

**PERFORMANCE WORK
STATEMENT (PWS)
DEPARTMENT OF VETERANS
AFFAIRS**

**Office of Small and Disadvantaged
Business Utilization Shared
Services Directorate**

**Information Technology Systems Integration (ITSI) Support
Services Contract**

DRAFT

1.0 BACKGROUND

The Office of Small & Disadvantaged Business Utilization (OSDBU) provides numerous services for Veterans and Service-Disabled Veterans who seek to open or expand a business. OSDBU provides outreach and liaison support to businesses (small and large) and other members of the public and private sectors concerning Small Business Acquisition issues.

OSDBU monitors the Department of Veterans Affairs (VA) implementation and execution of the contract socioeconomic programs. OSDBU operates and maintains the Veterans Enterprise Management System (VEMS). VEMS is a collection of capabilities integrated with single-sign-on access. **The VEMS backend is built on the Microsoft D-365 CRM platform, and the front end (the VetBiz Portal) utilizes Microsoft PowerApps Portals. This SaaS system is supported by Azure Services, located in the VA Enterprise Cloud (VAEC). VEMS is integrated with the VA Enterprise SharePoint online.**

The requirements for increased levels of efficiency necessitate a continually evolving and expanding demand for information systems support. To meet these growing demands, OSDBU has established a unified team that offers reliable and effective technology solutions and services to enable OSDBU leadership and staff to serve Veterans and other key stakeholders to achieve mission success. The OSDBU Information Technology Systems Integration team (ITSI) responsibilities include balancing the Information Management and Information Technology (IM&IT) demands of the OSDBU directorates and the OSDBU leadership priorities to manage IT. Additionally, the Department of Veterans Affairs (VA), Office of Information & Technology (OIT) utilizes the Enterprise Mission Assurance Support Service (eMASS) as its risk management framework. eMASS is a government-owned web-based application with a broad range of services for comprehensive, fully integrated cybersecurity management. Features include dashboard reporting, controls scorecard measurement, and the generation of a system security authorization package. eMASS provides an integrated suite of authorization capabilities and prevents cyber-attacks by establishing strict process control mechanisms for obtaining authorization decisions.

2.0 APPLICABLE DOCUMENTS

The Contractor shall comply with documents listed below. Additional documents may be listed in individual Task orders.

1. 44 U.S.C. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. "Federal Information Security Modernization Act of 2014"
3. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules"
4. FIPS Pub 199. "Standards for Security Categorization of Federal Information and Information Systems," February 2004

5. FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
6. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
9. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
10. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
11. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, <https://www.va.gov/vapubs/index.cfm>
12. VA Handbook 0710, "Personnel Security and Suitability Program," May 2, 2016, <https://www.va.gov/vapubs/index.cfm>
13. VA Directive and Handbook 6102, "Internet/Intranet Services," August 5, 2019
14. 36 C.F.R. Part 1194 "Information and Communication Technology Standards and Guidelines," January 18, 2017
15. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
16. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
17. NIST SP 800-66 Rev. 1, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," October 2008
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, "VA Cybersecurity Program," February 24, 2021
21. VA Handbook 6500, "Risk Management Framework for VA Information Systems VA Information Security Program," February 24, 2021
22. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)," March 12, 2019
23. VA Handbook 6500.5, "Incorporating Security and Privacy into the System Development Lifecycle," March 22, 2010
24. VA Handbook 6500.6, "Contract Security," March 12, 2010
25. VA Handbook 6500.8, "Information System Contingency Planning," April 6, 2011
26. VA Handbook 6500.10, "Mobile Device Security Policy," February 15, 2018
27. VA Handbook 6500.11, "VA Firewall Configuration," August 22, 2017
28. OIT Process Asset Library (PAL), <https://www.va.gov/process/> . Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp>
29. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)

30. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
31. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
32. VA Handbook 6510, "VA Identity and Access Management," January 15, 2016
33. VA Directive and Handbook 6513, "Secure External Connections," October 12, 2017
34. VA Directive 6300, "Records and Information Management," September 21, 2018
35. VA Handbook, 6300.1, "Records Management Procedures," March 24, 2010
36. NIST SP 800-37 Rev 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018
37. NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Federal Information Systems and Organizations," September 23, 2020 (includes updates as of 12/10/2020)
38. VA Directive 0735, "Homeland Security Presidential Directive 12 (HSPD-12) Program," October 26, 2015
39. VA Handbook 0735, "Homeland Security Presidential Directive 12 (HSPD-12) Program," March 24, 2014
40. OMB Memorandum 05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005
41. OMB Memorandum M-19-17, "Enabling Mission Delivery Through Improved Identity, Credential, and Access Management," May 21, 2019
42. OMB Memorandum, "Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation," May 23, 2008
43. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011, (NOTE: Part A of the FICAM Roadmap and Implementation Guidance, v2.0, was replaced in 2015 with an updated Architecture (<https://arch.idmanagement.gov/#what-is-the-ficam-architecture>))
44. NIST SP 800-116 Rev 1, "Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access," June 2018
45. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, "Digital Identity Guidelines," updated March 02, 2020
46. NIST SP 800-157, "Guidelines for Derived PIV Credentials," December 2014
47. NIST SP 800-164, "Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)," October 2012
48. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981, "Mobile, PIV, and Authentication," March 2014
49. VA Memorandum, VAIQ #7100147, "Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12)," April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)

50. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
51. VA Memorandum "Personal Identity Verification (PIV) Logical Access Policy Clarification," July 17, 2019, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>
52. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, <https://www.cisa.gov/publication/tic-30-core-guidance-documents>
53. OMB Memorandum M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative," September 12, 2019
54. OMB Memorandum M-08-23, "Securing the Federal Government's Domain Name System Infrastructure," August 22, 2008
55. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
56. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
57. Executive Order 13834, "Efficient Federal Operations," dated May 17, 2018
58. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
59. VA Directive 0058, "VA Green Purchasing Program," July 19, 2013
60. VA Handbook 0058, "VA Green Purchasing Program," July 19, 2013
61. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access," January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
62. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
63. "Veteran Focused Integration Process (VIP) Guide 4.0," January 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
64. VA Memorandum "Proper Use of Email and Other Messaging Services," January 2, 2018, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
65. "DevSecOps Product Line Management Playbook" version 2.0, May 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946>
66. NIST SP 500-267B Revision 1, "USGv6 Profile," November 2020
67. OMB Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," November 19, 2020
68. Social Security Number (SSN) Fraud Prevention Act of 2017
69. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018

3.0 SCOPE OF WORK

The Contractor shall provide project management, technical support, business process re-engineering support, systems integration, governance, and life cycle support for various information technology systems supporting OSD's line of business. The systems include OSD's core business systems such as the VetBiz Portal, the VetBiz

Stat (Goals Management, Predictive Analytics and Market Research system), Forecast of Opportunities (FCO), Event Management Software as a Service (EMSS), 2268NextGen and other applications being developed for the Veterans Enterprise Management System.

The Contractor shall provide IT expertise, technical knowledge, support personnel, and other related resources necessary to support the following areas:

1. IT Governance
2. Business process requirements definition
3. Microsoft Dynamic Customer-service Relationship Management (CRM) D365 administration and maintenance
4. Systems and User administration for all business systems as required
5. Cyber and systems security support
6. Lifecycle activities for software improvement, systems integration, and web/interface
7. Program and project management.
8. SharePoint development and maintenance
9. Portal development and maintenance
10. IT Technical Support

3.1 ORDER TYPE

The effort shall be proposed on a Firm Fixed Price (FFP) basis.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) for this requirement shall be a 12-month base period with four (4) 12-month option periods and one optional task. Optional task is as follow:

- a. Optional Task One "Phrase-Out Transition Support" This option may be exercised once during the duration of the contract in either the base or one of the option periods.

There are eleven (11) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Juneteenth	June 19
Independence Day	July 4

Veterans Day
Christmas Day

November 11
December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday
Washington's Birthday
Memorial Day
Labor Day
Columbus Day
Thanksgiving

Third Monday in January
Third Monday in February
Last Monday in May
First Monday in September
Second Monday in October
Fourth Thursday in November

Dates observed only by the District of Columbia as a holiday:

Inauguration day
Inauguration day

Monday January 20, 2025
Saturday January 20, 2029

If any of the holidays that are set by date falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if any of the dates falls on a Sunday, then Monday shall be observed as a holiday.

