (Attachment G). Attachment G is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool. **D.** Inventory of existing FF&E recommended re-use report which includes data sheets for any selected re-use. **E.** A report that identifies all conflicts between identified FF&E and A/E Design Documents
16.2.9	Design Submittal 2	IOTA contractor must deliver to the COR, used by the A/E all latest project information such as specific design requests as a result of user group meetings that occur prior to the delivery of DD2. Site activation team to provide due date of information to the A/E contractor to the activation contractor so to ensure A/E has time to include. Note: IOTA contractor shall upload directly into the SharePoint) Design submittal 2 shall include: **A.** Basis of Design Cut Sheets for all JSNs for the equipment on the drawings if selected by the VA prior to the activation contractor on board. **B.** Room by Room should match drawings and be reflected in the Contents Acquisition plan located on the Government SharePoint site. **C.** All Rooms Contents List (Attachment G). Attachment G is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool. **D.** A report that identifies all conflicts between identified FF&E and A/E Design Documents
16.2.10	Equipment Reuse and Disposal Plan (Attachment I is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool Note: IOTA contractor shall utilize SharePoint to enter data directly into system)	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION SharePoint List BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE The IOTA contractor shall develop and maintain an FF&E Reuse and Disposal Plan to ensure full coordination of activities, and that the information updated reflect status and changes as they occur throughout the life of the project. The Equipment Reuse and Disposal Plan should outline how the IOTA contractor will determine if equipment is reusable. Equipment determined to be reusable shall be incorporated into the acquisition plan to ensure all reuse equipment is accounted for in the Final budget and procurement efforts. The Equipment Reuse and Disposal plan shall also describe how non-reusable equipment will be disposed and final location of disposed equipment (The Government will be responsible for disposing of non-reusable equipment). Accountable equipment whether reusable or designated for disposal will need to be coordinated with the Supply Chain Management Service to ensure equipment property records are accurately updated in AEMS/MERS.

16.3 Concept of Operations (CONOPS) Transition Planning, and Project Staffing Planning

The IOTA contractor shall facilitate CONOPS planning identified below. The IOTA contractor shall meet with key stakeholders in processes that involve multiple departments (to be determined after contract award) and facilitate groups to identify, determine and document key organizational CONOPS for use in the new facility.

A. **Micro (R&D facility wide operations) level CONOPs**: Assess current operations, define new operations, and obtain facility approval of business practices based on new conditions in space, equipment, staffing, and operations. Includes assessing how the programmed space and design will be used in the new facility in terms of best practices for vivarium and animal care and safety and security of laboratory staff, and document departmental hours of operation, workflow, staff workspaces, staff efficiency, egress of staff, movement of equipment and supplies within the department, and safety and security for staff, to include emergency preparedness. The current Attachment S Continuity of Operations (COOP) Plan is attached for reference.

B. **Transition and Preplanning Governance CONOPs:** High-level requirements and processes required to accomplish activation and preplanning activities. Transition CONOPs will detail transition from current state to the required future state at the new facility. Transition CONOPs shall support the schedule development and acquisition, installation, and occupancy timelines. The IOTA contractor shall provide detailed transition CONOPs by functional area. The IOTA contractor shall identify key requirements and constraints that will empower or impede decision making processes, approvals, or the ability to manage the activation activities. The IOTA contractor shall make recommendations for improvement where constraints, impediments, or other problems are identified. Recommendations cannot include changes that would require a change order and must work within the parameters of the project. This information shall be documented in the Transition Plan.

C. **General CONOPS:** Develop welcome/orientation kits for new employees, (i.e. facility maps, policies, service access, contact information, etc.)

D. **Project Staffing Planning:** The IOTA contractor shall facilitate Full Time Equivalent (FTEE) planning. The IOTA contractor shall meet with key stakeholders in impacted departments and facilitate groups to identify, determine, and document positions that should be transferred from existing facility and additional staffing/positions required to fully operate the new facility. The IOTA contractor shall report Full Time Equivalent Employee (FTEE) requirements by individual impacted departments and services. VA staffing requirements can be located HR Library and Resources Office of the Chief of Human Capital Officer (OCHCO) SharePoint at *http://vaww.va.gov/ohrm/HRLibrary/Dir-Policy.htm.*

#	Deliverable Name	Deliverable Description
16.3.1	Micro CONOPS	Micro CONOPS shall define how each specific operational unit conducts business. See task description above.
16.3.2	Transition CONOPS	Create and update Transition CONOPS. Transition CONOPS support the schedule development, acquisition, installation, and occupancy timelines. The contractor shall provide Transition CONOPS by functional areas. Transition CONOPS shall include a Day in the Life Plan, which describes the IOTA contractor's plans for preparing Day in the Life scenarios to help prepare employees to work in the newly activated space and identify gaps, concerns, or safety hazards in the newly constructed environment that can be mitigated and resolved prior to opening for Research Services. The IOTA contractor will work with the COR and the VHA SimLEARN lab to develop Day in the Life scenarios. The IOTA contractor will compile a single list of recommendations and outcomes for incorporation into transition CONOPS.

16.3.3	General CONOPS	The General CONOPS shall provide material to employees outlining policies, access, and contact information. It will also include facility maps.
16.3.4	Transition Plan	The IOTA contractor shall develop and maintain a transition plan ensuring that it is updated to reflect the current status and changes as they occur throughout the life of the project. The transition plan at a minimum should address all major actions necessary for successful completion of project. The transition plan should, at a minimum include a: **A.** Delivery and installation plan **B.** Government acceptance plan **C.** Temporary, building protection plan **D.** Security plan **E.** Sequencing and outfitting plan **F.** Calibration and testing plan **G.** Department master move schedule **H.** Department activity (individual service report) **I.** Cleaning and housekeeping plan **J.** Training plan **K.** Day in the life plan
16.3.5	Integrated Move Plan (Attachment H is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool Note: IOTA contractor shall utilize SharePoint to enter data directly into system)	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION SharePoint list BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE The IOTA contractor shall use construction drawings to update the existing move plan on the Government SharePoint site. IOTA contractor shall identify any special characteristics of the space.

16.3.6	Project Staffing Plan: Proposed FTE Report (Attachment J is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool Note: IOTA contractor shall utilize SharePoint to enter data directly into system)	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION SharePoint list BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE Proposed FTE report shall identify (at a minimum) the department/service, R&D facility/program, projected need date, position description, grade, current/proposed new # of FTEs, justification, estimated salary and benefits. See task description above.

16.4 ACQUISITION PLANNING SERVICES

The IOTA contractor shall develop the Acquisition Plan for the activation project. The Acquisition Plan located on the Government SharePoint site shall be updated to identify project spaces as identified on A/E drawing and, at a minimum, long lead time items, number of packages, and estimated timelines for procurement by package group. Additionally, other fields required by the SharePoint list should be completed as they occur throughout the procurement process. The contractor shall ensure employees performing acquisition services are well-versed in federal acquisition regulations prescribed by the FAR and the Veterans Affairs Acquisition Regulation (VAAR). NOTE: The number of acquisition packages has not been determined. Specific task(s) associated with this type of work include:

- **A.** Identify the number of procurement packages for the project using FF&E list.
- **B.** Develop an activation project acquisition plan.
- **C.** Identify new items to be purchased.
- **D.** Identify long lead-time items and submit the packages.
- **E.** Identify items that require early installation.
- **F.** Update the SharePoint list as packages work through the procurement process.

For VHA Healthcare furniture packages, the VHA is mandated to use the VHA Equipment Acquisition Strategy (EAS) Healthcare Furniture and Services IDIQ. The IOTA Contractor must adhere to any VHA mandatory procurement vehicles and templates created per contract. The IOTA Contractor will work with the local Interior Design team to create the furniture procurement packages using the templates provided by the EAS mandatory contract COR and CO, to include following the Ordering Instructions established for the mandatory contract for Using the Strategic Acquisition Center VHA Healthcare Furniture IDIQ, Minimum Technical Requirements (MTR) and other provided templates/documents. The local VA Interior Design team, or delegated personnel, will submit the furniture package through FORCE to the identified contracting office for acquisition. Updated templates will be provided by the identified contracting office or the local interior designer. IOTA Contractor will coordinate furniture delivery and installation according to the acquisition, installation and overall activation schedule and work closely with Interior Design Team.

The IOTA contractor shall determine if any items are available through sources listed on the National Acquisition Center Contract Catalog Search Tool (CCST). If an item is available through a CCST listed source, that information

shall be documented on the market research form. Items available through a mandatory source should be grouped, when possible, into one package.

For items not available through a mandatory source, the IOTA contractor shall group items into procurement packages in a manner which enables maximum competition among sources listed in priority order at VAAR 819.7004 Contracting Order of Priority when possible (i.e. SDVOSBs, VOSBs, other Economically Disadvantaged Small Businesses, Small Businesses, and then Other Than Small Businesses).

An example of mandatory sources (order of priority to be determined by awarding Contracting Office)

- **A.** National Acquisition Center Med Surg Catalog Search (Medical Surgical Prime Vendor)
- **B.** GSA eLibrary and GSA advantage
- **C.** National Strategic Source Listing – National Contracts, BPAs, and BOAs http://dsbs.sba.gov/dsbs/search/dsp_dsbs.cfm
- **D.** Unicor
- **E.** Ability One http://www.abilityone.gov/

Package Acquisition Lead Time (PALT) refers to the suitable length of time necessary for the VA to award a contract and shall be used by the IOTA Contractor during JSN requirement planning. The PALT timeline starts when a procurement requirements package is deemed actionable by the Contracting Officer and ends with the distribution of the award documents and obligation of dollars on the Purchase Order. An actionable purchase package contains all the elements required to begin the acquisition process; it includes and is not limited to a description of the requirement; an independent government cost estimate; an approved funding document; market research; relevant security checklist(s); and any other appropriate information determined necessary for the acquisition.

