PRODUCT DESCRIPTION (PD) TEMPLATE
DEPARTMENT OF VETERANS AFFAIRS

VA VISN 8 SUNSHINE NETWORK

Brand Name or Equal (BNE) PAR Excellence Weight Based Inventory Management System (WBIMS)

Date: July 10, 2026
VA-26-00068907
PD Version Number: 1.0

Contents

1.0 BACKGROUND 3
2.0 PRODUCT REQUIREMENTS 3
2.1 SALIENT CHARACTERISTCS 4
2.2 LICENSING 6
2.3 FACILITY INSTALLATION SERVICES 6
2.4 HOTLINE SUPPORT AND PERFORMANCE MONITORING 7
2.5 TRAINING 8
2.6 PROJECT MANAGEMENT 9
2.6.1 CONTRACTOR PROJECT MANAGEMENT PLAN 9
2.6.2 TECHNICAL KICKOFF MEETING 10
2.6.3 REPORTING REQUIREMENTS 10
2.7 RISK CONTROL 11
3.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508) 11
3.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS 11
3.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY 12
3.3 ACCEPTANCE AND ACCEPTANCE TESTING 12
4.0 SHIPMENT OF HARDWARE OR EQUIPMENT 12
4.1 SPECIAL SHIPPING INSTRUCTIONS 13
5.0 GENERAL REQUIREMENTS 14
5.1 VA TECHNICAL REFERENCE MODEL 14
5.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS 14
5.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION 14
5.4 INTERNET PROTOCOL VERSION 6 (IPV6) 15
5.5 SOFTWARE AND LICENSING REQUIREMENTS 15
5.6 TRUSTED INTERNET CONNECTION (TIC) 15
5.7 POSITION/TASK RISK DESIGNATION LEVEL(S) 16
6.0 POINTS OF CONTACT 17
7.0 INFORMATION SECURITY CONSIDERATIONS 17
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE 20

DRAFT

1.0 BACKGROUND

The Department of Veterans Affairs (VA), the VISN 8 Sunshine Network has a requirement to implement and support a Weight Base Inventory Management System (WBIMS) in secondary inventory locations with a brand name or equal (BNE) PAR Excellence (PAR Ex) WBIMS.

BNE PAR Ex is an inventory management technology that uses calibrated or weighted bins to capture data related to end user usage, stock replenishment, and other inventory related transactions in a supply closet. This technology captures transactions and usage data and keeps it stored on the user's workstation, allowing them to run reports, analyze data, and manage inventory. The primary purpose of BNE PAR Ex is to identify on-hand quantities and values between VISTA Generic Inventory Package (GIP) and the BNE PAR bins system.

The period of performance shall be 12-months from date of award, with two 12-month option periods to be exercised at the Governments discretion.

2.0 PRODUCT REQUIREMENTS

The Contractor shall provide and install a BNE PAR Excellence system at facilities listed below within the VISN 8 Sunshine Network to include Secondary inventory locations within those facilities. This shall include any ancillary components that may be required for the system to be fully operational. The BNE PAR Excellence system shall be able to meet the salient characteristics detailed in section 2.1-Salient Characteristics. Installation shall include all bins, scales, accessories, parts, labor, hardware, software, and training. The Contractor shall provide all tools or services required to complete the installation of the BNE PAR Excellence system.

During the base year the Contractor shall provide and install all bins, scales, accessories, parts, labor, hardware, software, and training at each VISN 8 Medical Facility locations as identified in Appendix A.1: TBD. The Contractor shall provide a 1-year warranty for all installed equipment and software, which includes replacements for defects or damage not caused by VA personnel. Warranties shall start upon completion of the installation and after VA verifies the system operates correctly. In each option period the Contractor shall provide necessary sustainment and support of the installed system to include software and hardware.

Travel for this effort shall be built into the Contractor's firm fixed price. Work may be performed at remote locations with prior concurrence in writing from the Contracting Officer's Representative (COR).