4.2 PLACE OF PERFORMANCE

Efforts under this requirement shall be performed at the Contractor facilities. The Contractor shall identify the Contractor's place of performance in their Task Execution Plan submission.

4.3 TRAVEL

The Government does not anticipate travel associated with the task under this PWS.

4.4 RESERVED

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 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 PWS. 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 PoP.

Deliverable:

- A. Contractor Project Management Plan (CPMP)
- B. CPMP Updates

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Weekly 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 week.

The Weekly 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.

Deliverable:

- A. Weekly Progress Report

5.1.3 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within ten (10) days after contract award. The Contractor shall coordinate the date, time, and location (can be virtual) with the Contracting Officer (CO) as the Post-Award Conference Chairperson, the VA PM as the Co-Chairperson, the Contract Specialist (CS), and the COR. The Contractor shall provide a draft agenda to the CO and VA PM at least five (5) calendar days before the meeting. The Contractor shall distribute a final agenda to all meeting attendees upon government approval. During the kickoff meeting, the Contractor shall present, for

review and approval by the Government, the details of the intended approach, work plan, onboarding schedule and project schedule for each effort via a Microsoft Office PowerPoint presentation.

The Contractor shall deliver the presentation with a final slide entitled "Summary Report," which shall include notes on any significant issues, agreements, or disagreements discussed during the kickoff meeting and the following statement: "As the Post-Award Conference Chairperson, I have reviewed the entirety of this presentation and assert that it is an accurate representation and summary of the discussions held during the Technical Kickoff Meeting for "Information Technology Systems Integration (ITSI) Support Services Contract." The Contractor shall submit the final updated presentation to the CO for review and signature within three (3) calendar days after the meeting.

The Contractor shall also work with the CS, the Government's designated note taker, to prepare and distribute the meeting minutes of the kickoff meeting to the CO, COR and all attendees within three (3) calendar days after the meeting. The Contractor shall obtain concurrence from the CS on the content of the meeting minutes before distribution of the document.

Deliverables:

- A. Kickoff Agenda
- B. Kickoff Presentation/ final slide entitled "Summary Report"
- C. Kickoff Meeting Minutes

5.1.4 ONBOARDING

The Contractor shall manage the onboarding of its staff. Onboarding includes steps to obtain a VA PIV card, network and email account, complete training, initiate background investigations, and gain physical and logical access. In addition, the Contractor shall identify individuals that may require elevated privileges to the necessary development and test environments for the various systems to be enhanced. After review by the Contractor and VA, a decision will be made as to the necessity of obtaining GFE for the onboarding staff. If approved, Contractor shall follow the appropriate steps to obtain the equipment.

A single Contractor Onboarding point of contact (POC) shall be designated by the Contractor that tracks the onboarding status of all Contractor personnel. The Contractor Onboarding POC shall be responsible for accurate and timely submission of all required VA onboarding paperwork to the VA COR. The Contractor shall be responsible for tracking the status of all their staff's onboarding activities to include the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security and role-based training, and their next required training date. The Contractor Onboarding POC shall also report the status at the staff level during onboarding status

meetings. The Contractor shall provide an Onboarding Status Report weekly for any staff with outstanding onboarding requests for review by the COR, VA Program Manager and Project Manager.

Deliverable:

A. Monthly Onboarding Status Report

5.1.5 KEY PERSONNEL

The Contractor shall be responsible for managing and overseeing the activities of all Contractor personnel, as well as subcontractor efforts, used in performance of this effort. This effort demands a high level of technical proficiency. Contractor resources shall be identified, be PIV eligible and begin the onboarding process on day one of the TO, to include submission of all required security and PIV documentation in order to have access to the VA network.

The Contractor has a contractual obligation to mitigate the consequences of the loss of Key Personnel and shall promptly secure any necessary replacements in accordance with (IAW) this PWS section, with approval of the COR/PM and concurrence of the CO. The Contractor shall suitably and timely replace Key Personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work, and be reasonably forthcoming about the need for such replacement. Failure to do so, or if the resultant reduction of productive effort would be so substantial as to impair the successful completion of the task order, may result in the task order being terminated by the CO for default or for the convenience of the Government, as appropriate. In addition, if the Contractor is found at fault for a delay or impairment to the contract work because of a loss of key personnel, the CO may elect to equitably decrease the contract price to compensate the Government for any resultant delay, loss, or damage.

The labor categories below are identified as Key Personnel. Key Personnel must meet the corresponding requirements identified in the Labor Description column below:

Key Personnel Positions	Name
System/Dev Ops Engineer Expert	
CRM D365 System Admin	
Cyber Security Expert	
SharePoint Developer	
D365 CRM Developer / Solution Architect	

LCAT	Minimum Technical Capabilities	Minimum Qualifications
System/Dev Ops Engineer Expert Computer and Information Systems Manager, Senior	<p>Expertise providing the following:</p> <ul style="list-style-type: none"> • Azure Dev Ops • Azure Cloud hosting • Ability to support ASP.NET, Microsoft Structured Query Language (SQL), .NET Core, SSL, and TLS • Design, develop, and maintain scalable and stable Azure solutions. • Automate tasks through scripting and other appropriate tools. • Ensure security and compliance with Azure policies and procedures. • Provide technical support and troubleshooting to resolve infrastructure-related issues. • Collaborate with software developers to optimize application performance. • Stay updated with the latest trends in Azure services and DevOps methodologies. • Document and maintain Azure environment configurations and custom scripts. 	<p>Required Years of Experience:</p> <p>8 -15 years of experience performing work relevant to the PWS task requirements.</p> <p>Required Education: Bachelor's degree in computer science, Information Technology, Engineering, or a relevant field. ***Preferred certifications and years of experience can be substituted for education, only if requested.</p> <p>Required Professional/Technical Expertise:</p> <ul style="list-style-type: none"> • Proven experience as an Azure DevOps Engineer or similar role in cloud engineering. • Expertise in Azure cloud services and DevOps practices. • Experience with scripting languages. • Understanding of network architectures and services (e.g., VPN, routing, firewall, etc.). • Knowledge of container and orchestration services. • Proficiency in using Git for version control. <p>Preferred Professional/Technical Expertise:</p> <ul style="list-style-type: none"> • Experience navigating the VA OIT organization. <p><u>Microsoft Certified</u></p> <ol style="list-style-type: none"> 1. Azure Developer Associate 2. Azure Fundamentals <p>Preferred Certifications:</p>

		<ul style="list-style-type: none"> Microsoft Certified: Designing and Implementing Microsoft DevOps Solutions <p><u>Microsoft Certified</u></p> <ol style="list-style-type: none"> Azure Administrator Associate DevOps Engineer Expert
CRM D365 System Admin Computer Systems Analyst, Senior	Expertise providing the following: <ul style="list-style-type: none"> Ability to Configure D365 elements, including custom entities, fields, views, model-driven apps, business process flows, workflows, and business rules. Ability to create dashboards and charts. Ability to integrate Power BI and CRM D365 dashboards. Ability to provide recommendations and identify critical issues and processing faults. Ability to perform testing on system changes and document dependencies. 	<p>Required Years of Experience:</p> <p>4-8 years of experience performing work relevant to the PWS task requirements.</p> <p>Required Education:</p> <p>Associate degree in a field of study relevant to the PWS task requirements. ***Preferred certifications and years of experience can be substituted for education, only if requested.</p> <p>Required Professional/Technical Expertise:</p> <p><u>Microsoft 365 Certified</u></p> <ol style="list-style-type: none"> Fundamentals Azure Fundamentals <p>Preferred Certifications:</p> <p><u>Microsoft 365 Certified:</u></p> <ol style="list-style-type: none"> Collaboration Communications Systems Engineer Associate Endpoint Administrator Associate Configure secure access to your workloads using Azure networking Create and manage automated processes by using Power Automate Information Protection and Compliance Administrator Associate