The IOTA Contractor shall use the VA PALT Table below to aid in planning purchase and delivery timeframes.

VHA PALT Standards

Action Type	Contract Type	Actions ≤10K	Actions >10K - ≤25K	Actions >25K - ≤250K	Actions >250K - ≤1M	Actions >1M - ≤7M	Actions >7M
DEFINITIVE	Architect/Engineering	30	60	60	120	120	180
DEFINITIVE	Commodities	30	60	60	120	120	180
DEFINITIVE	Construction	30	60	60	120	120	180
DEFINITIVE	Healthcare Resources	30	60	60	120	120	180
DEFINITIVE	Services	30	60	60	120	120	180
DO/TO	Architect/Engineering	30	30	45	45	60	90
DO/TO	Commodities	30	30	45	45	60	90
DO/TO	Construction	30	30	45	60	60	90
DO/TO	Healthcare Resources	30	30	45	45	60	90
DO/TO	Services	30	30	45	45	60	90
IDV	Architect/Engineering	30	60	60	120	120	180
IDV	Commodities	30	60	60	120	120	180
IDV	Construction	30	60	60	120	120	180
IDV	Healthcare Resources	30	60	60	120	120	180
IDV	Services	30	60	60	120	120	180
PO	Architect/Engineering	30	30	45	60	90	120
PO	Commodities	30	30	45	60	90	120
PO	Construction	30	30	45	60	90	120
PO	Healthcare Resources	30	30	45	60	90	120
PO	Services	30	30	45	60	90	120

#	Deliverable Name	Deliverable Description
16.4.1	Room Contents and Acquisition Plan	IOTA CONTRACTOR MUST UTILIZE OCAMS ACTIVATION SharePoint list BUILT INTO THE GOVERNMENT PROVIDED PROJECT SPECIFIC SHAREPOINT SITE

	(Attachment G is a representation of required data/information. Actual deliverable data/information requirements are defined in SharePoint tool Note: IOTA contractor shall utilize SharePoint to enter data directly into system)	The IOTA contractor shall update and maintain the Room Contents & Acquisition Plan on the Government SharePoint site to include a procurement package list (how the procurement packages should be organized), how many packages are anticipated to be needed, milestone dates to ensure the FF&E is available to meet the project schedule, and any identified associated risks and mitigation suggestions. The IOTA contractor shall verify and update the SharePoint acquisition plan spaces to be consistent with final design drawings. The plan shall include a schedule to identify the number of procurement packages by type (procurement packages, credit card packages, ECAT packages, furniture/artwork packages, and any other mandatory VA ordering package), date needed to "procure by" to account for acquisition timelines (See PALT schedule) as well as manufacturing lead times, delivery dates, planned installation dates, and where each package is in the process. The schedule shall also identify the deadline to have the package in for Government review prior to submission to contracting for acquisition. The plan shall highlight FF&E identified as long lead time items to ensure time frames can be incorporated into the transition plan. The plan should be utilized to monitor ongoing reconciliation of the FF&E budget and schedule. It should contain any specific information related to equipment procurements, responsibility of FF&E (VA, VV, CC, etc.) as well as funding appropriation for any VC or VV items. When applicable, the plan shall identify the appropriate Minimum Technical Requirement (MTR) number for each JSN.

16.5 Acquisition Packages Development

The IOTA contractor shall develop procurement packages for items to be procured based on information provided by end users and VA Interior Designers during user group meetings. The IOTA contractor shall use the Procurement Package Checklist (Attachment L) to determine package completeness. The Procurement Package shall include a completed Procurement Package Checklist, and all documentation needed in accordance with the completed checklist. Minimum procurement package requirements are as follows:

- **A.** Assist with coordinating the approval of VA Form 2237 Procurement Request.
- **B.** Completed Procurement Package Checklist (Attachment L)
- **C.** Completed Market Research Form (Attachment L)
- **D.** Completed Handbook 6500.6 (Checklist for Security Requirements) with appropriate signatures (Attachment L)
- **E.** Complete description of the Government requirement (e.g. item description, quantity, basis of design to include model and salient characteristics (as defined in VAAR 811.001) cutsheet images if needed, for "or equal quotes."
- **F.** Estimate of cost.
- **G.** Delivery requirements (e.g. warehouse address, required delivery date range, warehouse points of contact).
- **H.** Vendor installation/delivery requirements (e.g. instructions for coordinating delivery with warehouse POCs, special requirements for installation).
- **I.** Provide IOTA contractor support to develop complete procurement packages of the FF&E to include, but not limited to, the SOW, Independent Government Cost Estimates (IGCEs), market research, brand name/sole source justifications, and route security documents for signature.
- **J.** Work with the identified Government contracting office to submit complete procurement packages for award.

K. Make edits/changes to procurement packages based on review and requires approval by VA Designated Representative Decision Authority or VA Interior Design Team for furniture, and/or recommendations from the identified Government contracting office making award.

L. IOTA contractor shall identify special delivery requirements and any warehousing site constraints (e.g. lift gates, loading docks, etc.)

M. Assist with gathering all documents to be uploaded into SEPG & EER will be done by the Government.

N. The contractor is responsible for providing complete and accurate procurement packages. Procurement packages must be approved by a CO at the Contracting Office that is responsible for procuring the items/service in the acquisition package.

O. Provide updates to the acquisition plan and schedule as necessary.

The Interior Design team shall submit furniture related VA Form 2237 requests. Research staff will submit all equipment related procurement packages and 2237s. The designated government service will upload all package documents produced as required by this section to the contracting office via Forecast of Opportunities and Requirements Center for Excellence (FORCE), which can be accessed at the Acquisition Knowledge Portal (AKP) at http://vaww.ecms.va.gov/CARE/ on any computer that has VA network access. An Electronic Contract Management System (eCMS) account is required the government service. Government employees performing this function shall review the training slides located on the FORCE site as well as any additional FORCE training as required. The Interior Design team will ultimately submit the approved package through FORCE, along with the approved 2237.

The IOTA contractor shall determine if any items are available through sources listed on the National Acquisition Center Contract Catalog Search Tool (CCST), available at https://www.va.gov/nac. If an item is available through a CCST listed source, that information shall be documented on the market research form. Items available through a mandatory source should be grouped, when possible, into one package.

For VHA Healthcare furniture packages, the VHA is mandated to use the VHA Equipment Acquisition Strategy (EAS) Healthcare Furniture and Services IDIQ, ECAT and Pcards. IOTA contractor will work with the local Interior Design team to create the furniture procurement packages using the templates provided by the EAS team. The furniture package will be sent to the identified contracting office for acquisition. A sample of the EAS Furniture templates and ordering guide are provided for in Attachment K. Updated templates will be provided by the identified contracting office or the local interior designer. IOTA contractor will coordinate furniture delivery and installation according to the acquisition, installation and overall activation schedule.

For items not available through a mandatory source, the IOTA contractor shall group items into procurement packages in a manner which enables maximum competition among sources listed in priority order at VAAR 819.7004 Contracting Order of Priority when possible (i.e. SDVOSBs, VOSBs, other Economically Disadvantaged Small Businesses, Small Businesses, and then Other Than Small Businesses). The IOTA contractor is responsible for providing complete and accurate procurement packages. Procurement packages must be approved by a CO at the Contracting Office that is responsible for procuring the items/service in the acquisition package.

IOTA contractor employees shall identify themselves as such when communicating with vendors while conducting market research. IOTA contractor employees shall not give the impression that they are obtaining quotes on behalf of the Government when obtaining estimated prices for market research. IOTA contractor employees shall not communicate with vendors regarding an open solicitation. All communication with vendors regarding an open solicitation shall be through the Contracting Office responsible for the solicitation.

The IOTA contractor shall work with the Contracting Office in the event incorrect or damaged items are received.

#	Deliverable Name	Deliverable Description

16.5.1	Procurement Packages	Procurement packages shall be developed in accordance with the terms specified in the PWS. Procurement packages shall be prioritized by estimated lead times. IOTA contractor shall report on all procurement packages submitted through FORCE to the acquiring contracting office and COR.

16.6 Relocation of Reuse and Personnel Files

IOTA contractor to provide for all labor, materials, transportation, and equipment for the relocation of Reuse equipment, personnel files, and expendable/non-expendable supplies. IOTA contractor to provide the physical relocation of miscellaneous supplies, equipment, etc. into the new space. Proper logistical requirements will be provided by the VA Research Department for any specialized equipment that is identified for re-use and relocation. A non-exhaustive list of equipment to be moved for reuse is included in Attachment R.

The Research Department has approximately 12 research teams (approximately 35-50 individuals in total) for relocation from the main hospital campus 3350 La Jolla Village Dr. San Diego, CA 92161 and off Campus-Adjacent Building located 9575 Gilman Dr. La Jolla, CA 92093.

Each research team represents a research laboratory with research materials not limited to documents, supplies, chemicals and biological agents, and biomedical laboratory equipment. Some research laboratories have genetically engineered animals that need to be transported.

With a maximum of 100 boxes per laboratory, there will be a maximum 1200 boxes/bins for relocation. Additionally, there will be specialized laboratory equipment, freezers (-80 and -20 degrees), histology equipment, behavior equipment, high speed centrifuge, critical biological and other laboratory samples, chemicals, and consumables for relocation.