Tasks under this Contract shall be performed at the following VA facilities:

<u>Inventory Locations</u>:

VA Medical Centers (VAMC):

1. Bay Pines VA Healthcare System,10000 Bay Pines Blvd, Bay Pines, FL 33744
2. Orlando VA Healthcare System, Lake Baldwin VA Clinic 5201 Raymond Street Orlando, FL 32803-8208
3. Caribbean VA Healthcare System, 10 Casia St. San Juan, PR 00921-3201
4. James A. Haley Veteras' Hospital and Clinics, 13000 Bruce B. Downs Blvd Tampa, FL 33612
5. Miami VA Healthcare System, Bruce W. Carter VAMC ,1201 NW 16th Street Miami FL 33125
6. West Palm Beach VA Healthcare System, 7305 North Military Trail, West Palm Beach, FL, 33410
7. North Florida/South Georgia VA Healthcare System, 1601 S.W. Archer Road Gainesville, FL 32608-1197

2.1 SALIENT CHARACTERISTCS

The BNE PAR Excellence System shall have the following physical, functional and performance characteristics:

The BNE PAR Excellence System shall produce an accurate real-time reading of quantities on-hand accessible by a web-based program and provide data mining capabilities that shall include at a minimum: current stock levels, recommended re-order points, average usage levels per item and ability to track medical supply usage per patient treated at VISN 8 Medical Facility locations identified in section 2.0 .

The BNE PAR Excellence System shall interface with the Generic Inventory Package (GIP). The primary purpose of the interface is to identify out of balance on-hand quantities and values between GIP and the BNE PAR Excellence System. The BNE PAR Excellence System shall identify any out of balance on hand quantities and values, accounting for any due outs or due ins. If the out of balance condition is caused by a pending due in or due out, it shall be displayed separately to easily identify.

The BNE PAR Excellence System due-ins and due-outs shall automatically be removed when GIP due-ins and due-outs are "cleared".

The BNE PAR Excellence or Weight Based Inventory Management System shall:

1. Be a weight based inventory management system.
2. The system uses the empty bin weight to calculate actual supply quantities and inventory levels. Provide real-time visibility into our Secondary Inventory locations to include supply closets and primary inventory points within the following facilities.
    - Bay Pines VA Healthcare System
    - Orlando VA Healthcare System
    - VA Caribbean Healthcare System
    - James A. Haley Veteras' Hospital and Clinics
    - Miami VA Healthcare System

- West Palm Beach VA Healthcare System
- North Florida/South Georgia VA Healthcare System

3. Be integrated with VA Generic Inventory Package (GIP) package in Integrated Funds Distribution, Control Point Activity, Accounting, and Procurement (IFCAP) for real time data on available inventory.
4. Have wall mounted bins that are physically connected to the VA network (cannot use wireless).
5. VA Technology Reference Model (TRM)-approved.
6. Capable of tracking, adjusting, and reporting comprehensive real time information pertaining to the inventory of primary and secondary locations within the facilities in section 2.0.
7. Upon depletion of stock, the system shall trigger distribution tickets based on Periodic Automatic Replacement (PAR) levels/minimum order levels, Re-order points, and Emergency Stock Levels.
8. Software shall be intuitive and easy to train on in accordance with (IAW) Section 2.5 of this Product Description.
9. Allow its software to utilize multiple users with different levels of permissions.
10. Generate reports that are relevant to American Production and Inventory Control Society (APICS) Principles of Inventory Management.
11. Be able to handle a wide range of products in variation of and based on size, thickness, and weight.
12. Complete generic identification, solution shall uniquely identify and track all medical and surgical supplies through standardized item attributes, including manufacturer, item description, catalog number, lot number, expiration date, and inventory classification..
13. Convey equipment status - Communication about system status including system failures IAW Section 2.3.
14. Provide status of materials management related to–
    a. Open Orders.
    b. Emergency/Critical Item Levels.
    c. Negative Quantities on-Hand.
15. Provide item locations.
16. Provide current inventory levels –
    a. Level recommendations by cost and usage demand SKU reduction recommendations.
    b. Items over established baseline par levels.
    c. The system/solution will be able to recognize value trends and usage trends pertaining to stock outs and critical hit PAR level/minimum order level values over time.
17. Consumption tracking.
    a. Average monthly usage.

DRAFT

   b. Consumption analysis including time.
   c. Consumption deviation.
   d. Consumption over time.