Cyber Security Expert Information Security Analyst, Senior	Expertise providing the following: <ul style="list-style-type: none"> • Drafting documents required as evidence in the Risk Management Framework. • Interpreting cyber security policies and their impact on information systems. • Updating Risk Management Framework. • Tracking POAMs for remediation. • Managing Authorization to Operate (ATO) Process. 	6. Azure Administrator Associate Required Years of Experience: <p>10-12 years of experience performing work relevant to the PWS task requirements.</p> <p>Required Education:</p> <p>Bachelor's degree in computer science, Information Technology, Engineering, or a relevant field.</p> <p>***Preferred Professional/Technical Expertise and years of experience can be substituted for education, only if requested.</p> <p>Required Professional/Technical Expertise:</p> <p>CompTIA Security+ certified (CySA+)</p> <p>Preferred Professional/Technical Expertise:</p> <ul style="list-style-type: none"> • VA Experience attaining an ATO. • Enterprise Mission Assurance Support Service (eMASS) experience. • Certified Information Systems Security Professional (CISSP) • Information Technology Infrastructure Library (ITIL) Foundation.
SharePoint Developer Software Developer, Systems Software, Senior	Expertise providing the following: <ul style="list-style-type: none"> • Collaborate with business stakeholders to build apps that address their specific needs. • Develop SharePoint sites utilizing SharePoint Online. 	Required Years of Experience: <p>6-10 years of experience performing work relevant to the PWS task requirements.</p> <p>Required Education:</p> <p>Bachelor's degree in computer science, Information Technology,</p>

	<ul style="list-style-type: none"> • Create automated forms and workflows using power apps/automate. • Integrate SharePoint lists with Power BI. • Maintain All OSDBU SharePoint sites, lists, apps, workflows and document repositories as required. • Update all OSDBU SharePoint sites, lists, apps, workflows and document repositories as required. 	<p>Engineering, or a relevant field. ***Preferred certifications and years of experience can be substituted for education, only if requested.</p> <p>Required Professional/Technical Expertise:</p> <ul style="list-style-type: none"> • Experience with SharePoint Online and InfoPath forms. • Experience with PowerApps, Power Automate and Power BI. • Experience in the collection and documentation of user's requirements, development of user stories. • Experience with MS Teams and Office 365. • Experience maintaining release schedules. • Experience publishing, consuming, and using XML and/or JSON. • Experience in SharePoint Designer, InfoPath, Web Parts, and workflow creation. <p>Preferred Professional/Technical Expertise:</p> <p>Microsoft SharePoint Certification</p>
<p>D365 CRM Developer / Solution Architect Computer Systems Engineer/Architect, Senior</p>	<p>Expertise providing the following:</p> <ul style="list-style-type: none"> • Design, develop, and implement Dynamics 365 CRM solutions tailored to meet client requirements. • Engage with stakeholders to scope, map out, and document business requirements, translating them into 	<p>Required Years of Experience:</p> <p>6 – 10 years of experience performing work relevant to the PWS task requirements.</p> <p>Required Education:</p> <p>Bachelor's degree in computer science, Information Technology, Engineering, or a relevant field. ***Preferred certifications and years of experience can be substituted for</p>

	<p>technical specifications.</p> <ul style="list-style-type: none"> • Provide consulting expertise in Dynamics 365 CRM for both internal and external client-facing roles, ensuring optimal solution delivery. • Work cooperatively with cross-functional teams, including developers, consultants, and business analysts, to ensure successful project execution. • Stay current with the latest developments in Dynamics 365 CRM and related technologies, providing guidance on best practices and industry standards. • Familiarity with Power Platform (Power Apps, Power BI, Power Automate). • Knowledge of Azure services and integration patterns. 	<p>education, only if requested.</p> <p><i>Required Professional/Technical Expertise:</i></p> <ul style="list-style-type: none"> • Experience in both internal and external client-facing roles. • Proficient in C# and JavaScript and SQL. • Strong understanding of Dynamics CRM architecture and customization. • Experience with CRM integrations and data migration. • Excellent problem-solving and communication skills <p><u>Microsoft Certified</u></p> <ol style="list-style-type: none"> 1. Dynamics 365 Business Central Developer Associate 2. Power Platform Developer Associate <p><i>Preferred Certifications:</i></p> <p><u>Microsoft Certified</u></p> <ol style="list-style-type: none"> 1. Dynamics 365: Finance and Operations Apps Developer Associate 2. Microsoft Certified: Azure Solutions Architect Expert
--	--	--

5.1.6 PROJECT COORDINATION

The Contractor shall conduct quarterly in-progress review meetings to discuss the status of all sub-tasks in this PWS, as well as schedules, risks, and any issues encountered throughout the PoP. The Contractor shall provide the COR with the agenda for quarterly in-progress review briefings via email at least one business day before the meeting, addressing the information to be discussed during the quarterly in-process review meeting. Upon completion of all quarterly in-progress review meetings, the Contractor shall provide quarterly in-progress meeting minutes detailing all meeting discussions and action items, and they shall provide a copy of the slide deck used in the briefing. These quarterly meetings shall be conducted via VA-approved virtual meeting applications or systems.

Deliverable:

- A. Quarterly In-Progress Review Briefing Slide Deck

B. Quarterly In-Progress Review Meeting Minutes

5.2 INFORMATION TECHNOLOGY (IT) GOVERNANCE SUPPORT

The Contractor shall provide IT governance support functions ensuring IT projects comply with VA standards, guidance, and directives. The Contractor shall support the activities and operating efficiency of OSDBU technical systems, development, and integration. The Contractor shall continuously identify deficiencies found within the OSDBU IT portfolio and provide a Written Corrective Actions Recommendations Report, which shall include the identification of the deficiency and the steps that need to be accomplished to resolve it entirely. The Contractor shall develop Standard Operating Procedures (SOPs) for the administration, operation, and maintenance of all OSDBU systems, including but not limited to user access procedures, trouble ticket procedures, continuity of operation procedures, systems administration procedures, IT governance procedures, change control procedures, requirements development procedures, SharePoint development, deployment, and system administration procedures.

The Contractor shall conduct impact analyses and submit an Impact Analysis Report for changes that have a direct or asymmetric impact on the Veterans Enterprise Management System (VEMS), of which the VetBiz Portal is the front door, applications (VetBiz Stat (Goals Management, Predictive Analytics and Market Research system), Forecast of Opportunities (FCO), Event Management Software as a Service (EMSS), 2268 Next Generation and any other system added to the OSDBU IT portfolio during the period of performance.

To accomplish this effort, the Contractor shall achieve full operational capability to support the requirements outlined below:

1. The Contractor shall provide technical support to enable OSDBU federal staff to evaluate and scrutinize all ongoing and planned projects, develop the OSDBU Portfolio Assessment Framework, and develop an updated Portfolio Assessment Framework.
2. The Contractor shall assess processes against proven practices (e.g., Veteran-focused Integration Process (VIP), Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMI), Agile Development Operations and other industry best practices).
3. The Contractor shall recommend improvements in processes and practices for managing the IT investment portfolio that serves as a foundation for a roadmap to OSDBU's success.
4. The Contractor shall provide technical support to enable OSDBU federal staff to develop a framework for recommending and communicating process changes, resource management, and value delivery.
5. The Contractor shall Identify strengths and weaknesses with the current tools and provide recommendations on the tools needed to support current and future business needs.

6. The Contractor shall Identify and assess organizational climate and major capabilities that must be in place to establish an OSDBU-wide IT Portfolio management framework.
7. The Contractor shall assess the current "as-is" state and recommend any required changes in a "to-be" state. This will be presented as the IT Portfolio As-Is and To-Be Assessment Report.
8. The Contractor shall provide a written report called the IT Portfolio Gap Analysis Report provides a recommended road map from the "to-be" state to the "as-is" state.
9. The Contractor shall develop a recommended IT Governance Strategy Support and Framework Report for approval by VA, ensuring IT efforts and resources are value-added and reflect best practices.
10. The Contractor shall provide technical support to enable OSDBU federal staff to develop and maintain a catalog of OSDBU web services, Service Level Agreements, service Artifacts, Service Descriptions, and a Service Registry.
11. The Contractor shall identify core services that are consistently required on OSDBU systems and document options for how these could be combined in a core services package that all current and future systems leverage to create an economy of scale for all IT activity.
12. The Contractor shall manage change request prioritization and incorporation into current/future development cycles using a change control register.
13. The Contractor shall utilize Azure Dev Ops (ADO) to manage backlog and provide a scrum master to manage the sprint process.
14. The Contractor shall provide technical support and develop and maintain Standard Operating procedures.