Please note that animals will be moved by this IOTA contract.

Specialized equipment will require temperature control. Weather proofing/water proofing is required, and equipment shall not be exposed to the environmental elements. Microscope and high-speed centrifuge equipment will require anti-vibration protection during transfer to the new location. A non-exhaustive list of equipment to be moved for reuse is included in Attachment R.

A truck with electrical outlet connections will be needed for the transport of refrigerators, freezers, and biological specimens to maintain freezers at -20 degrees or -80 degrees as appropriate to the specific freezers.

Transfer of live animals should be performed according to AAALAC guidelines and must acquire approval of IACUC prior to transfer. Here are guidelines:

1. The animal cages must be appropriately covered to avoid drawing attention to the animals and protect light sensitive animals from bright light. A laboratory coat, cloth, fabric drape, or similar is appropriate for covering the cages without inhibiting air flow. Plastic bags must never be used to cover cages/containers/animals during transport because they can restrict airflow and place the animals at risk. Additionally, a barrier must also be placed between the cages/pet carrier and the upholstery or floor of the vehicle. Cages or carriers should be secured from tipping by placing them on the floor or securing them to the seat with a seat belt or other means.

2. No eating, drinking, applying cosmetics, smoking, vaping, or use of any tobacco products is permitted in vehicles transporting animals in the same compartment as personnel.

3. During the transport of animals, unnecessary stops are not permitted (i.e., drive-through at a bank or restaurant). Animal transport must be direct from the housing area to the facility they are being transported to. Animals must never be left unattended in a vehicle.

are present.

Tasks include but are not limited to:

A. Physical movement of files.
B. Physical movement of accountable equipment (barcoded non-expendable supplies/equipment).
C. Physical movement of expendable supplies.
D. Physical movement of live animals.
E. Physical movement of FF&E identified to be reused in the Reuse Plan.
F. Physical movement of all reused equipment and furniture.
G. Packing and unpacking of files, supplies and equipment.
H. Labeling of all items to be moved to coordinate with floorplans.
I. Execute the Move Plan

#	Deliverable Name	Deliverable Description
16.6.1	Relocation Services	IOTA contractor shall provide for all labor, materials, and equipment for relocation services from old facility to new facility.
16.6.2	Staff Move Guide	The guides shall include general moving instructions, pre-move checklists, labels, move routes, schedule, etc.

16.7 Activation Services and Post Occupancy Support

The IOTA contractor shall provide comprehensive Activation Services to include transitioning, installation and move plan implementation activities to bring the Research & Development (R&D) facility into full operations prior to Day one. IOTA contractor shall provide post occupancy support post Day One to close out the activation project. Activation milestones shall be identified and tracked on the activation project schedule and the Activation Integrated Master Schedule. The plan shall describe the process to be used to deliver and install the new items for the activation project to ensure Government acceptance. The Plan shall include recommended installation processes, coordination, and scheduling of equipment delivered directly to the facility by vendors as well as installation processes for items delivered from the warehouse. The plan shall include a process to provide the required information to VA for VA to update its inventory system. The Plan shall also include the IOTA contractor's plan for wall and floor protection to minimize damage to the facility during installation as well as a plan for cleanup. The Plan shall also include a laydown plan and punch list if used. Finalized FF&E layouts by room are to be affixed to each room (on the door or other prominent location) to facilitate installation, inspection, and acceptance. Each layout shall identify the applicable location/room.

The IOTA contractor shall develop and provide a Delivery, Installation, Testing, and Acceptance Plan. This plan shall document how the IOTA contractor plans to accomplish the delivery, installation, testing, and acceptance of FF&E to ensure the successful activation of the facility as required by milestones in the Master Project Schedule. Key processes and procedures of the plan include:

A. Site Access Control
B. Product Delivery
C. Building Protection
D. Placement and Installation of Product
E. Transfer of Custody
F. Life Safety
G. Occupational Safety
H. Physical Security
I. Waste Management

The IOTA contractor shall provide delivery, staging, and installation. Delivery, staging, and installation shall be identified and tracked on the master project schedule. The IOTA contractor shall transport and place/install all ordinary JSNs in the designated room per the MPS. These JSNs include low technology, non-medical, common equipment, and furnishings such as waste receptacles, mats, furniture, dispensers, refrigerators, appliances, clocks, lamps, curtains, and other similar types of material.

IOTA contractor shall provide for all labor, materials and equipment for FF&E coming from the warehouse. The IOTA contractor shall provide all labor, materials, equipment, tools, transportation, and supervision to de-install, prepare for movement, transport, deliver, and install all designated government-owned assets to be reused in the new R&D facility. Installation of all items shall be in accordance with manufacturer instructions. The IOTA contractor shall install all FF&E except for those items designated by the Government to be installed by the manufacturer/vendor or general contractor. As items are placed and installed, records shall be updated by the IOTA contractor to provide an auditable trail of custody throughout the JSN delivery, installation, and acceptance process. The Interior Design Team should be involved in furniture installations, walk-throughs, and sign-offs of installations. Research Department representatives should be involved in biomedical laboratory furniture and equipment installations, walk-throughs, and sign-offs of these installations. IOTA contractor to oversee equipment, furniture and artwork vendors with placement and installation.

The IOTA contractor is responsible for removing all trash and debris generated during the installation process (e.g. removing debris off-site). IOTA Contractor to provide a dumpster. If the IOTA contractor plans to use on-site dumpsters, the contractor must submit a laydown plan for dumpsters delivered. The laydown plan should be included as part of the Delivery, Installation, Testing, and Acceptance Plan. The COR will be responsible for coordinating the laydown plan with the Construction & Facilities Management (CFM) Resident Engineer (RE).

Government acceptance of installation services will occur after installation of items is complete. For items that the Government does not accept due to installation issues by the contractor or when acceptance is contingent upon additional work by the contractor, the contractor shall provide a punch list and a punch list schedule to the COR.

IOTA contractor personnel shall transport and place research equipment in accordance with the MPS. At the room designated by Biomedical Equipment Maintenance Technicians (BMET), contractor shall unpack and install or assemble the equipment. Upon completion of work, the space shall be left as clean as possible with all packing materials/debris removed from the building. The installing technician will update, initial, and date the IOTA Contractor's record of installation before departing the area.

IOTA contractor to support VA research personnel with inspection (i.e. acceptance test) for compliance with manufacturer specifications and VA standards prior to initial use. The use of any such equipment is prohibited until it has passed inspection and has been accepted into the hospital's Medical Equipment Management Program (MEMP) inventory. The Government will identify items that require biomed checks/testing to be performed by the Government

During room outfitting, logistics will provide the IOTA Contractor with (VA) barcode labels to attached to each item and capture product data to satisfy internal and government inventory management requirements. Logistics shall provide the contractor with the barcoding inventory, so the contractor can verify all acquisition on the SharePoint acquisition page project page as received. Site logistics team will be responsible for inputting into the VA property management system.

IOTA contractor shall also provide welcome/orientation kits to ensure new employees are familiar with the new space and location. Kits should include such items such as facility maps, help desk numbers, how to use the phone system, important phone #s, furniture ergonomics & usage, etc.

The IOTA contractor shall provide all management, materials, tools, supervision, labor, and equipment to facilitate the final turnover of the facility, applicable documents, and closeout of the activation project. The IOTA contractor shall provide for the facilitation of full POE services for the project or for participation in POE activities as needed.

IOTA contractor shall identify and support management of any post-move issues; log vendor claims and direct issues/claims needing resolution by the CO; facilitate project files/history transfer between the project SharePoint site and the COR.

The IOTA Contractor is not responsible for sterilizing the VA Research and Development equipment and/or animal cages. The IOTA Contractor will work closely with the separate sterilization contractor during the activation.

#	Deliverable Name	Deliverable Description
16.7.1	Activation, Installation, Transitioning and Relocation Plan and Implementation	The plan shall describe the process to be used to deliver and install the new items for the activation project to ensure Government acceptance. The Plan shall include recommended installation processes, coordination, and scheduling of equipment delivered directly to the facility by vendors as well as installation processes for items delivered from the warehouse. The plan shall include a process to provide the required information to VA for VA to update its inventory system. The Plan shall also include the IOTA contractor's plan for wall and floor protection to minimize damage to the facility during installation as well as a plan for cleanup. The Plan shall also include a laydown plan and punch list if used. Finalized FF&E layouts by room are to be affixed to each room (on the door or other prominent location) to facilitate installation, inspection, and acceptance. Each layout shall identify the applicable location/room.
16.7.2	Post Occupancy and Project Close out Report	Report shall include all post-move issues noted and resolved, along with vendor claims and issues.
16.7.3	Employee Orientation Services	Develop welcome/orientation kits for new employees, (i.e. facility maps, policies, service access, contact information, phone usage, printer usage, furniture & ergonomics guide, etc.)
16.7.4	Warranty Management and Maintenance Support Plan (MSP)	The IOTA contractor will develop and provide to the Government, a warranty Management and Maintenance Support Plan (MSP) for all critical and non-critical installed medical equipment to also include FF&E. The MSP will include maintenance schedules, warranties, and life-cycle analysis. The MSP will clearly describe installed building equipment by name, type, manufacture, date installed, location and photo of the item. The MSP will identify maintenance schedules, inspection requirements and the method of service performance.

16.8 Staff Training and Orientation

Assist in coordination of training for R&D facility staff on operation of installed equipment to include, but not limited to Research equipment and maintenance equipment. The IOTA contractor is to provide all management, materials, supervision, and labor to support the training of research personnel for the necessary training on any new equipment and all the safety aspects of the new space.

