PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Financial Management Business Transformation (FMBT)
Technology Product Management

Date: 05/21/2025
TAC Number: VA-26-00002411
PWS Version Number: 0.2

Contents

1.0 BACKGROUND 5
1.1 Program Background 5
2.0 APPLICABLE DOCUMENTS 7
3.0 SCOPE OF WORK 10
4.0 PERFORMANCE DETAILS 11
4.1 PERFORMANCE PERIOD 11
4.2 PLACE OF PERFORMANCE 11
4.3 TRAVEL 12
5.0 SPECIFIC TASKS AND DELIVERABLES 12
5.1 PROJECT MANAGEMENT 12
5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN 13
5.1.2 KICKOFF MEETING 14
5.1.3 REPORTING REQUIREMENTS 15
5.1.3.1 Bi-Weekly Status Report 15
5.1.3.2 Staffing/Resource Plan 16
5.1.3.3 Weekly and Monthly Status Meetings 16
5.1.3.4 Monthly Program Management Review 17
5.1.3.5 Monthly COR Progress Report 18
5.1.3.6 Monthly Task Order Report 18
5.1.4 KEY PERSONNEL 19
5.1.5 QUALITY ASSURANCE AND QUALITY CONTROL 21
5.1.6 PRIVACY AND HIPAA TRAINING 23
5.1.7 ACTIVITY BASED COSTING 23
5.1.8 SCALED AGILE FRAMWORK 23
5.2 Product Support 24
5.2.1 Service Desk Support Incident and Service Request Support Tickets 24
5.2.1.1 Baseline Enhancements 26
5.2.2 Product and Baseline Enhancements 27
5.2.2.1 Enhancement Implementation (OPTIONAL) 28
5.2.3 Supplemental Service Management (Help Desk) Design (OPTIONAL) 28
5.2.4 Supplemental Tier 2 Support (OPTIONAL) 29
5.3 INFRASTRUCTURE OPERATIONS and Maintenance 29
5.3.1 OM Disaster Recovery Testing 29
5.3.2 Technical Operations/Administration 30
5.3.3 Maintenance Support 35
5.3.4 Findings and Vulnerabilities 35
5.3.5 Database Administration (OPTIONAL) 35
5.3.6 Database Patches and Upgrades (OPTIONAL) 38
5.4 operations and maintenance scaling support (optional) 38
5.4.1 Initial Scaling Support (OPTIONAL) 39
5.4.2 Mature Scaling Support (OPTIONAL) 39
5.5 Business Process Validation Sessions (OPTIONAL) 39
5.6 WAVE IMPLEMENTATION (OPTIONAL) 41
5.6.1 Integrated Project Schedule (OPTIONAL) 41

5.6.2 System Test Plan (OPTIONAL) 42
5.6.3 Wave Implementation Plan and Schedule (OPTIONAL) 42
5.6.4 Business Operations Planning, Concept of Operations (CONOPS) (OPTIONAL) 44
5.6.5 iFAMS Configuration 44
5.6.5.1 iFAMS ACS Configuration 44
5.6.5.2 ACS Testing (Optional) 44
5.6.5.3 Feeder System and Interface Support 45
5.6.5.4 Data Validation and Reconciliation (OPTIONAL) 46
5.6.5.5 Financial and Acquisition Management Segment Target State (OPTIONAL) 47
5.6.5.6 Treasury Financial Management 47
5.7 Post-Implementation Support (OPTIONAL) 48
5.8 Accounting Classification Structure (OPTIONAL) 49
5.8.1 ACS Element Mapping (OPTIONAL) 49
5.8.2 ACS Training (OPTIONAL) 50
5.8.3 ACS Timeline (OPTIONAL) 51
5.9 Training Support (OPTIONAL) 51
5.9.1 Training Support Plan 51
5.9.2 Training Development (OPTIONAL) 51
5.9.3 Training Execution (OPTIONAL) 54
5.9.4 Introduction to iFAMS Training Boot Camp (OPTIONAL) 57
5.9.5 O&M Training Development (OPTIONAL) 57
5.9.6 Sustainment Organizational Change Management Plan and Delivery (OPTIONAL) 58
5.9.7 Sustainment Training Delivery (OPTIONAL) 58
5.9.8 Transition Plan (OPTIONAL) 59
5.10 Parallel Activities (OPTIONAL) 59
5.11 Operations and Maintenance System Testing (OPTIONAL) 61
5.11.1 Operations and Maintenance Automated Testing Support (OPTIONAL) 62
5.12 Wave Testing (OPTIONAL) 63
5.12.1 Wave Test Plan 63
5.12.2 Wave System Testing and Test Reporting (OPTIONAL) 63
5.12.3 Wave Regression Testing (OPTIONAL) 64
5.12.4 Wave User Acceptance Testing (UAT) Support (OPTIONAL) 65
5.12.5 End-To-End/Production Simulation Testing (OPTIONAL) 65
5.12.6 Wave Automated Testing Support (OPTIONAL) 65
5.12.7 Wave Test Scripts/Cases (OPTIONAL) 66
5.12.8 Wave Test Management (OPTIONAL) 66
5.12.9 Wave Test Execution (OPTIONAL) 68
5.13 Independent Verification and Validation Review SUPPORT (OPTIONAL) 69
5.13.1 Independent Verification and Validation Support 69
5.13.1.1 Independent Verification and Validation Environment (OPTIONAL) 71
5.14 Business Intelligence (BI) Support (OPTIONAL) 71
5.14.1 Internal Momentum Reports 72
5.14.2 BI Project Management (OPTIONAL) 73