Deliverables:

- A. Written Corrective Actions Recommendations Report
- B. Impact Analysis Report
- C. IT Portfolio As-Is and To-Be Assessment Report
- D. IT Portfolio Gap Analysis Report
- E. IT Governance Strategy Support and Framework Report
- F. Change Control Register
- G. Standard Operating Procedures
- H. Monthly ADO Task Report by contract CLIN
- I. Technical Support
- J. Identify Core Services

5.3 BUSINESS PROCESS RE-ENGINEERING SUPPORT

To support Federal staff Business Process Re-engineering (BPR) efforts, the Contractor shall interpret complex information and support federal staff in producing engaging visualizations, defining functionality, and producing flowcharts, wireframes, and templates of the OSDBU information system, VEMS and the OSDBU SharePoint sites.

This technical support includes creating test cases for change management vetting, to-be process maps to support the evaluation of recommendations, root cause analysis reports to document emergent issues and make recommendations for changes, gap analysis reports to document the gaps or deficiencies between the current and desired state, conceptual models to provide visual representation of system design and ad-hoc reports to support process management.

The Contractor shall use Azure Development Ops, Jira, and Trello. The Contractor shall use Microsoft Teams, Cisco WebEx, OSDBU Event Management System and any other widely used video teleconferencing tool. The Contractor shall provide application and business planning, analysis, requirements, application design, testing, maintenance, and validation support for OSDBU's programmatic, administrative, business intelligence, and strategic business Applications.

The Contractor shall liaise with OSDBU directorates and ITSI to achieve full operational capability to support the requirements outlined below:

1. The Contractor shall create the information architecture and proposing interaction designs (both site maps and page-level wireframes) for Portals, websites and mobile applications.
2. The Contractor shall support business process modeling through research and analysis.
3. The Contractor shall review all documents on VEMS/VetBiz and OSDBU SharePoint (VIP, VetBiz Stat, FCO, EMSS, 2268NextGen and any other system added to the OSDBU IT portfolio during the period of performance.) and identify areas of improvement, analysis of current processes, data management, data quality assurance, and system testing.
4. The Contractor shall document recommendations on areas of improvement with To-Be Process Maps.
5. The Contractor shall provide a gap analysis report to assess the differences in performance between the system's current state and the recommended future state.
6. The Contractor shall document processes utilizing conceptual models.
7. The Contractor shall support implementation of system changes by providing test cases for use in User Acceptance Testing.
8. The Contractor shall participate in weekly Business Process Modeling sessions for at least five major projects per year, acting as a subject matter expert in sketch sessions.
9. The Contractor shall support process management and create ad-hoc reports to document recommendations and findings.
10. The Contractor shall perform analysis during cyclical processes.
11. The Contractor shall participate in root cause analysis to recommend product enhancements or other appropriate actions to improve productivity for the business units and ITSI.

Deliverables:

- A. Test Cases
- B. To-Be Process Maps
- C. Root Cause Analysis Report
- D. Gap Analysis Report
- E. Conceptual Models
- F. Ad-hoc Reports
- G. Flowcharts
- H. Wireframes
- I. Templates
- J. Attend Weekly Meetings
- K. Document processes

5.4 ACCREDITATION & AUTHORIZATION (A&A) ARTIFACTS

The Contractor shall maintain all existing A&A artifacts for the VEMS/VetBiz system and develop additional artifacts required to support modification or enhancements to the systems as required by VA Handbook 6500. The contractor shall develop all A&A document artifacts required to achieve an ATO for VEMS/VetBiz, VetBiz Stat, FCO, EMSS, 2268NextGen and any other system added to the OSDBU IT portfolio during the period of performance.

The Contractor shall work with VA personnel to facilitate the successful maintenance of the A&A process for OSDBU systems throughout the PoP. The Contractor shall establish a standardized process, set of activities, general task descriptions, and a management structure to verify, validate, implement, and maintain the security and privacy posture of the OSDBU system portfolio. The Contractor shall work through the completion of the A&A process to obtain an Authorization to Operate (ATO).

To accomplish this effort, the Contractor shall:

1. The Contractor shall establish a structured, repeatable, OSDBU-focused A&A process.
2. The Contractor shall Be Certified using Enterprise Mission Assurance Support Service (eMASS).
3. The Contractor shall utilize eMASS as the repository for all accreditation & authorization (A&A) artifacts.
4. The Contractor shall Liaise with VA OIT Information Security and Privacy Personnel to ensure OSDBU follows the most recent guidance.
5. The Contractor shall review all existing A&A artifacts to determine gaps and remedy non-compliance.
6. The Contractor shall develop a schedule documenting the critical tasks and key milestones for the A&A process.
7. The Contractor shall coordinate obtaining the required A&A designation for all OSDBU systems.

8. The Contractor shall develop and submit all required A&A document artifacts for VEMS and the VetBiz Portal (VIP, VetBiz Stat, FCO, EMSS, 2268NextGen) and any other system added to the OSDBU IT portfolio during the period of performance.

Deliverable:

- A. Accreditation & Authorization (A&A) Document Artifacts
- B. eMASS Reports and remediation plans
- C. Communicate with Stakeholders
- D. Review A&A artifacts
- E. Provide a Schedule of the A&A process

5.5 VEMS O&M SUPPORT AND SHAREPOINT SERVICE

The Contractor shall support OSDBU's existing systems, VEMS/VetBiz Portal and the OSDBU SharePoint portal, continuously improving collaboration, information communication, and operating efficiencies. The system portals are the primary platforms for OSDBU ITSI customers to access business services and directorate-specific functionality. The VEMS/VetBiz portal provides a single sign-on destination for Veteran entrepreneurs seeking business opportunities with the VA.

The Contractor shall support day-to-day site collections administration, site improvements, automated capabilities, metrics, and embedded performance tools to maximize self-service and efficiency. The Contractor shall create, test, and deploy solutions utilizing VA-maintained and hosted hardware and software resources including ASP.Net, C#, CRM D365, CSS, HTML, iDashboard, InfoPath, JavaScript, jQuery, Microsoft Azure SQL, Microsoft Forms, Microsoft Teams, Microsoft Visual Studio, North52, Power Apps, Power Query, PowerShell, PowerRest Power Pages, API, SharePoint Object model, SharePoint Online and the Microsoft Office Suite (Word, PowerPoint, VISIO, ACCESS and Excel).

The Government estimates an average of 15 monthly SharePoint support requests, including bug fixes, site requests, solution requests, permissions, and enhancements. The Government estimates an average of 115 monthly VEMS support requests, including bug fixes, site requests, solution requests, permissions, and enhancements. The Contractor shall provide detailed requirements for review and approval by the VA PM before the commencement of the design phase.

The Contractor shall meet the below service levels for the resolution of each trouble ticket received:

- a. Initial response due within 1 hour for critical- work stoppage (i.e., primary work functions lost with no workaround available);
- b. 4 hours for high-work degradation (i.e., some work functions lost with no workaround available);

- c. 8 hours for med-work degradation with a workaround available (i.e., some work functions are lost, but a temporary workaround is available);
- d. 24 hours for low-impact minimal work degradation (i.e., some work functions reduced with no workaround required);
- e. Follow-up responses will be due based on the needs of the issue.

To accomplish this effort, the Contractor shall achieve full operational capability to support the requirements outlined below:

1. The Contractor shall provide a Technical Analysis Report of all configuration changes and modifications necessary as a result of guidance provided by the ITSI Program Manager or to meet the needs to support system development and integration to enable OSDBU's business systems to meet mission requirements. Trouble Ticket Tracking Report shall be produced from CRM D365 or another trouble ticket tool provided by the Government. The trouble ticket tracking system shall be updated in accordance with the service level agreements cited above.
2. The Contractor shall maintain a generated log of all technical issues, including the progress of unresolved issues elevated to OIT or third-party providers. The Contractor shall prepare a weekly Trouble Ticket Tracking Report to show the status of all open and resolved tickets from the previous week. The report shall include a summary description of the issues being reported, the total number of issues reported year to date, and an estimate of when remaining open tickets shall be resolved.
3. The Contractor shall provide the accepted solution to issues.
4. The Contractor shall work directly with OSDBU directorates to define and meet their requirements through the development, implementation and sustainment of CRM D365 solutions as follows:
 - a. Monitor CRM D365 solution deployment across OSDBU;
 - b. Work with IT Project Managers and Analysts to design and develop CRM D365 solutions to address OSDBU business needs;
 - c. Research and analyze OSDBU CRM D365 procedural problems and provide recommendations for improvements and changes;
 - d. Identify opportunities and propose improvements to the CRM D365 environment to make the CRM D365 environment a more effective solution;
 - e. Provide OSDBU the appropriate CRM D365 solution design recommendations, develop business services infographics to enhance user experience, and incorporate information visualization based upon industry best practices;
 - f. Coordinate with Team Lead and OSDBU directors in standardizing and optimizing the way data/information is stored, secured, shared, and retrieved;