Tasks include but not limited to:

A. Initial hands-on, face-to-face training for the following types of staff:
   a. R&D facility

B. Provide training reports in an Excel or compatible database to track all training completed

#	Deliverable Name	Deliverable Description

16.8.1	Training and Simulation Plan	The IOTA contractor shall develop, maintain, and provide to the Government a Training and Simulation Plan in an excel database or compatible for all critical and non-critical installed equipment. The plan shall identify which equipment requires training and which staff will be trained. The IOTA contractor will coordinate with COR and the VHA SimLEARN simulation team to develop the simulation plan.
16.8.2	Training Reports	The IOTA contractor shall provide Training Reports to show what equipment and/or simulation plan for which training was completed listed by the employees' name and service.

17.0 OPTIONAL TASKS

Optional tasks are pre-priced and will be exercised via modification to the existing contract at time of need. The Period of Performance for the optional tasks will be from date of exercise and shall not extend past the overall Contract's period of performance.

17.1 Warehousing and Warehousing Management Services

The IOTA contractor shall provide comprehensive warehousing services to include the provision of warehouse space for the FF&E that will be staged prior to installation and as needed during the activation process. All items must be stored in such a way as not to void manufacturer warranties. It is the IOTA contractor's responsibility to determine warehouse size requirements based on the most current FF&E list (Attachment Q).

Please note that specialized equipment will require temperature control. Weather proofing/water proofing is required, and equipment shall not be exposed to the environmental elements. Microscope and high speed centrifuge equipment will require anti-vibration protection during transfer to the new location.

Warehousing services include tracking, receiving, documenting, reporting, and storing all identified FF&E. Please note that Government acceptance of items delivered to the warehouse must be done by Government personnel. The IOTA contractor must have the ability to report all assets stored in the facility with daily updates provided as items are delivered to the facility. IOTA contractor will provide temporary warehousing, including all necessary receiving, inventorying, storing and all transportation and logistical services as required to facilitate all IOTA services under this contract.

Warehouse requirements:

- **A.** The warehouse must be centralized (or located within 15 miles) between old facility and new (or as otherwise agreed to by the Government POC)
- **B.** Identify items that will need to be warehoused and/or determine warehousing requirements
- **C.** The warehouse must have a sprinkler system, security system, racking, and loading docks.
- **D.** The IOTA contractor shall provide appropriate insurance to protect the VA in case of loss or damage to VA property stored at the warehouse
- **E.** The IOTA contractor shall provide delivery of items from warehouse to final location on site
- **F.** The IOTA contractor shall develop and provide a Warehousing Plan (workflow process).
- **G.** Provide necessary Material Handling equipment to include Forklift, pallet-jacks, etc.

#	Deliverable Name	Deliverable Description
17.1.1	Warehouse Plans	The Warehousing Plan shall describe how the IOTA contractor plans to meet the warehousing requirements of the PWS and an Emergency Management Plan for the warehouse. The Warehousing Plan shall include at a minimum: **A.** Address of the warehouse

		B. Hours of operation **C.** Pictures of the interior of the warehouse prior to FF&E being received **D.** Details of how IOTA contractor will meet the minimum warehouse requirements (i.e. sprinkler system, fire protection, racking, loading docks, climate control area (if required), security system), **E.** Warehouse security plan **F.** Copy of the certificate of insurance. **G.** Description of methodology used to control inventory, and all FF&E accepted at the warehouse.
17.1.2	Receiving Logs	The IOTA contractor shall receive and manage inventory of FF&E items directly at the warehouse. The contractor shall fill in all pertinent data on the documents as it pertains to property accountability and deliver all completed documents to the Logistics POC daily. The Receiving Logs shall be submitted on a weekly basis which identifies daily receipt of items.
17.1.3	FF&E Inventory Logs	The IOTA contractor shall report on all items scheduled for delivery to be warehoused, received at the warehouse, condition/defects, date scheduled for installation, installation date, and BMET check/test date. The Inventory Logs shall be submitted on a weekly basis which identifies daily inventory of items.
17.1.4	Warehousing Activities Report	IOTA contractor shall report on all warehousing activities to include operations, FF&E activities, delivery, installation, and relocation activities.

18.0 Deliverables

Deliverables have established delivery schedules as specified in the PWS. Failure to comply with the delivery schedule will cause the contractor to be delinquent in performance. Such tardiness will be annotated in the Contractor Performance Assessment Rating System (CPARS) interim and/or final ratings.

18.1 Deliverable Schedule

Submittals are required deliverables mutually agreed upon within the contract. Submittals have established delivery schedules as specified in the PWS. Failure to comply with these delivery schedules makes the contractor delinquent in performance. Such tardiness will be annotated in the contractor Performance Assessment Rating System (CPARS) interim and/or final ratings.

Delivery schedule for deliverables is identified below. Due to the variations in project schedules, construction timelines, etc., deliverable due dates may be adjusted with prior notification and approval by the VA CO. For deliverables with a schedule yet to be determined, a mutually agreed upon schedule and/or format will be determined during the performance period. The agreed upon date must not delay the project schedule and must be tracked in the Activation Project Schedule for verification.

The IOTA contractor shall provide deliverables per the task/delivery schedule. Deliverables may be a “moving target date” depending on construction schedule. Deliverables with a “moving target date” dependent on construction schedule will be identified as "Building Occupancy Date (date building is turned over for outfitting etc.) minus X number of days".

Deliverable No.	Deliverable Name	Due
16.1.1	Monthly Project Status Report	Monthly by date agreed upon by COR, additional updates as required

16.1.2	Activation Integrated Master Schedule (AIMS)	1 month following the effective date of the contract and updated within 30 days of any validated changes
16.1.3	Individual Service Project Schedules	1 month following the effective date of the contract and updated within 30 days of any validated changes
16.1.4	Risk Management Plan and Log	1 month following the effective date of the contract and updated within 5 days of risk identification
16.1.5	Change Management Plan and Log	1 month following the effective date of the contract and updated within 5 days of facility activation coordinator requested change
16.1.6	WBS	1 month following the effective date of the contract and updated within 30 days of any validated changes
16.1.7	Integrated Project Team (IPT)	1 month following the effective date of the contract and updated within 30 days of any validated changes
16.1.8	SharePoint Site	Update and maintain governmental SharePoint site at a minimum weekly or as changes occur. This includes adding new data packages as it occurs in the field.
16.1.9	Meeting minutes and Meeting agenda	Agendas shall be distributed no less than [**3 days]** prior to the meeting. Minutes shall be distributed no more than [**5 days**] post meeting
16.1.10	PWS Deliverable updates	Updates must be completed no later than 5 workdays after identification of need by either the Government or the Contractor.
16.2.1	FF&E Cut Sheets	3 months following the effective date of the contract; updated as needed; finalized by final design submission
16.2.2	Master Key Plan	6 months prior to building turnover
16.2.3	Room by Room Master Equipment and Furniture list (MEL)	Initial MEL draft due 1 month after DD2, final MEL due 1 month after Acquisition plan is finalized
16.2.4	FF&E Layouts	2 weeks (timeline should be adjusted based on CFM schedule) after each DD2 submission, FFE layout is due to include a conflict report. 2 weeks (timeline should be adjusted based on CFM schedule) after each CD1 submission, a final revised FF&E layout is due to include a conflict report.
16.2.5	3-Dimensional Design Renditions (if applicable)	2 weeks (timeline should be adjusted based on CFM schedule) after each DD2 submission, 3-Dimensional Design renditions are due to include a conflict report. 2 weeks (timeline should be adjusted based on CFM schedule) after each CD1 submission, a final revised 3-Dimensional Design renditions are due to include a conflict report.
16.2.6	Rough Order of Magnitude (ROM)	Initial ROM draft due 1 month after Acquisition plan is finalized and updated as the time of market research.
16.2.7	Mock-up Services and Mock-up Report	Mock-up results Report to be submitted as part of the response of DD2 review period.
16.2.8	Design Submittal 1	Design Submittal 1 package is after User group meeting (UMG) 1 is completed (timeline shall be adjusted based on CFM schedule)

16.2.9	Design Submittal 2	Design Submittal 2 package is after User group meeting (UMG) 2 is completed (timeline shall be adjusted based on CFM schedule)
16.2.10	Equipment Reuse and Disposal Plan	Initial Equipment Reuse and disposal draft plan is due at Design submittal 1. Final Equipment reuse and disposal plan is developed prior to Procurement Package development.
16.3.1	Micro CONOPS	Initial draft 6 months before BOD, final 30 days after draft approval
16.3.2	Transition CONOPS	Initial draft 6 months before BOD, final 30 days after draft approval
16.3.3	General CONOPS	6 months before BOD; updated as required
16.3.4	Transition Plan	6 months before BOD; updated as required
16.3.5	Integrated Move Plan	6 months before BOD; updated as required
16.3.6	Project Staffing Plan: Proposed FTE Report	3 months after effective date of contract; updated as required
16.4.1	Room Contents and Acquisition Plan	Room Contents and Acquisition Plan is due 2 weeks after final AE design; updated to all fields as required.
16.5.1	Procurement Packages	Procurement Packages due according to the approved Acquisition plan, and prior to facility procurement package review and approval. As procurement activities are completed, the Procurement related acquisition plan fields will be updated. For Long Lead Times: Procurement Packages are due after final AE design according to the timelines specified in the construction contract schedule; updated as required.
16.6.1	Relocation Services	Contractor shall provide for all labor, materials, and equipment for relocation services from old facility to new facility.
16.6.2	Staff Move Guide	The guides shall include general moving instructions, pre-move checklists, labels, move routes, schedule, etc.
16.7.1	Activation, Installation, Transitioning and Relocation Plan and Implementation	Weekly, during the activation phase as defined in the approved Activations Integrated Master Schedule (IMS).
16.7.2	Post Occupancy and Project Close out Report	1 month post occupancy
16.7.3	Employee Orientation Services	Start of Building Occupancy Date (BOD), completed one week prior to Day One
16.7.4	Warranty Management and Maintenance Support Plan (MSP)	Start of BOD, completed one week prior to Day One
16.8.1	Training and Simulation Plan	14 calendar prior to first training event