18. Provide reports which include:
   a. Activity detail (sales, receipts, adjustments, etc.) to include time inventory on hand changed.
   b. Quantity on-hand Value on-hand.
   c. Department transactions.
   d. Cycle count sheet.
   e. Out of balance with GIP – on hand Due-ins.
   f. Due outs.
   g. Issue multiple discrepancy between GIP and PAR Bin.
   h. Emergency levels.
19. Provide Order status to include:
   a. Existing orders.
   b. Order preview.
20. Provide item details to include:
   a. Item master Item history.
   b. Item classification Reconciliation history.
   c. Most recent reconciliation per item.

2.2 LICENSING

The Contractor shall provide a yearly license agreement for use of BNE PAR Excellence System and related support starting immediately after installation for the life of the contract including the option period. Licensing shall include automatic software upgrades of the installed program and software. A BNE PAR Vision web-based program shall be available on any computer and/or mobile device for reporting purposes and evaluation of inventory levels for an unlimited number of users.

2.3 FACILITY INSTALLATION SERVICES

The Contractor shall provide installation of the BNE PAR Excellence system.

The Contractor shall provide notification to VA within 10 days prior to starting on-site activities. The Contractor shall coordinate with VA site escorts for installation.

The Contractor shall begin installation no later than 45 business days after the Technical Kickoff Meeting. Installation shall be phased by location area/closet and begin at the VISN 8 facilities in section 2.0 -

The Contractor shall complete on-site visits installation and setup based on award date and receipt of equipment. The installation shall furnish all secondary inventory point equipment, supplies and software necessary to achieve an operational system. All parts

DRAFT

supplied shall be compatible given room dimensions, access to data, and access to power. Contract parts coverage shall include all system options and shall include all manufacturer supplied software including that used by third party devices for no less than 12 months after completion.

The Contractor shall ensure that VA staff are able to access the BNE PAR Excellence system, and that VA staff are able to provision additional users themselves.

After installation is completed VA COR/PM or other VA appointed personnel will verify the BNE PAR Ex system is operating correctly, by verifying the scales are working properly, the scales are interfacing with or being monitored by a BNE PAR Ex Dashboard, and a BNE PAR Ex Dashboard is interfacing with the VA IFCAP/GIP to measure whether secondary inventory needs to be replenished.

Prior to start of installation in a secondary area/closet, if the area/closet has any old inventory or storage equipment (Omnicell or other), the Contractor shall remove the old inventory or storage equipment that will be replaced by BNE PAR Excellence and move it to a VA on-site designated area.

The Contractor shall remove all debris and trash to the VA's on-site designated trash/recycling location once installation is completed.

2.4 HOTLINE SUPPORT AND PERFORMANCE MONITORING

Functionality and accuracy of the installed equipment will be continuously monitored by VA Logistics staff to ensure equipment operates according to the salient characteristics detailed in paragraph 2.1 and provides accurate and timely information for inventory and reordering purposes. VA will notify the Contractor's Support Hotline of any issues via Contractor's support phone number or email.

The Contractor shall provide VA with a Support Hotline telephone number and email that VA can use to notify the Contractor of any issues with the installed equipment or software. The Support Hotline shall be staffed 7:00AM – 8:00PM EST and available 24x7x365 to provide support or assistance to VA. The Contractor shall respond to service calls no later than 24 hours after being notified of a problem with either equipment or installed software and resolve within 48 hours of notification by VA any defects or functionality problems detected.

The Contractor shall work with VA onsite to replace supported hardware within 48 hours of notification of a problem if VA is not at fault for damage or defect. This assumes there is backup equipment onsite. If backup equipment is not onsite, the Contractor's support staff shall work with VA onsite to replace equipment when it arrives via Contractor's return merchandise authorization process.

The Contractor shall provide performance monitoring. The Contractor's PTPS (Proactive Technical Product Support) or similar system shall monitor the installed equipment and software remotely by daily check-ins that shall occur remotely at least

four times every 24 hours for 12 months for each period of performance after installation completed. The Contractor shall notify VA and provide maintenance support in the event of a problem with equipment or software detected during the performance monitoring.

The Contractor shall communicate about support via telephone calls, electronic messaging, or email and meet (in person or can be virtual) with the COR monthly to address and provide any corrective action for any unresolved issues.