- g. Provide post-installation support, configuration, security, operation, and maintenance of CRM D365, equipment, and software related to CRM D365;
 - h. Apply expert process innovation, guided by industry standards and lessons learned, for delivering process improvement that optimizes business functions;
 - i. Provide release management support to increase usability and solution longevity;
 - j. Synthesize complex or diverse information, collect and research data, and use experience to complement data, workflows, and procedures;
- 5. The Contractor shall work directly with clients to define and meet their requirements through the development, implementation, and sustainment of Power Apps/Power Pages solutions through:
 - a. Monitor Power Apps/Power Pages solution deployment across OSDBU;
 - b. Provide OSDBU the appropriate Power Apps/Power Pages solution design recommendations, develop business services infographics to enhance user experience, and incorporate information visualization based upon industry best practices;
 - c. Coordinate with the Team Lead and OSDBU directors in standardizing and optimizing the way data/information is stored, secured, shared, and retrieved;
 - d. Apply expert process innovation, guided by industry standards and lessons learned, for delivering process improvement that optimizes business functions;
 - e. Provide release management support to increase usability and solution longevity;
 - f. Synthesize complex or diverse information, collect and research data, and use experience to complement data, workflows, and procedures;
 - g. Work with IT Project Managers and Analysts to design and develop Power
 - i. Apps/Power Pages solutions to address OSDBU business needs;
 - h. Research and analyze OSDBU Power Apps/Power Pages procedural problems and provide recommendations for improvements and changes;
 - i. Identify opportunities and propose improvements to Power Apps/Power Pages to make the environment a more effective solution;
 - j. Configure applications on the VetBiz Portal to meet stakeholder requirements using the Microsoft Power Apps/Power Pages design tools and any other industry-standard software development kit (SDK);
 - k. Provide OSDBU the appropriate Power Apps/Power Pages solution design recommendations, develop business services infographics to enhance user experience, and incorporate information visualization based upon industry best practices;
 - l. Provide backup System Administrative support for information systems residents in the VetBiz Portal. Should become familiar with EMSS, VetBizStat, Forecast of Opportunities, 2268 Next Generation.

6. The Contractor shall work directly with clients to define and meet their requirements through the development, implementation and sustainment of OSDBU SharePoint solutions through:
- a. Monitor SharePoint Portal Server performance, user access and solution deployment across OSDBU;
 - b. Implement SharePoint across OSDBU; act as SharePoint Subject Matter Expert (SME). Participate in planning and execution of tasks related to the evaluation of new SharePoint-based initiatives, third-party solutions and Integration with additional Enterprise Systems;
 - c. Develop, configure, and maintain SharePoint processes to support OSDBU business processes. Perform typical system administrative activities such as site creation, backup, restore and issue resolution;
 - d. Migrate OSDBU's SharePoint to any future version approved by VA;
 - e. Work with IT Project Managers and Analysts to design and develop SharePoint solutions to address OSDBU business needs;
 - f. Research and analyze OSDBU SharePoint portal procedural problems and provide recommendations for improvements and changes;
 - g. Identify opportunities and propose changes to the SharePoint to make the SharePoint environment a more effective solution;
 - h. Maintain industry knowledge of publishing, collaboration, information management concepts, and best practices and procedures for SharePoint solutions.
 - i. Provide technical guidance to the team in the technologies related to the support of an Enterprise SharePoint environment (understanding integration with Active Directory, Structured Query Language (SQL), Customer Relationship Management (CRM) D365, Microsoft (MS) Office, etc.);
 - j. Configure SharePoint to meet stakeholder requirements using the Microsoft SharePoint Designer, Power Apps design tools and any other industry-standard software development kit (SDK)
 - k. Provide technical support of InfoPath forms and related workflows, including communicating the location of form libraries, their purpose and their ability to provide first and second-line issue resolution;
 - l. Coordinate with the Team Lead and OSDBU directors in standardizing and optimizing the way data/information is stored, secured, shared, and retrieved;
 - m. Provide post-installation support, configuration, security, operation, and maintenance of SharePoint online equipment and software related to SharePoint online;
 - n. Apply expert process innovation, guided by industry standards and lessons learned, for delivering process improvement that optimizes business functions;
 - o. Provide release management support to increase usability and solution longevity;

- p. Synthesize complex or diverse information, collect and research data, and use experience to complement data, workflows, and procedures;
- 7. The Contractor shall provide the COR/PM a weekly interactive status briefing slide deck that provides the status of each system. The weekly interactive status briefing slide deck should include specifics on bugs, fixes, changes, development and blockers.
- 8. The Contractor shall develop and maintain user help guides for VEMS/VetBiz (VIP, Engagement Management, Goals Management, Predictive Analytics and Market Research, Customer Service and 2268 Next Generation) and SharePoint.

Deliverables:

- A. Technical Analysis Report
- B. Trouble Ticket Tracking Report
- C. Resolution Report
- D. Weekly Interactive Status Briefing Slide Deck
- E. User Guides

5.6 DATA & SYSTEM INTEGRATION SUPPORT

The Contractor shall integrate third-party systems or Application Programming Interface/web-based data services into the OSDDBU VetBiz Portal to improve the accuracy, productivity, and efficiency of the Veterans Enterprise Management System (VEMS/VetBiz), as needed. The third-party systems include the VIP, VetBiz Stat, FCO, EMSS, 2268NextGen and any other system added to the OSDDBU IT portfolio during the performance period.

The Contractor shall attend interface working group meetings to coordinate with OSDDBU federal staff and other systems subject matter experts to ensure that all interface rules and data regarding interfaces between the external systems and VEMS are captured. The Contractor shall develop Interface Control Documents (ICDs) to interface with each of the systems listed above. Following approval of the ICDs, the Contractor shall update the System Architecture Diagram to depict new or updated interfaces.

For ICD projects, the following activities are required:

- 1. The Contractor shall provide support to OSDDBU federal staff that will enable them to define and document modeling guidelines such as recording assumptions, constraints, issues, approaches, documentation, templates, and notations.

2. The Contractor shall provide support to OSDDBU federal staff that will enable them to define the functional part(s) of the system being developed, external relationships, interaction with the user and other system elements.
3. The Contractor shall provide a Logical Specification Document - Define the system's internal logic, explaining how it operates.
4. The Contractor shall illustrate a Model underlying business as irrelevant to technology and provide a conceptual data model document.
5. The Contractor shall translate the conceptual model into a Logical Data Model Document that can be implemented by describing the data in as much detail as possible, without regard to how it may be physically implemented.
6. The Contractor shall provide a Physical Specification Document that specifies how to physically implement the logical design by specifying items such as tables, columns, and formal relationships between data and tables in a Physical Data Model.

Deliverables:

- A. Interface Control Document
- B. Logical Specification Document
- C. Conceptual Data Model Document
- D. Logical Data Model Document
- E. Physical Specification Document

5.7 MICROSOFT DYNAMICS CUSTOMER SERVICE RELATIONSHIP MANAGEMENT (CRM) ADMINISTRATION

The Contractor shall configure Microsoft Dynamics 365 CRM to meet OSDDBU business needs using predominantly out-of-the-box tools and techniques. Leverage Microsoft Dynamics 365 CRM to provide custom forms, interfaces, and dashboards to collect, analyze and manage workflows for Customer Service, Procurement Review Programs, Strategic Outreach Communications, Quality Assurance, Shared Services and other OSDDBU entities as required.

To accomplish this effort, the Contractor shall achieve full operational capability to support the requirements outlined below:

1. The Contractor shall design and customize solutions according to requirements using custom forms, views, entities, relationships, and JavaScript events.
2. The Contractor shall identify creative workarounds to meet requirements without developing custom code.
3. The Contractor shall design and integrate business process workflows in CRM D365.
4. The Contractor shall design and integrate business processes and data flows between CRM D365 and other applications.