16.8.2	Training Reports	1 month prior to Day One
Task #	**Optional Tasks**	**Optional Task Deliverables**
17.1.1	Warehouse Plans	1 month after award of optional task
17.2.2	Receiving Logs	Upon, after receipt of items into the warehouse
17.2.3	FF&E Inventory Logs	Daily, after receipt of items into the warehouse
17.2.4	Warehousing Activities Report	Weekly, after receipt of items into the warehouse

18.2 Deliverable Formatting

Reports and documents delivered by the IOTA Contractor in performance of this contract will be considered "technical data" as defined in the applicable "Rights in Data" clause of the contract. All documentation shall reflect the latest version number, unless specifically directed otherwise by the Government. All documentation shall be prepared in accordance with standard industry practices, ensuring electronically produced documents, which reflect logical flow of material, tables of contents, indices, and page numbering. The unexcused failure to comply with the delivery schedule makes the contractor delinquent in performance. Such tardiness will be annotated in the IOTA Contractor's past performance evaluation.

The IOTA contractor shall deliver documentation in electronic format unless otherwise directed in the solicitation/contract. Contractor may be required to submit deliverables using software, such as MS Word 2010/2016, MS Excel 2010/2016, MS PowerPoint 2010/2016, MS Project 2010/2016, MS Access 2010/2016, MS Visio 2010/2016, AutoCAD 2010/2016, Adobe Postscript Data Format (PDF), Adobe Acrobat Pro, Revit 2010/2016, SPEXX, Submittal Exchange or similar, and Bluebeam, unless otherwise directed in the PWS, solicitation, or contract. All deliverables must be submitted in an editable format, such as Word. Example, PDFs are acceptable for final deliverables, as long as the Government is provided an editable version.

The IOTA contractor is responsible for determining additional software needs, acquiring the software licenses, installing, and maintaining necessary software (to include PlanGrid) throughout the project is at the cost of the contractor.

18.3 Files

The IOTA contractor shall maintain complete and accurate files of documentation, records, copies of original results and reports, verified original data, corrected data, and corrected supporting final report required under the terms of the contract. The IOTA contractor shall not allow access to the files by any Government agency, non-Government agency, or individual unless specifically authorized by the CO or designated representative. Files shall be made available to the CO, COR, or designated representative upon request. All files will become the property of the Government and shall be turned over to the CO, COR, or designated representative at the completion or termination of this contract. All briefings, reports, and other files produced by the IOTA contractor for the Government under the terms of this contract shall be property of the Government.

18.4 Government Submission Review

Unless specifically stated in the deliverable schedule, the Government has 10 business days to review and provide comments on submitted deliverables, unless deliverable reviews and changes are dependent upon third parties (i.e., construction Contractor, A/E firm, RE, etc.), in which case a reasonable review period will be discussed with the Contractor. The IOTA Contractor has five (5) business days to complete any necessary revisions and resubmit for Government review and acceptance. Any deliverable submitted to the Government that is not reviewed and returned within 10 business days shall be considered “accepted” by the Government, except in the case described above regarding third party dependencies. The Government will make every effort to accomplish review in as little time as practicable.

19.0 National Archives Records Administration (NARA) Management

A. *Applicability*

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. *Definitions*

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. Includes VHA records.
2. Does not include personal materials.
3. Applies to records created, received, or maintained by Contractors pursuant to their VHA contract.
4. May include deliverables and documentation associated with deliverables.

C. *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. Ch. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

4. Research & Development Facility Lease and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of Research & Development Facility Lease or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, the Contractor must report to VHA. The agency**/** Research & Development Facility Lease must report to promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the Contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it

shall be returned to Research & Development Facility Lease control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the Firm Fixed Price. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government Research & Development Facility guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with Research & Development Facility policy.

8. The Contractor shall not create or maintain any records containing any non-public Research & Development Facility information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. The Research & Development Facility owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which Research & Development Facility shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

11. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take VHA-provided records management training, Talent Management System (TMS) Item #3873736, Records Management for Records Officers and Liaisons. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

[Note: To the extent an agency requires contractors to complete records management training, the agency must provide the training to the contractor.]

D. Flow down of requirements to Subcontractors

1. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this [FFM], and require written subcontractor acknowledgment of same.

2. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

20.0 Records Management

- Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.
- Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.
- Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.
- Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.
- The Government Agency owns the rights to all data/records produced as part of this contract.
- A master Record Plan will be maintained and updated on a weekly basis per VA standard.

- The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.
- Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].
- No disposition of documents will be allowed without the prior written consent of the CO. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.
- Contractor is required to obtain the CO's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

21.0 Contract Authority

Only a warranted CO, acting within their delegated limits, has the authority to issue modifications or otherwise change the terms and conditions of this contract. If an individual other than the CO attempts to make changes to the terms and conditions of this contract you shall not proceed with the change and shall immediately notify the CO. Coordination of routine technical matters with project members shall be accomplished through the CO’s Representative (COR).

22.0 Contracting Officer’s Representative

A Contracting Officer’s Representative (COR) will be designated for this contract. The COR is authorized to act as an official representative of the CO. CORs are authorized to act within the limitations specified herein and according to their COR delegation letter (signed by the COR, CO and Contractor) and written restrictions specifically imposed under the terms of the contract and by the CO. If delegations and restrictions of the COR delegation letter differ from the delegations and restrictions of the PWS, the delegation and restrictions of the COR delegation letter shall take precedence. The COR will be the primary Government point of contact for the contractor regarding general "tasking" requirements, deliverables, and other requirements under the contract.

CORs do not have the authority to direct changes in scope, price, or terms and conditions of the contract. CORs do not have the authority to execute modifications to the contract which require the signature of the CO to bind the Government by contract in terms of a proposed change.

23.0 Business Relations

The contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The contractor shall manage the timeliness, completeness, and quality of problem identification. The contractor shall provide corrective action plans, proposal submittals, timely identification of issues, and effective management of subcontractors. The contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all contractor personnel.

24.0 Contract Management

The contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. The contractor must maintain continuity between the support operations at the facilities where IOT&A services are being performed and the contractor's corporate offices. The Contractor shall designate an Activation Project Manager and alternate whom shall serve as the Government's primary point of contact and be responsible for overall coordination and scheduling of the work.

25.0 Contract Administration

The contractor shall establish processes and assign appropriate resources to effectively administer the requirements. The contractor shall respond to government requests for contractual actions in a timely fashion. The contractor shall identify a single point of contact between the Government and contractor personnel assigned to the contract. The contractor shall assign work effort, maintaining proper and accurate time keeping records of personnel assigned to work on the requirements.

26.0 Personnel Administration

The contractor shall provide personnel management and support as required. The contractor shall maintain the currency of their employees by providing initial and refresher training as required to meet the PWS requirements. The contractor shall make necessary travel arrangements for employees. The contractor shall provide necessary infrastructure to support contract tasks. The contractor shall provide administrative support to employees in a timely fashion (time keeping, leave processing, pay, emergency needs).

27.0 Subcontract Management

The contractor shall be responsible for any subcontract management necessary to integrate work performed on this requirement and shall be responsible and accountable for subcontractor performance on this requirement. The Prime contractor will manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations.

28.0 Employee Identification

All contractor employees working at a government facility shall wear company identification and government issued identification to distinguish themselves as contractor personnel. When conversing with government personnel during business meetings and over the telephone, contractor employees shall identify themselves as such. Where practicable, contractor employees occupying space within a government facility should identify their workspace area with their name and company affiliation.

29.0 Invoicing

The Contractor shall submit invoices, including all back-up data, to the COR for review and approval prior to electronic invoice submission. Invoice back-up data at a minimum will include the Monthly Project Status Report. The Monthly Project Status Report submitted with the invoice shall cover the same billing period as the invoice. The Monthly Project Status Report shall provide sufficient documentation that the work being billed for has been completed. Upon receipt of an accurate and complete invoice, the COR will return an approved copy to the Contractor within five (5) business days. If the invoice is incomplete or inaccurate, the COR will return the unapproved invoice to the Contractor for correction within five (5) business days.

The Contractor shall submit approved invoices for payment following the electronic invoicing procedures below. The date on the invoice submitted electronically shall not be before the date of the COR's invoice approval.

30.0 Mandatory Electronic Invoice Submission

- VA Financial Services Center (FSC) Mandatory Electronic Invoice Submission - The Department of Veterans Affairs published a final rule in the Federal Register on November 27, 2012 to require contractors to submit payment requests in electronic form to enhance customer service, departmental productivity, and adoption of innovative information technology, including the appropriate use of commercial best practices. The rule is effective December 27, 2012.
- Vendor Electronic Submission Methods - Facsimile, email, and scanned documents are not acceptable forms of submission for payment requests. Electronic form means an automated system transmitting information electronically per the accepted electronic data transmission methods below:
    - VA's Electronic Invoice Presentment and Payment System - The FSC uses a third-party contractor, Tungsten, to transition vendors from paper to electronic invoice submission. Please go to this website: http://www.tungsten-network.com/US/en/veterans-affairs/ to begin submitting electronic invoices, free of charge.