2.5 TRAINING

All VISN 8 Medical Facilities require training for VA Logistics staff end users, super users, supervisors, and leadership. End users are the supply technicians, super users are the Lead Supply technicians, supervisors are supervisors for supply technicians, and leadership includes the Chief and Assistant Chiefs for Logistics Management Specialists (LMS) and the Supervisor for Acquisition.

The Contractor shall provide a detailed Training Plan that VA can use to verify the training will meet VA's training requirement for the BNE PAR Excellence system for end users, super users, supervisor, and leadership.

The Contractor shall provide training for end-users, super-users, supervisors, and leadership at all locations where the BNE PAR Excellence system is installed. The Contractor shall provide materials designed to facilitate continued internal training by VHA personnel throughout the lifecycle of the system (i.e., train-the-trainer). The Contractor shall hold the training at a secondary inventory location so all trainees can learn hands-on. The Contractor shall record the supply technician training at every site. The training shall include, but not be limited to:

a. Adding items to an inventory
b. Removing items from an inventory
c. Assigning items
d. Weighing items and recalibrating scales
e. Editing items
f. Troubleshooting
g. Reporting functions
h. Future/upcoming enhancements
i. Swapping Scales and making sure they are working.
j. Turn the BNE PAR Location equipment on or off
k. Disconnect and reconnect power from the BNE PAR location equipment
l. Add, change, remove and register scales
m. Properly register and exchange BNE PAR location equipment
n. Visually and verbally assist Service Provider in diagnosing BNE PAR location equipment problems
o. Maintain the system database
p. Build and extract orders.

DRAFT

q. Build and extract applicable interfaces.
r. Perform system backup.
s. Visually and verbally assist Service Provider in diagnosing Software problem.

The Contractor shall provide training materials (brochure, book, Power Point slides) designed to facilitate VA's train-the-trainer program throughout the lifecycle of the system. The training materials will be used by the Contractor-trained VA Supply Technicians to train the VA supply technicians on the next hospital/clinic shift, who will train the VA supply technicians on the hospital/clinic shift after that, so that all VA supply technicians for that closet can operate the system.

The Contractor shall maintain records of supply technician training participants and whether the participants completed the training or not and provide the records to the COR upon request.

The Contractor shall coordinate all supply technician training dates with the COR who will communicate to the supply technicians the date of their training.

The Contractor shall provide the VA supply technicians with the tools and knowledge to fully operate the scales and conduct checks per the manufacturer's instructions, as well as answer any questions personnel may have regarding the BNE PAR Excellence system.

The Contractor shall provide User Manuals and Technical Maintenance Manuals.

Deliverables:

A. Training Plan
B. Supply Technician Training
C. Supply Technician Training Recording (for each secondary inventory location)
D. User Manuals/Technical Maintenance Manuals
E. Training Materials

2.6 PROJECT MANAGEMENT

2.6.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PD. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the Period of Performance (PoP).

Deliverable:

A. Contractor Project Management Plan

2.6.2 TECHNICAL KICKOFF MEETING

A technical kickoff meeting shall be held within 10 business days after Contract is awarded. The Contractor shall coordinate the date, time, and location (can be virtual) with the Contracting Officer, VA PM, Contract Specialist, and the Contracting Officer Representative. The Contractor shall provide a draft agenda to the CO and VA PM at least 5 business days prior to the meeting. Upon Government approval of the final agenda, the Contractor shall distribute to all meeting attendees. During the technical kickoff-meeting, the Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule in a Technical Kickoff Meeting Presentation. The Contractor shall submit the final updated technical kickoff meeting presentation to the CO within three (3) business days after the meeting. The Contractor shall prepare and distribute the meeting minutes of the kickoff meeting to the CO, COR and all attendees within three business days after the meeting.

VA will provide the VA Project Team email distribution list to the Contractor at the Technical Kickoff Meeting.

Deliverables:

A. Technical Kickoff Meeting Agenda
B. Technical Kickoff Meeting Presentation
C. Technical Kickoff Meeting Minutes

2.6.3 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month. The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall meet (e.g., can be virtual in person, telephone, etc.) with the COR monthly to address any unresolved issues and discuss any unresolved and/or continuous issues and corrective actions for them with the Contracting Officer (CO).