5. The Contractor shall analyze and document network infrastructure, authentication, and security to support the CRM D365 and its integrated technologies.
6. The Contractor shall provide Deficiency Reports (DR) identifying MS Dynamics 365 CRM problems requiring documentation or programmatic changes.
7. The Contractor shall create or Customize Microsoft Dynamics 365 CRM Dashboards, which provide a collection of view lists, charts and iFrames that can display data from the CRM D365 database and pull in information from web services that can be modified to show key performance indicators and other important data. In real-time, the Custom Dashboards shall communicate useful business information from all CRM D365 developed solutions to OSDBU employees, Directors, Deputy Executive Director and Executive Director. The CRM D365 Customer Dashboards shall include but are not limited to, the following: Customer Service Dashboard, Procurement Review Dashboard, Strategic Outreach and Communications Dashboard, Quality Assurance Dashboard and Shared Services Dashboard.
8. The Contractor shall utilize Power BI or other designated data analytics tools to create and customize Dashboards, which provide data and charts that can display data from the CRM D365 database and pull in information from web services that can be modified to show key performance indicators and other important data. In real-time, the Dashboards shall communicate useful business information from all CRM D365-developed solutions to OSDBU employees, Directors, and Executive Directors. CRM D365 dashboard shall, but is not limited to, the following: Customer Service Dashboard, Procurement Review Dashboard, Strategic Outreach and Communications Dashboard, Quality Assurance Dashboard and Shared Services Dashboard.
9. The Contractor shall work closely with ITSI Business Process Re-engineer and other team members to provide Microsoft Dynamics 365 CRM subject matter expertise on all major projects requiring a Dynamics 365 CRM solution.
10. The Contractor shall generate or assist users in creating standard and Ad hoc MS Dynamics 365 CRM reports quickly and easily with charts, tables, and drill-through capabilities.
11. The Contractor shall develop training on any new functionality/CRM D365 solution.

Deliverables:

- A. Deficiency Report
- B. Custom Dashboards
- C. Integrated Workflows
- D. Standard/Ad hoc Reports
- E. Training materials
- F. Create creative workarounds
- G. Design Processes and Workflows
- H. Subject matter expertise
- I. Power BI
- J. Solutions

5.8 OSDBU WEB PORTAL OPERATIONS & MAINTENANCE

The Contractor shall operate and maintain all OSDBU web portals as the central access points for all OSDBU services and applications. The Contractor shall ensure the OSDBU web portals are operated and maintained in accordance with the service level agreements cited below.

The Contractor shall meet the below service levels for resolution of all web portal maintenance requirements:

Initial response due within 1 hour for critical- work stoppage (i.e., primary work functions lost with no workaround available)

- A. 4 hours for high-work degradation (i.e., some work functions lost with no workaround available)
- B. 8 hours for med-work degradation with a workaround available (i.e., some work functions lost, but a temporary workaround is available)
- C. 24 hours for low-impact minimal work degradation (i.e., some work functions reduced with no workaround required)
- D. Follow-up responses will be due based on the needs of the issue.

To accomplish this effort, the Contractor shall achieve full operational capability to support the requirements outlined below:

1. The Contractor shall analyze business processes to identify opportunities to apply Web/Portal technologies focused on OSDBU's customers and vendors.
2. The Contractor shall host design review sessions to identify areas for improving portal design, operations, and maintenance needs.
3. The Contractor shall analyze requests for application changes and provide a Systems Impact Plan that addresses the maintenance activities identified.
4. The Contractor shall provide ongoing portal support and maintenance to customers, business owners, end-users, and system administrators.
5. The Contractor shall provide recommendations and develop a close-out procedure for solutions when they have been determined inactive or obsolete.
6. The Contractor shall provide a weekly Recommended Improvements Report that delineates user and maintainer-requested changes, including recommendations and justification for future actions.
7. The Contractor shall provide an OSDBU Web Portal Operations & Maintenance Support Responsiveness Report that portrays the portal's uptime, downtime, and reason for downtime.
8. The Contractor shall maintain and update Training and User Guides for all OSDBU web portals and develop Standard Operating Procedures and Work Instructions for web portal access request procedures, content management procedures, and change request procedures.

9. The Contractor shall develop standard operating procedures and working instructions for OSDDBU staff and other stakeholders regarding OSDDBU web portal operations, maintenance procedures, reports, and recovery procedures.
10. The Contractor shall utilize OpenText TeamSite CC Professional or other VA-provided software to maintain the VA.gov internet and intranet portals.
11. The Contractor shall use 508 Compliance software to test and remediate IT accessibility issues on all OSDDBU Portals.

Deliverables:

- A. Systems Impact Plan
- B. Close-Out Procedure for Solutions
- C. Recommended Improvements Report
- D. 508 compliance remediation report
- E. OSDDBU Web Portal Operations & Maintenance Support Responsiveness Report
- F. Develop Standard Operating Procedures
- G. Maintain and Update Training User Guides
- H. Host Sessions
- I. Conduct Testing

5.9 MICROSOFT POWER AUTOMATE DEVELOPMENT

The Government requires a low-code development collaborator to provide automation and workflow development, with hands-on experience using Microsoft Power Automate. The low-code development collaborator will work closely with various stakeholders to understand their needs and create automated workflows that enhance business processes and reduce manual effort. The low-code development collaborator will build complex business solutions within the following areas of responsibility:

The Contractor shall perform the following:

1. The contractor shall create, configure, and maintain workflows using Microsoft Power Automate.
2. The contractor shall develop custom connectors, actions, and triggers in Microsoft Power Automate.
3. The contractor shall integrate Power Automate with other Microsoft services (e.g., SharePoint, Dynamics 365, Office 365) and third-party applications to include external Application Programming Interfaces (APIs).
4. The contractor shall work with stakeholders to identify automation opportunities and gather requirements.
5. The contractor shall analyze existing processes and recommend improvements through automation.
6. The contractor shall provide technical expertise and recommendations for implementing new workflows.
7. The contractor shall conduct thorough testing of automated workflows to ensure functionality and reliability.
8. The contractor shall troubleshoot and resolve issues with existing workflows.
9. The contractor shall continuously monitor and optimize workflows for performance and efficiency.
10. The contractor shall document all workflows, including design, development, and deployment processes.
11. The contractor shall provide training and support to end-users on using automated solutions.
12. The contractor shall create user guides and technical documentation for solutions developed.

Deliverable:

- A. Microsoft Power Automate Design and Development
- B. Microsoft Power Automate Collaboration and Requirements Gathering
- C. Microsoft Power Automate Testing and Maintenance
- D. Microsoft Power Automate Documentation and Training

5.10 MICROSOFT POWER APPS DEVELOPMENT

The Government requires a low-code development collaborator to provide digital automated processes, with hands-on experience using Microsoft Power Apps. The low-code development collaborator will work closely with various stakeholders to understand their needs and create custom apps that enhance business processes and reduce

manual effort. The low-code development collaborator will build rich business logic and workflow capabilities within the following areas of responsibility:

The Contractor shall perform the following:

1. The contractor shall develop canvas and model-driven apps using Microsoft PowerApps.
2. The contractor shall re-write and re-engineer custom legacy applications to Microsoft PowerApps solutions.
3. The contractor shall create, integrate, and maintain workflow connections to database sources in the underlying data platform within the Microsoft Dataverse and online and on-premises data sources (i.e. Microsoft Azure, SharePoint, Dynamics 365, Office 365, Structured Query Language (SQL) Server, Microsoft Power BI)
4. The contractor shall work with stakeholders to identify and form customized business logic client-side scripting using JavaScript when declarative business rules do not meet the governments requirements.
5. The contractor shall analyze and troubleshoot query performance and take corrective actions to solve issues in real time through end-to-end problem resolution.
6. The contractor shall create, test, and debug complex Transact-SQL (T-SQL) scripts, stored procedures, functions, and triggers to support application development.
7. The contractor shall implement the DevOps process and build-test-release pipelines.
8. The contractor shall develop, and maintain database objects, a data dictionary and ensure the quality and integrity of the databases.
9. The contractor shall identify, develop, and deploy reports in the underlying data platform within the Microsoft Dataverse (i.e. SQL Server, Microsoft Power BI).

Deliverable:

- A. Microsoft Power Apps Design and Development
- B. Microsoft Power Apps Collaboration and Requirements Gathering
- C. Microsoft Power Apps Testing and Maintenance
- D. Microsoft Power Apps Documentation and Training

5.11 MICROSOFT POWER BUSINESS INTELLIGENCE (BI) DEVELOPMENT

The Government requires a low-code development collaborator to provide visually appealing interactive reports and dashboards, with hands-on experience using Microsoft Power BI. The low-code development collaborator will work closely with various

stakeholders to understand their needs and drive analyses that enhance data-driven decision-making processes. The low-code development collaborator will build data transformation and modeling capabilities within the following areas of responsibility.