5.14.3 Data and Reporting Governance Support (OPTIONAL) 73
5.14.4 Data Estate and BI Development (OPTIONAL) 74
5.14.5 Data Estate and BI Operations and Maintenance (OPTIONAL) 75
5.14.6 Data Estate and BI Product Management (OPTIONAL) 75
5.14.7 Data Estate and BI Infrastructure Management (OPTIONAL) 76
5.14.8 Data Estate and BI Training (OPTIONAL) 77
5.15 Transition Support (Optional Task) 77
5.15.1 Outgoing Transition Management 77
5.15.2 Hosting Transition and Migration Planning (OPTIONAL) 78
5.15.3 Gap Planning and Analysis (OPTIONAL) 79
5.15.4 Migration and Startup (OPTIONAL) 79
5.16 Stakeholder Support (OPTIONAL) 81
6.0 GENERAL REQUIREMENTS *(pending)* 90
6.1 ENTERPRISE AND IT FRAMEWORK 90
6.1.1 VA TECHNICAL REFERENCE MODEL 90
6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 90
6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6) 92
6.1.4 TRUSTED INTERNET CONNECTION (TIC) 92
6.1.5 STANDARD COMPUTER CONFIGURATION 93
6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM) 93
6.1.7 PROCESS ASSET LIBRARY (PAL) 93
6.1.8 AUTHORITATIVE DATA SOURCES 94
6.1.9 SOCIAL SECURITY NUMBER (SSN) REDUCTION 95
6.1.10 SOFTWARE AND LICENSING REQUIREMENTS 95
6.2 SECURITY AND PRIVACY REQUIREMENTS 95
6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 95
6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 96
6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 98
6.4 PERFORMANCE METRICS 98
6.5 FACILITY/RESOURCE PROVISIONS 99
6.6 GOVERNMENT FURNISHED PROPERTY 101
6.7 SHIPMENT OF HARDWARE OR EQUIPMENT 102
ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED <*DRAFT TBD*> **Error! Bookmark not defined.**
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE ..... **Error! Bookmark not defined.**

1.0 BACKGROUND

1.1 PROGRAM BACKGROUND

The Department of Veteran Affairs (VA) has considered the replacement of its aging financial system architecture since 1999. Two major efforts were initiated and subsequently canceled: the Core Financial and Logistics System (CoreFLS) in 2004 and the Financial and Logistics Integrated Technology Enterprise (FLITE) in 2010. The cancellation of these programs led to the proliferation of system workarounds and the development of add-on systems. This resulted in a fragmented financial system environment noted in VA financial statement audits as noncompliant with the Federal Financial Management Improvement Act of 1996 (FFMIA) and the Federal Managers Financial Integrity Act of 1982 (FMFIA).