- A system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) chartered by the American National Standards Institute (ANSI).

- Vendor e-Invoice Set-up Information - Please contact Tungsten at the phone number or email address listed below to begin submitting your electronic invoices to FSC for payment processing, free of charge. If you have questions about the e-invoicing program or Tungsten, please contact FSC at the phone number or email address listed below:
  Tungsten e-Invoice set-up information: 877-489-6135
  Tungsten e-Invoice email: VA.Registration@Tungsten-Network.com
  FSC e-Invoice Contact Information: 877-353-9791
  FSC e-Invoice email: vafsccshd@va.gov
  More information on the FSC electronic invoicing process can be found at http://www.fsc.va.gov/einvoice.asp.

31.0 Coordination with Other Contractors

For projects identified as a part of this contract, the Government may award other contracts for work not covered by this contract but necessary to overall project completion (such as construction). The Contractor will not meet with any other contractor(s) not associated with the identified project unless directed by the CO or COR administering this contract. The Contractor will not commit or permit any acts that will interfere with the performance of work by any other contractor or by any Government employee. The CO will resolve all work conflicts and provide written direction to the Contractor when required. Any additional work requirements (not within the scope of this contract that may be created as a result of work performance of other contractors will be brought to the attention of the CO. The CO, when required, will provide written direction to the Contractor.

32.0 Government Furnished Materials

All procedural guides, reference materials, and program documentation for the project and other government applications will 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.

32.1 Government Furnished Property, Equipment and Services

The Government may provide certain materials for exclusive use by the contractor as deemed appropriate for the contractor to perform the requirements of the contract. The Government makes no representation that the materials furnished by the Government are completely sufficient to accomplish the requirements of the contract. The contractor shall check the items furnished for adequacy and accuracy prior to utilization. The contractor is not authorized to distribute Government-supplied materials without the express approval of the CO.

32.2 Government Furnished Property (GFP)

If GFP is provided, it will be stated in the contract, and will be accounted for in accordance with the approved property management plan and any site-specific addendum to the property management plan. If property is acquired by the contractor during the performance of this work, the contractor acquired property (CAP) will also be accounted for in the same manner.

32.3 Government Furnished Property Close-Out

Upon completion or termination of the contract, the contractor shall promptly perform and report to the Property Administrator contract property closeout, to include reporting, investigating and securing closure of all loss, damage, destruction, or theft cases; physically inventorying all property upon termination or completion of this contract; and disposing of items at the time they are determined to be excess to contractual needs.

32.4 Use of Government Furnished Property

The contractor shall use Government property, either furnished or acquired under this contract, only for performing this contract, unless otherwise provided for in this contract or approved by the CO.

32.5 Administration of Government Furnished Property

FAR Part 45 and FAR 52.245-1 set forth the basic requirements to be observed by contractors in establishing and maintaining control over Government property provided pursuant to the terms of this contract.

32.6 Property Control Plan

The contractor shall establish a contractor's Property Management Plan in accordance with voluntary consensus standards and/or industry-leading practices and standards for Government property management except where inconsistent with law or regulation, FAR Part 45 and FAR 52.245-1 to control, use, protect, preserve, repair and maintain all Government property specified in this contract. During the period of performance, the contractor shall disclose any significant changes to their property management system to the Property Administrator prior to implementation. The plan shall be in writing and maintained (retained) by the contractor and made available to the Property Administrator and Contract Administrator for review not later than the contract start date.

32.7 Inventory of Government Furnished Property

The contractor shall periodically perform, record, and disclose physical inventory results for all GFP provided to them for use. Inventories shall be performed as stated in their PMP. The contractor shall account for durable, expendable and non-expendable GFP. The contractor when requesting approval to purchase replacement property, shall furnish a copy of the signed receipted turn-in document at time of request and provide the Property Administrator with a copy of the documentation and purchase request prior to purchasing replacement items. All other changes to property shall be routed through the COR to the Property Administrator and Contract Administrator for approval.

32.8 Reporting of Government Property

The contractor shall submit an annual report for all Government property on hand on September 30th of each year. The report shall be submitted to the Property Administrator no later than October 15th following the close of the period of which the report is made. The Government will provide unit acquisition costs for any GFP transferred to the contractor where relevant information is not available.

32.9 Loss, Damage, Destruction or Theft of Government Property

Loss, damage, destruction, or theft of GFP will be immediately reported to VA Police. Unless otherwise directed by the Property Administrator, the contractor shall investigate and promptly furnish a written narrative of all incidents of loss, damage, destruction, or theft to the property administrator as soon as the facts become known or when requested by the Government.

32.10 Other Government Furnished Information

VA will provide access to the facility's equipment inventory system (Maximo or Vista) if necessary in performance of this contract. VA will provide access to VA specific systems/networks as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPM, or VA Remote Access Security Compliance Update Environment (RESCUE). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, proPath, Primavera, and Remedy, including appropriate seat management and user licenses. Please note, contractor employees using VA specific systems/networks will require a PIV.

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 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.

33.0 Quality Assurance

This section describes the Quality Control components for this effort. The following sub-sections provide details of various considerations on this effort.

33.1 Quality Surveillance

Contractor performance is subject to surveillance by the COR to ensure compliance with this contract to include all elements of the Performance Metrics. The contract identifies two types of non-conformances: major and minor. All records of non-conformance and corrective actions will be documented in Corrective Action Reports (CAR), Quarterly Surveillance Reports, and CPARS.

33.2 Quality Assurance Surveillance Plan

The Government will monitor the contractor's performance under this PWS in accordance with the Governments Quality Assurance Surveillance Plan (QASP) (Attachment M). The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptance performance levels.

33.3 Non-Conformances

The Contractor shall identify and control non-conformances through root cause analysis, corrective actions and preventive actions. The Contractor shall focus on proactive identification and transparency of issues, and on eliminating the cause to prevent reoccurrences. The Contractor shall maintain records of non-conformities and actions taken.

The Contractor shall correct and provide response to all Government-identified non-conformances in accordance with timeframes specified by the CO.

33.4 Minor Non-Conformance

A minor non-conformance is a non-conformance, which by itself does not adversely impact the overall project mission, safety of personnel and/or equipment, performance (quality), or schedule (delivery). Minor non-conformances are typically low risk and may be communicated through a CAR form with the minor box checked.

Minor CARs are normally issued for any identified non-conformances. Second notice minor CARs are normally issued for repeat non-conformances or failing to correct issues within a reasonable amount of time or non-conformances that increases risk to one specific technical element or program. Upon receipt of a minor CAR addressing minor non-conformance, the Contractor shall complete applicable sections and return it to the CO within the time specified in the notice. A formal corrective action plan is not required for minor CARs. Minor non-conformances shall be documented in order to be used in support of a Quarterly Surveillance Report or CPAR rating.

33.5 Major Non-Conformance

A major non-conformance is a non-conformance that adversely impacts (or has the potential to impact) mission, safety of personnel and/or equipment, performance (quality), or schedule (delivery). This type of non-conformance increases risk to the Government and therefore has a risk assessment rating of moderate or high. For example, a CO may find that a situation of increasing risk exists where there are a significant number of recurring minor non-conformances creating an indication of inadequate preventive measures/actions which lowers the Government's confidence that the Contractor can provide quality services on time.

The CO will communicate major non-conformances on a CAR form with the major box checked. A suspense date for the Contractor's corrective action plan will be included as well as a summary of the minor CARs and documented customer complaints, if any, that have preceded this issuance. Major Non-conformances shall be documented in order to be used in support of a quarterly surveillance or CPAR rating. The Contractor shall generate a formal corrective action plan for major CARs and other documented Government complaints/concerns that will address at a minimum:

- Action taken to fix the immediate problem
- Root cause analysis of the problem to determine cause
- Corrective action on the cause of the problem
- Actions taken to prevent recurrence

Furthermore, any unresolved, validated major non-conformance issue(s) will result in less than satisfactory performance on the Contractor's quarterly ratings, CPAR and past performance ratings.

33.6 Contractor Performance Assessment Writing System

FAR 42.1102 directs all Federal agencies to collect past performance information on contracts. The VA has implemented CPARS to comply with this regulation. One or more past performance evaluations will be conducted to record the Contractor's contract performance as required by FAR 42.11.

The past performance evaluation is a paperless process using CPARS. CPARS is a web-based system that allows for electronic processing of the performance evaluation report and for Government use in evaluating past performance as part of a source selection action.

The Government requests the Contractor furnish the CO with the name, position title, phone number, and email address for each person designated to have access to the Contractor's past performance evaluation(s) for the contract. Each person granted access will have the ability to provide comments in the Contractor's portion of the report and state if the Contractor agrees with the evaluation, before returning the report to the Assessing Official. The report information must be protected as "source selection sensitive information not releasable to the public."

When the Contractor's Representative(s) (Past Performance Points of Contact) are registered in CPARS, they will receive an automatically-generated email with detailed login instructions. Further details, systems requirements, and training information for CPARS are available at https://www.cpars.gov. The CPARS User Manual, registration for On-Line Training for Contractor Representatives, and a practice application may be found at this site.