Deliverable:

A. Monthly Progress Report

DRAFT

2.7 RISK CONTROL

The Contractor, i.e., Contractor employees, responsible for installation and setup, shall have background check completed or show proof of background check completed no longer than one year ago, from date of award including fingerprint analysis. The VA will provide PIV sponsorship to Contractor employees performing work.

The Contractor may be installing a supply storage and tracking system in an area under construction. The Contractor shall be cognizant of staff movements, equipment and a plethora of activity during certain periods of the workday. The Contractor shall be accompanied by an escort during on-site activities. Installation staff shall have no patient contact or access to sensitive patient information. COR will be available for risk intervention should the need arise.

3.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508)

On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508 and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

3.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508 Standards and 255 Guidelines will be supplied upon request or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

The Contractor shall comply with “508 Chapter 2: Scoping Requirements” for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria
- ☒ E206 Hardware Requirements
- ☒ E207 Software Requirements

☒ E208 Support Documentation and Services Requirements

3.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY

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

3.3 ACCEPTANCE AND ACCEPTANCE TESTING

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

4.0 SHIPMENT OF HARDWARE OR EQUIPMENT

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Ship To and Mark For:

Bay Pines VA Healthcare System
Primary: Leroy J. Willis
Alternate: Joseph E. Hoyle
Address: 4614 Pet Ln., Lutz, FL 33559
Voice: 727-398-6661 x:15530
Email: Leroy.Willis@va.gov

Orlando VA Healthcare System
Primary: Hector De Jesus
Alternate: Veneshwarie Mulchand
Address: 13800 Veterans Way Orlando, FL 32827
Voice: 407-631-1000
Email: Hector.Dejesus1@va.gov

VA Caribbean Healthcare System
Primary: Brunilmarie Gonzalez-Rubio
Alternate: Maraida Velazquez
Address: VSS Logistics 1250 Imeson Park Blvd. Suite 213 Jacksonville FL 32218
Voice: 787-641-7582 Ext. 134941
Email: Brunilmarie.Gonzalez-Rubio@va.gov

James A. Haley Veteras' Hospital and Clinics

DRAFT

Primary: Ronkeisha Pughsley
Alternate: Jesse Mitsch
Address: 13000 Bruce B. Downs Blvd. Tampa, FL 33612
Voice: 813-972-2000 Ext. 104257
Email: Ronkeisha.Pughsley@va.gov

Miami VA Healthcare System
Primary: Eric Wilhelm
Alternate: Ryan Jackson
Address: 6725 NW 36th Street Suite 695 Miami Fl, 33166
Voice: 786-849-0500
Email: Eric.Wilhelm@va.gov

West Palm Beach VA Healthcare System
Primary: Andrea Fails
Alternate: Stevland Andrews
Address: 7305 North Military Trail, West Palm Beach, FL, 33410
Voice: 561-433-1200 ext. 2465
Email: Andrea.Fails@va.gov

North Florida/South Georgia VA Healthcare System
Primary: Jamie Dillard
Alternate: Sherry Spikes
Address: 1601 S.W. Archer Road Gainesville, FL 32608-1197
Voice: 352-548-6000 Ext 10-7154
Email: Jamie.Dillard@va.gov

4.1 SPECIAL SHIPPING INSTRUCTIONS

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

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

All shipments, either single or multiple container deliveries, shall bear the VA IFCAP Purchase Order number (if applicable) on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO or Contract number shall indicate total number of containers for the complete shipment (e.g. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO # or Contract No.: _____TBD_____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))
Project Description: (e.g. Tier I Lifecycle Refresh)

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

The VA shall provide 20 pallets spaces in the main facility for staging the product.

5.0 GENERAL REQUIREMENTS

5.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall comply with the VA OIT Technical Reference Model (VA TRM). Compliance with the VA TRM is achieved by using only technologies and standards that are listed as approved for use in the VA TRM. The Contractor shall provide all necessary information requested by VA to ensure TRM approval is obtained prior to use on VA's network.