On March 25, 2013, the Office of Management and Budget (OMB) issued Memorandum 13-08, *Improving Financial Systems through Shared Services*, directing all executive agencies to use a shared services solution for future modernizations of core accounting or mixed systems. VA then established the Financial Management Business Transformation (FMBT) program in accordance with OMB's directive.

During the system selection process, both of the potential enterprise resource planning (ERP) solutions considered by VA were integrated financial and acquisition management systems. VA has never had integration between those two systems and determined that the seamless integration of finance and acquisition offered by the ERP solutions was not only an industry best practice but would also provide enormous benefit to both the finance and acquisition communities. Accordingly, the integration of VA's financial and acquisition systems became a fundamental principle of the Financial Management Business Transformation (FMBT) Program.

To achieve the FMBT initiative's goal of modernizing VA's financial and acquisition management systems, the Office of Management (OM) is leveraging the Financial Services Center's (FSC) deep expertise in deploying Department-wide transformation efforts and relies on the center to be the system owner and long-term provider for VA. Collectively, federal staff from the FMBT program, alongside staff from FSC, oversee implementation and sustainment of the system.

The implementation of the system is strongly supported by Program Advisors (PAs) and Subject Matter Experts (SMEs) from across VA Administrations and Staff Offices and is closely partnered with the Office of Information and Technology (OIT) and the Office of Acquisition, Logistics, and Construction (OALC).

VA is migrating to the Momentum cloud solution, configured for VA as Integrated Financial and Acquisition Management System (iFAMS) and hosted in the VA Azure cloud. VA is gaining increased operational efficiency, productivity, agility, and flexibility

from a modern enterprise resource planning (ERP) cloud solution. The new system also provides additional security, storage, and scalability.

The FMBT program vision is to provide VA with a modern financial and acquisition management solution with transformative business processes and capabilities that enable VA to meet its goals and objectives in compliance with financial management legislation and directives. This financial and acquisition system modernization effort is increasing the transparency, accuracy, timeliness, and reliability of financial information, resulting in improved fiscal accountability to American taxpayers. iFAMS offers a significant opportunity to improve services to those who serve Veterans. The FMBT program is transforming the VA finance and acquisition business, enabling Administration and Staff Office employees to prioritize mission delivery.

The FMBT program is increasing the transparency, accuracy, timeliness, and reliability of financial and acquisition information across VA, resulting in improved fiscal accountability to American taxpayers and increased opportunity to improve services to those who serve Veterans.

The FMBT Program Goals are structured to enable VA to continue to meet its financial, acquisition and mission-related delivery requirements, alleviate the risks caused by the current system environment, and provide value to VA's business and the employee experience. The FMBT Program Goals are as follows:

- Implement a Modern System: Implement a modern, secure financial management and acquisition system hosted in the VA Azure cloud
- Standardize Processes: Standardize and automate business processes and transactions to promote operational efficiency and scalability
- Strengthen Compliance: Enhance VA's ability to meet federal regulations, strengthen financial process and internal controls, and mitigate long-standing audit deficiencies
- Provide Timely, Consistent and Robust Information: Enhance planning, analysis, and decision-making capabilities by improving data integrity, reporting capabilities, and business intelligence
- Focus on Mission Execution: Redirect resources toward mission-critical work from financial, acquisition, and administrative work to better serve those who serve Veterans

The purpose of this Performance Work Statement (PWS) is to detail the tasks required to implement and maintain iFAMS within the VA. These tasks include Project Management Support, System Support, Operations and Maintenance (O&M) Support, Implementation Support, and Transition Support. VA employs a Development, Security, and Operations (DevSecOps) methodology and Scaled Agile Framework (SAFe) practices focused on bringing about business value through continuous delivery and improvement. The requirements identified in this PWS are intended to provide business requirements, development, testing, deployment, and security and operations support for iFAMS.

2.0 APPLICABLE DOCUMENTS

(DRAFT)

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

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 FMBT program is migrating VA’s current financial management and acquisition environment to the new Integrated Financial and Acquisition Management System (iFAMS) utilizing the COTS Momentum Enterprise Suite, ERP solution through an incremental deployment approach. Each deployment, referred to as a “wave,” will deliver capabilities to a subset of the VA organization. The scope of each wave will define the VA organization, funds, Momentum functionality, business intelligence, data, legacy systems, and reports.