The Assessing Official will complete an interim or final past performance evaluation and the report will be accessible at http://www.cpars.gov. The Contractor Representative has the option to provide comments on the evaluation, indicate if they concur or do not concur with the evaluation, sign, and then return the evaluation to the Assessing Official. The Contractor Representative has 60 days following the Assessing Official's evaluation signature date to send comments. On day 15 following the Assessing Official's evaluation signature date, the evaluation will become available in CPARS with or without Contractor Representative comments and if it has been closed by the Assessing Official or Reviewing Official. If no Contractor Representative comments have been sent and the evaluation has not been closed, it will be marked as "Pending" in CPARS. On day 61 following the Assessing Official's evaluation signature date, the Contractor Representative will be "locked out" of the evaluation and may no longer send comments.

The following guidelines apply concerning Contractor Representative use of the past performance evaluation:

- Protect the evaluation as "source selection information." After review, transmit the evaluation by completing and submitting the form through CPARS. If for some reason, you are unable to view and/or submit the form through CPARS, contact the CO for instructions.

- Strictly control access to the evaluation within your organization. Ensure the evaluation is never released to persons or entities outside of your control.
- Prohibit the use of or reference to evaluation data for advertising, promotional material, pre-award surveys, responsibility determinations, production readiness reviews, or other similar purposes.

33.7 Government Remedies

The CO shall follow FAR 52.212-4, "Contract Terms and Conditions- Commercial Items" for contractor's failure to perform satisfactory services or failure to correct nonconforming services.

33.8 Quality Control Plan

The Contractor shall develop, implement, and maintain a comprehensive inspection system that assures compliance with all requirements of this contract in accordance with FAR Part 46, Quality Assurance.

The Contractor shall develop a Quality Control Plan (QCP). The QCP shall document how the Contractor will maintain an effective quality control program to ensure services are performed in accordance with the contract and this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractors QCP is how he assures himself that his work complies with the requirement of the contract.

The QCP is due within thirty (30) days after contract award. The Contracting Officer may notify the Contractor of required modifications to the plan during the PoP. The Contractor then shall coordinate suggested modifications and obtain acceptance of the plan by the Contracting Officer. Any modifications to the program during the PoP shall be provided to the Contracting Officer for review no later than 10 working days prior to effective date of the change. The QCP shall be subject to the Governments review and approval. The Government may find the QCP "unacceptable" whenever the Contractors procedures do not accomplish quality control objective(s). The Contractor shall revise the QCP within 10 working days from receipt of notice that QCP is found "unacceptable." The QCP shall demonstrate the Contractor's documented processes and procedures to monitor and control, to include but not limited to:

- Objectives in the Services Delivery Summary
- Contract and subcontractor invoicing
- Non-conformances
- Contractor employee qualifications and certifications

#	Deliverable Name	Deliverable Description
041	Quality Control Plan	The QCP shall document how the Contractor will maintain an effective quality control program to ensure services are performed in accordance with the PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractors QCP is how he assures himself that his work complies with the requirement of the contract. The QCP is not separately priced.

34.0 Performance Metrics

The table below is a summary of the Performance Metrics and Performance Standards/AQLs for the tasks associated with this contract. These metrics will be used in conjunction with the QASP (Attachment M) to conduct contract performance surveillance.

Performance Metric	PWS Para.	Performance Standard/AQL

1: Qualified Workforce	12.0	Not more than one (1) COR validated complaint per quarter
2: Quality Performance	33.0	Not more than one (1) COR validated complaint per quarter; all tasks completed comprehensively
3: Deliverables	18.0	All deliverables pass Government inspection on first submission 95% of time, per month when applicable. Includes being on time and containing complete information. Re-performance within required time-period after Government notice.
4: Quality Control	33.8	Contractor complies 95% with the Government- approved Quality Control Plan

35.0 Special Requirements

This section describes the special requirements for this effort. The following sub-sections provide details of various considerations on this effort.

35.1 Security and Safety

This section describes the security and safety for this effort. The following sub-sections provide details of various considerations on this effort

35.2 Position/Task Risk Designation Level(s)

The following position sensitivity classifications and background investigation requirements are in accordance with the Department of Veterans Affairs 0710 Handbook "Personnel Security Suitability Program" 6500 Appendix A:

Position Sensitivity Low Tier 1: National Agency Check with Written Inquiries (NACI)
A NACI is conducted by OPM and covers a five-year period. It consists of a review of records contained n the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA, it is used for Non-sensitive or Low-Risk positions.

Position Sensitivity Moderate Tier 2: Moderate Background Investigation (MBI)
An MBI is conducted by OPM and covers a five-year period. It consists of National Agency Check (NAC) records [OPM SII, DCII, FBI name check, and an FBI fingerprint check], a credit report covering a period of five 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.

Position Sensitivity Moderate/Secret Tier 3: Background Investigation (ANACI)
An Access National Agency Check with Inquiries (ANACI) – not applicable to VHA contractors in most cases.

Position Sensitivity High Tier 4: Background Investigation (BI)
A BI is conducted by OPM and covers a 10-year period. It consists of a review of NAC records [OPM SII, DCII, FBI name check, and an 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, and co-workers; court records, law enforcement check, and a verification of the educational degree.

Position Sensitivity High/Top Secret Tier 5: Background Investigation (SSBI)
Single Scope Background Investigations (SSBI) – Not applicable to VHA contractors in most cases.

The Government is required to identify the appropriate background investigation level (NACI, MBI, or BI) by PWS task using the Position Designation Automated Tool (PDT) at the US Office of Personnel Management Website at: https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/. The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are listed in PDAT Matrix (Attachment N).

The tasks identified in (Attachment N), and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for contractor individual, based upon the tasks the contractor individual will be working.

The submitted contractor Staff Roster (Attachment C) must indicate the required Background Investigation Level for each contractor individual based upon the task the contractor individual will be working, in accordance with their submitted quote.

35.3 Contractor Personnel Security Requirement Responsibilities

1) 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.

2) The contractor shall bear the expense of obtaining background investigations.

3) Within 3 business days after award, the contractor shall provide a completed Form 1A (Attachment O) for each employee and a roster of contractor and Subcontractor employees to the COR to begin their background investigations. The staff roster shall contain each contractor and Subcontractor employee's full name and individual background investigation level requirement.

4) The contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.

5) For a Low Risk designation, the following forms are required to be completed: OF-306 and DVA Memorandum - Electronic Fingerprints. For Moderate or High Risk designations, the following forms are required to be completed: VA Form 0710 and DVA Memorandum - Electronic Fingerprints. These should be submitted to the COR within 5 business days after contract award.

6) The contractor employee will receive an email notification from the Security and Investigation Center (SIC) through the Electronics Questionnaire for Investigations Processing (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF86). The contractor employee shall submit all required information related to their background investigations utilizing e-QIP.

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

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

9) A contractor employee may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) fingerprint results, completion of training delineated in VA Handbook 6500.6 (Appendix C, Section 4), and the signed "contractor Rules of Behavior." However, the contractor will be

responsible for the actions of the contractor personnel they provide to perform work for the VA. The investigative history for contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management.

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

11) Failure to comply with the contractor personnel security investigative requirements may result in termination of the contract for default.

36.0 ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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. 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 assessment and authorization (A&A).

VA Handbook 6500.3 defines the procedures for Assessment, Authorization and Continuous Monitoring of VA Information Systems. A&A is the process used to ensure information systems have effective security safeguards which have been implemented, planned for, and documented in a security plan. The A&A process is the mechanism by which management provides formal authority for a system to operate and process information. A&A is based on the approval of the AO who is the senior most VA official assigned responsibility for IT systems. A&A is required by information security legislation and Federal regulation and provides a framework for auditing the efficiency and effectiveness of security controls. Since this acquisition will not require services that involve connection of one or more contractor-owned IT devices (such as a laptop computer or remote connection from a contractor system) to a VA internal trusted (i.e. non-public) network, A&A requirements do not apply, and a Security Accreditation Package will not be required. Additionally, VA Sensitive information will remain protected as it will reside behind the VA firewall at all times.

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 COR, CO, the Activation 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 VA Handbook 6500.6, "Contract Security," April 22, 2024 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order, as applicable. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall create TMS accounts and complete all mandatory training courses identified on the current external VA training site, VALU VA Learning University. The VALU VA Learning University may be accessed at (https://www.tms.va.gov/learning/user/SelfRegistrationUserSelection.do). If local Program Office desires, the Contractor shall use the VALU VA Learning Website to complete their mandatory training, accessed at https://www.tms.va.gov/learning/user/SelfRegistrationUserSelection.

Once Contractor TMS accounts are created and mandatory training completed, Contractor TMS accounts may be move to VA domains where VA computer access for contractors are created to monitor training.

Contractor employees shall complete a VA Systems Access Agreement and submit an appropriate background investigation before permitted access privileges to VA computer systems.

A2.0 VA Enterprise Architecture Compliance

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 create, 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 created and are published with an effective date of December 21, 2000. Federal departments and agencies shall create 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 created 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:

_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 specified 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 specified smoking areas.
(4) Possession of weapons is prohibited.
(5) The Contractor shall obtain all necessary licenses and/or permits required to perform the work, except for software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

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 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 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 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 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 VA.

7. Contractor must adhere to the following:
    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.

37.0 ADDENDUM B

VA INFORMATION AND INFORMATION SYSTEMS SECURITY/PRIVACY LANGUAGE VA HANDBOOK 6500.6, APPENDIX C, APRIL 22, 2024

1. GENERAL. This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

2. VA INFORMATION CUSTODIAL LANGUAGE. This entire section applies to all acquisitions requiring any Information Security and Privacy language.