5.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and Plan of Action & Milestones (POAM) will not be accepted in the event these controls cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

5.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN

DRAFT

with the Integrated Control Number (ICN) in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

5.4 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). Which defines IPv6-only as the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-Only environments. IPv6-Only technology, in accordance with the USGv6 Program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 “USGv6 Profile” (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 “Guidelines for the Secure Deployment of IPv6” (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices, applications, and systems shall support all applicable functionality on native IPv6-Only as well as dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) shall support native IPv6-Only and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

5.5 SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration, operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor’s proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

5.6 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative“ (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 “Secure External Connections”, and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the

Cybersecurity & Infrastructure Security Agency (CISA)
(https://www.cisa.gov/publication/tic-30-core-guidance-documents.)

5.7 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity and Background Investigation Requirements by Service Task/Item Number

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
2.0	☒	☐	☐
2.1	☒	☐	☐
2.2	☒	☐	☐
2.3	☒	☐	☐
2.4	☒	☐	☐
2.5	☒	☐	☐
2.6	☒	☐	☐
2.7	☒	☐	☐

The Tasks identified above, and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working.

DRAFT

6.0 POINTS OF CONTACT

VA Program Manager:

Name: Ruben Rivera-Rivera
Address: 10 Casia St. San Juan, PR 00921
Voice: 787-664-0277
Email: Ruben.Rivera-Rivera@va.gov

Contracting Officer's Representative:

Name: Ruben Rivera-Rivera
Address: 10 Casia St. San Juan, PR 00921
Voice: 787-664-0277
Email: Ruben.Rivera-Rivera@va.gov

Contracting Officer:

Name: Jason King
Email: Jason.King6@va.gov

Contract Specialist:

Name: Christopher Franzese
Email: Christopher.Franzese@va.gov

7.0 INFORMATION SECURITY CONSIDERATIONS

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this Product Description.

a. Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA."
b. A requirement for data breach notification: Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access, the Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO, and Privacy Officer for the contract. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. See VA Handbook 6500.6, Appendix C, paragraph 6.a.
c. A requirement to pay liquidated damages in the event of a data breach: "In the event of a data breach or privacy incident involving SPI the contractor processes or

maintains under this contract, the contractor shall be liable to VA for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals." However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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

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

d. A requirement for annual security/privacy awareness training: "Before being granted access to VA information or information systems, all Contractor employees and Subcontractor employees requiring such access shall complete on an annual basis either: (i) the VA security/privacy awareness training (contains VA security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA's security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the Contractor. If the Contractor provides their own training that conforms to VA's requirements, they will provide the COR or CO, a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in VA's contract have received their annual security/privacy training that meets VA's requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9.
e. A requirement to sign VA's Rules of Behavior: "Before being granted access to VA information or information systems, all Contractor employees and Subcontractor employees requiring such access shall sign on annual basis an acknowledgement that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior which is attached to this contract." See VA Handbook 6500.6, Appendix C, paragraph 9, and Appendix D. Note: If a medical device vendor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the vendor's designated representative. The contract must reflect by signing the Rules of Behavior on behalf of the vendor that the designated representative agrees to ensure that all such

individuals review and understand the Contractor Rules of Behavior when accessing VA's information and information systems.

DRAFT

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE

NOTE: In the event of a conflict, VAAR Security Clauses take precedence over the language in this Addendum B.

APPLICABLE SECTIONS FROM: VA NOTICE 24-12, APRIL 22, 2024, UPDATE TO VA HANDBOOK 6500.6, CONTRACT SECURITY, APPENDIX C VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE

B1. 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.

B2. VA INFORMATION CUSTODIAL 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.

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).

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 contractor.

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 certain 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

DRAFT

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.

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees 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

DRAFT

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,

DRAFT

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.

B4. TRAINING

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 thirty 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.

B5. SECURITY INCIDENT INVESTIGATION

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

DRAFT

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.

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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 39.1, 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

DRAFT

support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository,

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.

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

DRAFT

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

DRAFT

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.

B8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING

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

DRAFT

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.

B9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING

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

DRAFT

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.

B10. VIRUSES, FIRMWARE, AND MALWARE

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.

B11. CRYPTOGRAPHIC REQUIREMENT

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.

B12. DATA CENTER PROVISIONS

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.

DRAFT