Each wave implemented will require distinct Project Management Support, Hosting Environment and Managed Services Support, Implementation Support, and Transition Support for the deployment of the outstanding waves and then continued O&M support to FSC, for previously implemented waves.

The Contractor shall support the development, configuration, and deployment of each wave implemented as part of this contract. The contractor shall continue to support the production configuration of iFAMS and its interfaces to support all implemented waves in operation and maintenance for the term of this contract. This support includes all requirements, configuration, development, testing, integration, architecture (with concurrence from FMBT and FSC architecture), refactoring as needed, and all ongoing planned and unplanned operations and maintenance support to include predictive, preventative, corrective, perfective, adaptive, and evolutionary through a cycle of Continuous Integration. Support of the production configuration and interfaces includes enhancements necessary to integrate with other modernization efforts and their systems to include but not limited to, Electronic Health Record Modernization (EHRM) and VA Logistics Redesign (VALOR).

VA employs a Development, Security, and Operations (DevSecOps) methodology and Scaled Agile Framework (SAFe) practices focused on bringing about business value through continuous delivery and improvement. The requirements identified in this PWS are intended to provide business requirements elicitation, configuration, development, testing, deployment, and security and operations support for iFAMS.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be 12 months from date of award, with up to five (5) 12-month option periods and fifty (50) optional tasks, to be exercised at the Government's discretion.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). If required, the CO may designate the Contractor to work during holidays and weekends.

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	November 11
Christmas Day	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	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at both Government and Contractor facilities and work may be performed at remote locations with prior approval of the Contracting Officer's Representative (COR).
It is anticipated that the majority of work under this PWS shall be performed at Contractor facilities. The Contractor facilities in Washington DC Metropolitan Area shall be Metro accessible and shall be used for collaboration, meetings, and training. The Contractor principals and key personnel shall be located within local travel distance of VA facilities in Washington DC and Austin, Texas, since face-to-face meetings with Government decision makers will be required.

VA anticipates face-to-face meetings in Washington DC and Austin, Texas. VA may provide a limited number of seats in support of** the work performed in this contract at the **Government facility in Austin, Texas. Temporary Duty (TDY) to a** government **facility within the effort does not change the Place of Performance to the Government Site.

4.3 TRAVEL

The Government anticipates travel under this effort to support the breadth of program management activities relating to FMBT planning, initiation, deployment, and sustainment, as well as to attend program-related meetings through the PoP.

Travel is on a cost reimbursable, no fee basis and shall be in accordance with the Federal Travel Regulations (FTR) and requires advance concurrence by the Contracting Officer Representative (COR). The Contractor shall provide cost estimates with each travel request to the COR. Each Contractor invoice must include copies of all requested, applicable, and required receipts (FTR §301-11.25: required for lodging, regardless of amount, and a receipt for every authorized expense over $75) that support the travel costs claimed in the invoice.

Contractor travel within the local commuting area of 50-miles will not be reimbursed. Travel performed for personal convenience and daily travel to and from work at the Contractor's facility will not be reimbursed. Contractor travel within the local commuting area will not be reimbursed.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

The Contractor shall plan, govern, coordinate, execute, and report on all tasks and activities performed under this TO. The Contractor shall provide management, ensure compliance, measure performance, and report on all activities through to delivery.

Project Management for all development and implementation activities shall utilize the Project Management Institute (PMI) standards or equivalent. Annual Software Maintenance and O&M support shall be based on the Software Engineering Institute's (SEI's) Software Maintenance Maturity Model (SMmm or S3M) or equivalent.

Consequently, the Contractor shall establish milestones for each task against which progress shall be monitored, measured, and evaluated. These milestones must be related to distinct and measurable products with specific outcomes. Each task shall be

subdivided into discrete work elements according to a structured top-down approach that emphasizes the relationship of work elements to each other and to the overall task. The discrete work elements shall be the basis for progress reporting and for financial monitoring and control of the project.

Project Management activities for Base and Optional Tasks should be tracked and billed against that particular activity so that optional task project management is only included when and if an optional task is exercised.