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter “contract”) unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 R*ights in Data – General.* The primary governing federal acquisition regulation used to define computer software license (not data/intellectual property first produced under this contractor or order) is FAR 27.405-3, *Commercial Computer Software.*

b. Information made available to the contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 *Rights in Data – General*.

c. VA information will not be co-mingled with any other data on the contractor’s information systems or media storage systems. The contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to contractor and subcontractor staff associated with the

contract) to VA, VA's Office Inspector General (OIG, and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contactor.

h. The contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

i. The contractor’s firewall and web services security controls, as applicable, shall meet or exceed VA’s minimum requirements.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.

k. Notwithstanding the provision above, the contractor 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 cert medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the contractor is in receipt of a court order or other requests for the above-mentioned information, the contractor shall immediately refer such court order or other requests to the VA CO for response.

l. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.

m. Any data destruction done on behalf of VA by a contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

n. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, *Guidelines for Media Sanitization* prior to termination or completion of this contract. If directed by the COR/CO, the contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The contractor shall hold the

appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO

3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS. This section applies when any person requires access to information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract.

a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of contractor/subcontractor and agent of contractor/subcontractor.

b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.

c. All contractors and subcontractors working with VA information are subject to the same security investigative and clearance 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 shall be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

d. All contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All contractors and subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the contractor must state where all non-U.S. services are provided. The contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.

e. The contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:

(1) Contractor/subcontractor personnel no longer has a need for access to VA information or VA information systems.
(2) Contractor/subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

(3) Contractor believes their own personnel or subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

(4) Any previously undisclosed changes to contractor/subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.

(5) Contractor/subcontractor personnel have their authorization to work in the United States revoked.

(6) Agreement by which contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for contractor personnel.

f. In such cases of contract fulfillment, termination, or other causes; the contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by contractor/subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.

g. Contractors/subcontractors who no longer require VA accesses will return VA-issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems, networks and VA property in their possessions removed, contractors shall notify the appropriate VA COR/CO.

4. TRAINING. This entire section applies to all acquisitions which include section 3.

a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:

(1)VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter

(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].

b. The contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training 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 required training is complete.

5. SECURITY INCIDENT INVESTIGATION. This entire section applies to all acquisitions requiring any Information Security and Privacy language.

a. The contractor, subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the contractor, subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.

b. To the extent known by the contractor/subcontractor, the contractor/ subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following: (1) The date and time (or approximation of) the Security Incident occurred.

(2) The names of individuals involved (when applicable).

(3) The physical and logical (if applicable) location of the incident.

(4) Why the Security Incident took place (i.e., catalyst for the failure).

(5) The amount of data belonging to VA believed to have been compromised.

(6) The remediation measures the contractor is taking to ensure no future incidents of a similar nature.

c. After the contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The contractor, subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

d. VA IT contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.

e. 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 the VA Office of 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.

f. The contractor shall comply with VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

g. With respect to unsecured Protected Health Information (PHI), the contractor is deemed to have discovered a data breach when the contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.

h. If the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the contractor/subcontractor processes or maintains under the contract; the contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT. This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (to include the subcomponents of each) designed or developed for or on behalf of VA by any non-VA entity.

a. Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).

b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the security and privacy requirements for cloud environments.

c. VA IT contractors, subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, *Risk Management Framework for Cloud Computing Services* and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39 and FAR 40.2, specifically the prohibitions referenced.

d. The contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M-22-18 (September 14, 2022). The term “software” includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

e. The contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the contractor did not develop, all software configurations and all customizations.

f. The contractor shall ensure all contractor delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.

g. The contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the contractor shall provide required technical support to develop the configuration settings.

h. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default "program files" directory with silently install and uninstall. The contractor shall perform testing of all updates and patching prior to implementation on VA systems.

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

j. The contractor-delivered solutions shall reside on VA approved operating systems. Exceptions to this will only be granted with the written approval of the COR/CO.

k. The contractor shall design, develop, and implement security and privacy controls in accordance with the provisions of VA security system development life cycle outlined in NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, VA Directive and Handbook 6500, and VA Handbook 6517.

l. The Contractor shall comply with the Privacy Act of1974 (the Act), FAR 52.224-2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.

m. The contractor shall ensure the security of all procured or developed information systems, systems, major applications, minor applications, enclaves and platform information technologies, including their subcomponents (hereinafter referred to as "Information Systems") throughout the life of this contract and any extension, warranty, or maintenance periods. This includes security configurations, workarounds, patches, hotfixes, upgrades, replacements and any physical components which may be necessary to remediate all security vulnerabilities published or known to the contractor anywhere in the information systems (including systems, operating systems, products, hardware, software, applications and firmware). The contractor shall ensure security fixes do not negatively impact the Information Systems.

n. When the contractor is responsible for operations or maintenance of the systems, the contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE. This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (cloud and non-cloud) hosted, operated, maintained, or used on behalf of VA at non-VA facilities.

a. The contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities. Security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place. The controls will be tested by VA or a VA sanctioned 3PAO and approved by VA prior to hosting, operation, maintenance or use of the information system or systems by or on behalf of VA. This includes conducting compliance risk assessments, security architecture analysis, routine vulnerability scanning, system patching, change management procedures and the completion of an acceptable contingency plan for each system. The contractor's security control procedures shall be the same as procedures used to secure VA-operated information systems.

b. Outsourcing (contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.

c. The contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) on non-VA leased or non-VA owned IT equipment used to store, process or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).

e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with contractor activities are also subject to such assessments. The contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.

f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

g. The contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessment using government personnel or a third-party if deemed necessary. The contractor shall correct or mitigate any weaknesses discovered during the assessment.

h. VA prohibits the installation and use of personally owned or contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved contractor OE will be subject to technical inspection at any time.

i. The contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.

j. For cases wherein the contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.

k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING. This entire section applies whenever section 6 or 7 is included.

a. Should VA request it, the contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the contractor's IT or systems and controls, to ascertain whether the contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the contractor.

b. Any audits or tests of the contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the contractor uses to destroy, maintain, receive, retain, or use VA information.

c. As part of these audits, tests and assessments, the contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.

d. The contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the contractor has generated as part of its own security assessment. The contractor shall also notify VA of the existence of any such security reports or other related assessments, upon completion and validation.

e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The contractor shall comply with recommendations which result from these regulatory assessments on the part of VA regulators and associated government agency partners.

9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.

a. The contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain", which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any

information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the contractor to procure equipment, the contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.

c. All contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The contractor shall make spare parts available. All contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The contractor shall apply encryption technology to protect procured products throughout the delivery process.

d. If a contractor provides software or patches to VA, the contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).

e. The contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report "The Minimum Elements for a Software Bill of Materials (SBOM)."

f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

g. Throughout the delivery process, the contractor shall demonstrate a capability for detecting unauthorized access (tampering).

h. The contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

10. VIRUSES, FIRMWARE AND MALWARE. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.

a. The contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.

b. The contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The contractor shall provide or arrange for the provision of technical justification as to why any "false positive" hit has taken place to ensure their code's supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.

d. The contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter "virus or other malware") onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the contractor shall:

(1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA's information networks, computer systems and information systems; and

(2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

11. CRYPTOGRAPHIC REQUIREMENT. This entire section applies whenever the acquisition includes section 6 or 7 is included.

a. The contractor shall document how the cryptographic system supporting the contractor's products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.

b. The contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.

c. The contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.

d. The contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.

e. The contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

12. PATCHING GOVERNANCE. This entire section applies whenever the acquisition includes section 7 is included

a. The contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the follow:

(1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and

(2) The approach and capability to remediate newly reported zero-day vulnerabilities for contractor products.

b. The contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.

c. The contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by contractor within these time periods, the contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.

d. The contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be

provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING). This entire section applies when the acquisition includes one or more Medical Device, Special Purpose System or Research Scientific Computing Device. If appropriate, ensure selected clauses from section 6 or 7 and 8 through 12 are included.

a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing Devices shall comply with all applicable Federal law, regulations, and VA policies. New developments require creation, testing, evaluation, and authorization in compliance with processes specified on the Specialized Device Cybersecurity Department Enterprise Risk Management (SDCD-ERM) Portal, VA Directive 6550, *Pre-Procurement Assessment and Implementation of Medical Devices/Systems*, VA Handbook 6500, and the VA Information Security Knowledge Service. Deviations from Federal law, regulations, and VA Policy are identified and documented as part of VA Directive 6550 and/or the VA Enterprise Risk Analysis (ERA) processes for Specialized Devices/Systems processes.

b. All contractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500 and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work though the COR/CO for governance or resolution.

c. The contractor shall certify to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA needs to be created, the contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.

d. The contractor shall comply with all practices documented by the Food Drug and Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Post market Management of Cybersecurity in Medical Devices.

e. The contractor shall design devices capable of accepting all applicable security patches with or without the support of the contractor personnel. If patching can only be completed by the contractor, the contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.

f. The contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the contractor cannot install an anti-virus / anti-malware application.

g. The contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to or installation at a VA location.

h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive information will be returned to the contractor with media removed. When the contract requires return of equipment, the options available to the contractor are the following:

(1) The contractor shall accept the system without the drive, firmware and solid state.

(2) VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn-in; or

(3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then: (a) The equipment contractor shall 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.

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

14. DATA CENTER PROVISIONS. This entire section applies whenever the acquisition requires an interconnection to/from the VA network to/from a non-VA location.

a. The contractor shall ensure the VA network is accessed by in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

b. The contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

c. The contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).

d. The contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.

e. The contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

f. The contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.