1. The contractor shall design, develop, implement, and support Business Intelligence solutions, including reports, dashboards, and templates for self-service BI.
2. The contractor shall provide performance optimization in Microsoft Power BI to include complex data modeling, and Data Analysis Expressions (DAX) scripting.
3. The contractor shall create, integrate, and maintain workflow connections to unrelated database sources in the underlying data platform within the Microsoft Dataverse and online and on-premises data sources (i.e. Microsoft Azure, Excel, SharePoint, Dynamics 365, Office 365, Structured Query Language (SQL) Server, APIs, Microsoft Power BI).
4. The contractor shall conduct data acquisition using Power Query for data transformation and preparation.
5. The contractor shall create and maintain SQL queries for data analysis.
6. The contractor shall collaborate with stakeholders to gather requirements and translate business needs into effective visualizations.
7. The contractor shall create and manage end-to-end Power BI projects, from requirements gathering to deployment.
8. The contractor shall develop the semantic layers for the Microsoft Power BI tools utilized by the organization.
9. The contractor shall consume and create interactive reports utilizing Power BI Service features, including sharing, collaboration, and administration.
10. The contractor shall ensure data accuracy, consistency, and integrity within Microsoft Power BI solutions.

Deliverable:

- A. Microsoft Power BI Design and Development
- B. Microsoft Power BI Collaboration and Requirements Gathering
- C. Microsoft Power BI Testing and Maintenance
- D. Microsoft Power BI Documentation and Training

5.12 TRANSITION SUPPORT (OPTIONAL TASK)

The Contractor shall provide a Transition Plan for 60 days of outgoing transition support for transitioning all tasks required in the PWS of the current contract to a follow-on contract/order or Government entity. This transition may be to a Government entity or another Contractor. The plan shall include formal coordination with Government staff, successor staff, and management. The plan shall also include the delivery of copies of

existing policies and procedures and the delivery of required metrics and statistics. This Transition Plan shall consist of, but is not limited to:

1. Coordination with Government representatives;
2. Review, evaluation, and transition of current testing services;
3. The transition of historical data to the new Contractor system;
4. Transfer of all necessary business and technical documentation;
5. Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes;
6. Disposition of Contractor purchased Government-owned assets (if applicable);
7. Transfer of Government Furnished Equipment (GFE) and Government Furnished;
8. Information (GFI) and GFE inventory management assistance;
9. The Contractor strategy regarding personnel staffing and training during the transition period;
10. Data and workflow process;
11. Any templates used in day-to-day operations

In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this contract to a successful provider. The government may exercise this optional task at any time during the base or option performance periods.

Deliverable:

- A. Transition Plan

6.0 GENERAL REQUIREMENTS

6.1 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none">1. Shows understanding of requirements2. Efficient and effective in meeting requirements<ol style="list-style-type: none">a. All CPMP sections are updated monthly	Satisfactory or higher

	<ul style="list-style-type: none"> b. 100% of all Online Help Guides are approved five business days prior to release <p>3. Meets technical needs and mission requirements</p> <ul style="list-style-type: none"> a. 100% of A&A artifacts are completed b. 98% of all Tier 2 and 3 incoming calls shall be answered within 1 hour c. 90% of all Tier 2 trouble ticket calls are resolved in the same business day d. Process model charts include 95% of the actual process e. Completes 95% of sustainment requirements within prescribed timeframes. <p>4. Provides quality services/products that do not require rework after delivery.</p> <p>5. Incorporates "ease of use" human-centered design principles in any software developed.</p>	
B. Project Milestones and Schedule	<p>1. Quick response capability</p> <ul style="list-style-type: none"> a. Initial response to 100% of trouble tickets and web portal maintenance requirements due within 1 hour for critical work stoppage b. 4 hours for high-work degradation c. 8 hours for med-work degradation with workaround availability 	Satisfactory or higher

	<ul style="list-style-type: none">d. 24 hours for low-impact minimal work degradatione. Follow-up responses will be due based on the needs of the issue <p>2. Products completed, reviewed, and delivered in accordance with the established schedule</p> <ul style="list-style-type: none">a. All CPMP's are delivered on scheduleb. All Weekly Status Reports are delivered on schedulec. 100% of A&A Artifacts are delivered on scheduled. Deficiency Reports completed on schedulee. Architecture Documents are completed and delivered on timef. 100% of Interface Design Documents are completed and delivered on timeg. 100% of Updated Architecture Documents are complete and delivered on timeh. Process Model Charts and Model Outputs are delivered on timei. All required training completed, and certificates of	
--	---	--

	<p>completion submitted to the COR on schedule</p> <p>2. Notifies customer in advance of potential problems</p>	
C. Cost & Staffing	<p>1. Currency of expertise and staffing levels appropriate</p> <p>2. Personnel possess the necessary knowledge, skills and abilities to perform tasks</p>	Satisfactory or higher
D. Management	<p>1. Integration and coordination of all activities to execute the effort</p>	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the contract's life to ensure that the Contractor performs the services this PWS requires at an acceptable level. The Government reserves the right to alter or change the QASP at its discretion. The COR will use a Performance Based Service Assessment in accordance with the QASP to assess Contractor performance.

6.2 ENTERPRISE AND IT FRAMEWORK

The required Assurance Levels for this specific contract are Identity Assurance Level (IAL) 3, Authenticator Assurance Level (AAL) 3, and Federation Assurance Level (FAL) 3, in reference to the Federal Identity, Credential, and Access Management (FICAM) requirements.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 10 (64bit), Edge (Chromium based), and 365 Apps for enterprise. Applications delivered to VA and intended to be deployed to Windows 10 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using Microsoft Endpoint Configuration Manager (CM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the client operating system being used.

6.3 ORGANIZATIONAL CONFLICT OF INTEREST

All functions related to Acquisition Support shall be on an advisory basis only. Please be advised that since the awardee of this Contract will provide systems engineering, technical direction, specifications, work statements, and evaluation services, some restrictions on the awardee's future activities may be required in accordance with FAR 9.5. As appropriate, the Contractor and its employees shall be required to sign Non-Disclosure Agreements (Appendix A).

6.3.1 PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL). The PAL scope includes the full spectrum of OIT functions and activities, such as VIP project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT workforce, Government and Contractor personnel. The Contractor shall follow the PAL processes to ensure compliance with policies and regulations and to meet VA quality standards. The PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at

https://www.va.gov/PROCESS/artifacts/maps/process_CONB_ext.pdf. The main PAL can be accessed at www.va.gov/process.

6.3.2 AUTHORITATIVE DATA SOURCES

The VA Enterprise Architecture Repository (VEAR) is one component within the overall EA that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department's Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below. The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA's Master Person Index (MPI) (formerly the Master Veteran Index (MVI)) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor and vendor, and solicitation information above the micro-purchase threshold, if the solution relies

on procurement data. ECMS is the authoritative source for VA procurement actions data.

4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with Vet360 to access personal contact information, if the solution relies on VA Veteran personal contact information data. Vet360 is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying active-duty military service data. VADIR is the authoritative source for Qualifying Active-Duty military service in VA.