Requirements contained within this Task Order requires coordination with several different resources which may be Government personnel or other Contractors. Duties will be performed through collaboration with all parties. Proper chain of command and roles and responsibilities shall be established, documented, and maintained to work effectively in this type of environment.

Coordination shall take place in writing through formal processes such as team working agreements, status reports and participation in project meetings and informal processes while working side by side. The Contractor shall work effectively with all contractors supporting FMBT.

Any configuration decisions that affect the Enterprise Configuration discussed in informal processes (examples include working side by side, or in office hours meeting) will be documented and presented in formal change control process for approval.

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor Project Management Plan (CPMP) task involves the management and oversight of all activities performed by Contractor personnel, including sub-Contractors, to satisfy the requirements identified in this PWS. The Contractor shall identify a Program Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this contract. The VA shall retain overall Program Management Responsibility. The Contractor shall operate and coordinate within the FMBT Program Management Office. The Contractor's Program and Project Managers shall coordinate their efforts with VA Program and Project Managers.

The Contractor shall deliver a 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 Contractor shall describe in the CPMP the organizational resources, and management controls the Contractor shall employ to meet the support, schedule, quality, and performance requirements defined in this PWS. The Government will use this CPMP to manage, track, and evaluate the Contractor's performance. The VA PM will approve the Contractor's baseline CPMP prior to execution. The VA PM will approve any updates to the CPMP that the Contractor prepares.

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

5.1.2 KICKOFF MEETING

The Contractor shall conduct a Kickoff meeting within five (5) calendar days after award to introduce the Government team, including but not limited to the COR and CO, to the Contractor's Project Leadership Team and present the Contractor's overall operating plans and approach for this effort. At the meeting, the Contractor shall present a Staffing and Quality plan, overall CPMP, and high-level schedule, at the task order level. Two (2) days prior to the Kick-off Meeting, the Contractor shall submit to the government an agenda, location, and virtual option of the meeting for COR approval. The Contractor's Staffing Plan and milestones shall address all aspects of onboarding personnel required to access VA information or networks. The Contractor shall provide the meeting minutes two (2) days after the Kick-off Meeting.

During the kickoff-meeting, the Contractor shall present, via Microsoft Office PowerPoint, the following:

- A high-level management intended approach that addresses the scope, resources, project assumptions, constraints, task objectives, key milestones, Contractor's project organization and Contract administration, delivery schedule, and deliverables
- A high-level work plan for all activities, by month
- Contractor's high-level approach, schedule, and Agile methodology for the during the task order period of performance
- Contractor's high-level operating plan and approach, containing methodology to address risks, security, staffing/ resource issues including any sub-contractors.
- Identification of Key Personnel as well as a Responsible, Accountable, Consulted, and Informed (RACI), and discuss Staffing/Resource Planning.

5.1.3 REPORTING REQUIREMENTS

5.1.3.1 Bi-Weekly Status Report

The Contractor shall provide the COR and PM with Biweekly (every two weeks) Status Reports in electronic form per Government designated format and media. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall provide accurate, timely, and complete project information supporting FMBT Reporting Requirements and reflect data as of the last day of the preceding Biweekly report.

The Biweekly Status Report shall include the following data elements for each product Task Order (TO) supported:

a. TO Name
b. Overview and description of the TO
c. Overall high-level assessment of TO progress
d. Product Increment (PI) and Sprint including upcoming future releases being reported on including date and a brief summary of releases planned within next 30 days.
e. All Work In-Progress (WIP) vs work in-progress limit (as defined by SAFe) and completed during the reporting period
f. Identification of any TO related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
g. Explanations for any unresolved issues, including workable solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
h. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation
i. Work planned for the subsequent four (4) reporting periods, when applicable Current TO schedule overlaid on original TO schedule showing any delays or advancement in schedule
j. Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. After the initial labor baseline is provided and approved, each report shall identify any changes in staffing identifying each person who was added to the TO or removed from the TO. The report shall include the replacement personnel's resumes that include education level and other information as to replacement personnel's qualification in general.
k. Training Certificates, after initial and updated certificates are provided, each report shall identify any changes for all Contractor personnel including the dates of expiration and the due date for the next time due

l. A Government Furnished Equipment (GFE) Report for all equipment issued to Contractor personnel performing on the effort during the current reporting period including a record of transfer of any GFE. The report shall include up-to-date information on the physical location of the GFE and to whom the GFE is assigned.
m. Original schedule of deliverables and the corresponding deliverables made during the current reporting period.