6.3.3 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity, and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

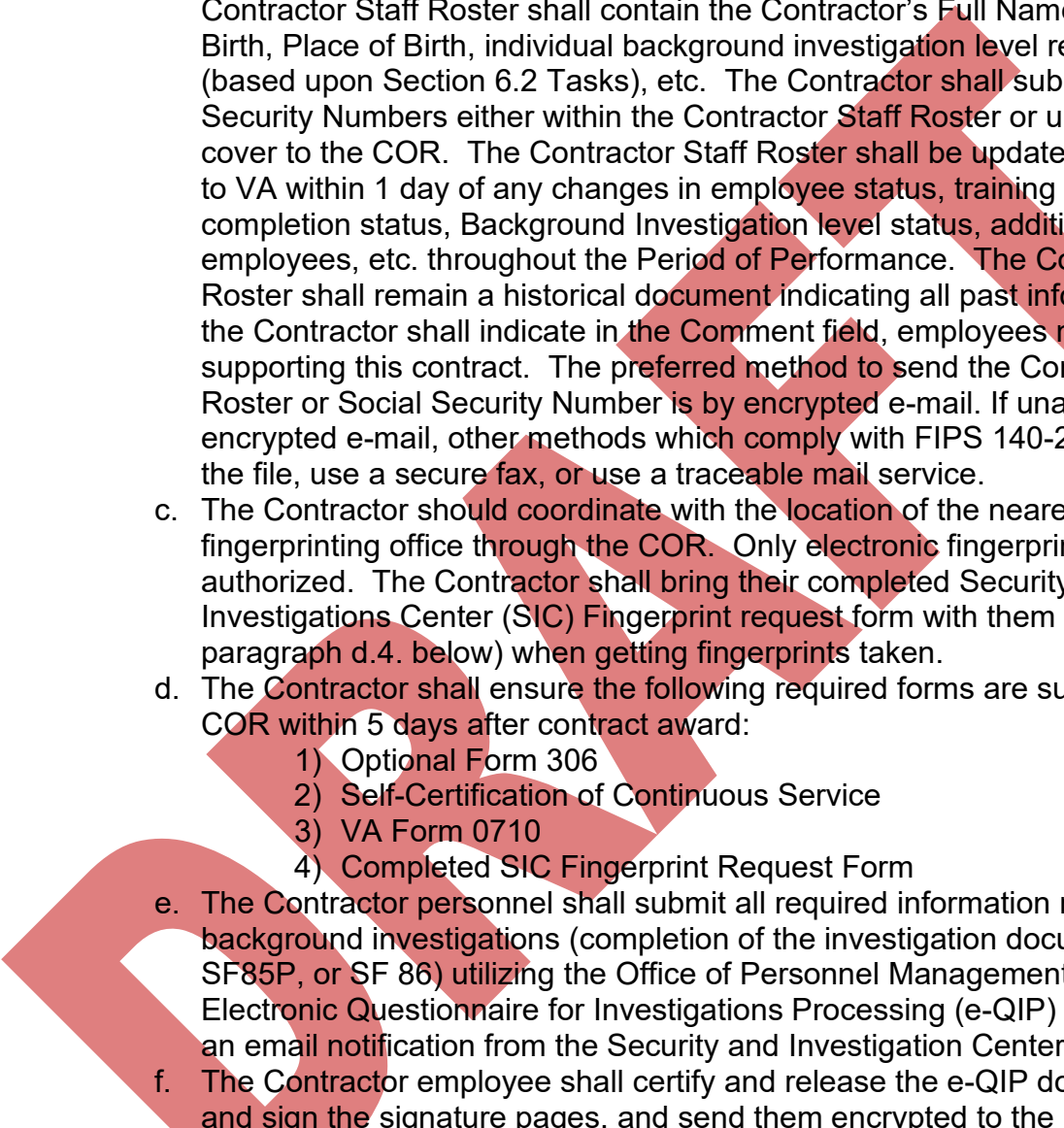
Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.3.4 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

- 
- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
 - b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
 - c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
 - d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) Optional Form 306
 - 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed SIC Fingerprint Request Form
 - e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
 - f. The Contractor employee shall certify and release the e-QIP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
 - g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this

contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

- h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
- i. 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.
- j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
- k. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

- A. Contractor Staff Roster

6.4 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: Microsoft 365, MS Word 2000/2003/2007/2010/2019, MS Excel 2000/2003/2007/2010/2019, MS PowerPoint 2000/2003/2007/2010/2019, MS Project 2000/2003/2007/2010/2019, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010/2019, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and

program documentation for the project and other Government applications will also be provided on an as-needed basis.

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

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print, or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, documents, and requirements repositories, etc. as required for the development, storage, maintenance, and delivery of products within the scope of this effort. The Contractor shall not transmit, store, or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, 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 PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to

**ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and
ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM
SECURITY/PRIVACY LANGUAGE.**

6.6 GOVERNMENT FURNISHED PROPERTY

The Government has multiple remote access solutions available to include Citrix Access Gateway (CAG), Site-to-Site Virtual Private Network (VPN), and RESCUE VPN.

The Government's issuance of Government Furnished Equipment (GFE) is limited to Contractor personnel requiring direct access to the network to: development environments; install, configure and run Technical Reference Model (TRM) approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner); upload/download/ manipulate code, run scripts, and apply patches; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

When necessary, the Government will furnish desktops or laptops, for use by the Contractor to access VA networks, systems, or applications to meet the requirements of this PWS. The overarching goal is to determine the most cost-effective approach to providing needed access to the VA environment coupled with the need to ensure proper Change Management principles are followed. Contractor personnel shall adhere to all VA system access requirements for on-site and remote users in accordance with VA standards, local security regulations, policies, and rules of behavior. GFE shall be approved by the COR and Program Manager on a case-by-case basis prior to issuance.

Based upon the Government assessment of remote access solutions and requirements of this effort, the Government estimates that the following GFE will be required by this effort:

A. 8-10 laptops

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra Personal Identity Verification card readers, peripheral devices, or additional Random Access Memory (RAM). The Contractor is responsible for providing these types of IT accessories in support of this effort as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

Additionally, the Contractor shall provide a status of all reportable GFE as part of the Monthly this report, reportable GFE includes equipment that is furnished by the Government as tangible "personal" property which the Contractor takes possession of, physically leaves a Government facility, and needs to be returned the end of Contractor performance. The following information shall be provided for each piece of GFE:

1. Name of Contractor employee assigned to the GFE

2. Type of Equipment (Make and Model)
3. Tracking Number/Serial Number
4. VA Bar Code
5. Location
6. Value
7. Total Value of Equipment
8. Anticipated Transfer Date to Government
9. Anticipated Transfer Location

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

Not Applicable

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 and continuous monitoring.

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, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, 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 VA Handbook 6500.6, "Contract Security," March 12, 2010, 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. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS) 2.0, and will be

tracked therein. The TMS 2.0 may be accessed at

<https://www.tms.va.gov/SecureAuth35/>
<https://www.tms.va.gov/SecureAuth35/>

- If you do not have a TMS 2.0 profile, go to and click on the "Create New User" link on the TMS 2.0 to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with 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). 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): https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1056&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1055&FType=2

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

On January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. 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.

A3.1. 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: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>. A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is available from the Access Board: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule>.

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

A3.2. Compatibility 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.

A3.3. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the 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.

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 always wear visible identification while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

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 CO 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 CO 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 CO.
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.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

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

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work

on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

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

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

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractor/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification

by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

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

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Directive 1605.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above-mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 10 and future versions, as required.

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

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

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying assigned to the individual.

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than 60 days.

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

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting

compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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

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

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and

Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

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

f. VA prohibits the installation and use of personally owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

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

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

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

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

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

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

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for

the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

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

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

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
 - a) date of occurrence;
 - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;
- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- 8) Known misuses of data containing sensitive personal information, if any;
- 9) Assessment of the potential harm to the affected individuals;

- 10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
- 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

- 1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior, relating to access to VA information and information systems;

- 2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS 2.0 # VA 10176) and complete this required privacy and information security training annually;
- 3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

- a. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.
- b. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete. The Contractor shall report completion of the following training requirements or equivalent:

Course Number	Course Name	Required Participants	Frequency
1357076	Information Security and Privacy Role-Based Training for System Administrators (WBT)	Required for Elevated privileges for personnel performing System Administrator duties.	Before elevated privileges are approved and then annually
1016925	Information Security and Privacy Role-Based Training for Software Developers (WBT)	Required for Elevated privileges for personnel performing Software Developer duties.	Before elevated privileges are approved and then annually
1357083	Information Security and Privacy Role-Based Training for Network Administrators (WBT)	Required for Elevated privileges for personnel performing Network Administrator duties.	Before elevated privileges are approved and then annually
3867205	Elevated Privileges for System Access (WBT)	Required for Elevated privileges for all personnel.	Before elevated privileges are approved and then annually
4563250	PKI Certificate Management – Overview (On Demand)	Required for Elevated privileges for all personnel.	Before elevated privileges are approved and then annually

10203	Privacy and HIPAA Training	Required for all personnel.	Before a PIV is issued and then annually
10176	VA Privacy & Information Security Awareness and Rules of Behavior	Required for all personnel.	Before a PIV is issued and then annually
4192704	Records Management for Everyone (WBT)	Required for all personnel.	Before a PIV is issued and then annually

DRAFT