Deliverable:

A. Bi-Weekly Progress Status Report

5.1.3.2 Staffing/Resource Plan

The Contractor shall deliver a Staffing/Resource Plan to the Government for approval. The Staffing/Resource Plan shall include an analysis of current and projected resource needs to meet the system requirements for performance, product quality, and security. The Contractor shall identify any known technology resource requirements and provide the materials that are needed to support the task order. The Contractor shall identify, secure, and utilize the minimum levels of staff, with optimal skill sets, that are required to support the complete iFAMS ecosystem. This includes Momentum, the iFAMS enterprise service bus (ESB), iFAMS-EZ, and business intelligence and reporting platform and content. The Staffing/Resource Plan shall include an analysis of current and projected resource needs to meet the system requirements for performance, product quality, and security.

Deliverable:

A. Staffing/Resource Plan

5.1.3.3 Weekly and Monthly Status Meetings

Weekly status meetings shall be scheduled by the Contractor to address progress, planned activities, risks, or conflicts that may impact the schedule, scope, or cost and any change management impacts. Weekly status meetings will also include the status on the development and implementation and Operations and Maintenance efforts.

The Government and the Contractor PM shall jointly chair weekly status meetings, and these will be attended by the Contractor and Government team leads. Tasks and sub-tasks will be discussed at this meeting, with agreed upon delivery dates. The meetings shall schedule and present risks, risk status, and risk mitigation strategies.

The first weekly status meeting of the month will become a monthly status meeting where the Contractor shall discuss major schedule and project accomplishments during the prior month, Performance metrics, and risk mitigation strategies and efforts.

The Contractor shall attend and support Change Control Board (CCB) meetings on a weekly basis. The Contractor shall present the status of the tasks closed during the prior week, tasks scheduled to be worked on during the current week, and the following week, impediments.

In addition, ad-hoc meetings, executive briefings, and demonstrations may be requested by the Government on an as-needed basis.

The Contractor shall produce agendas at least twenty-four (24) hours before scheduled meetings and meeting minutes no later than two (2) business days following the meeting.

In conjunction with the weekly status meetings, the Contractor shall prepare and distribute a weekly Status Report that documents the activities and achievements in the prior week and the planned activities, milestones, deliverables due, and meetings for the following week.

Deliverable:

A. Weekly Status Meeting

5.1.3.4 Monthly Program Management Review

The Contractor shall prepare a Monthly Program Management Review (PMR), to be distributed on the first weekly status meeting of the month that documents the activities and achievements in the prior month and the planned activities, milestones, and deliverables due for the following month. The PMR report shall document any problems or unresolved issues that may impact the triple constraint (scope, schedule, and cost).

The Contractor shall prepare and deliver a PMR Report in VA format provided in Attachment A. The PMR Report shall outline primary activities conducted by the Contractor for each reporting period. The PMR Report shall measure the Contractor's cost and schedule performance using either the Government-approved WBS or a separate arrangement as mutually agreed upon by the Government and the Contractor. It shall also include but not be limited to the following:

- Activities completed in reporting period
- Identified risks and mitigation of risks
- Any Government action needed
- Monthly Performance Metrics
- iFAMS System Availability

- Performance Baseline
- GFE inventory implemented
- Projected GFE requirements
- Lessons learned
- Current licenses: Licenses used for development and testing shall be annotated separately from those used in Production

The Contractor shall require all sub-contractors to provide input to the PMR Report where there are critical or significant tasks related to the prime contract, if applicable. The Government will update the PMR template based on business needs and reporting requirements. All changes to the PMR templates will be communicated by the Government to the contractor one reporting period prior to the change.

5.1.3.5 Monthly COR Progress Report

The Contractor shall provide the COR with Monthly COR Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding month.

The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status (see section A 3.0). 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. Monthly COR Progress Report

5.1.3.6 Monthly Task Order Report

The Contractor shall provide to the Government's designated personnel a Monthly FMBT Task Order report in accordance with the format specified by the government. The Monthly Task Order Report shall include a list of Contractor personnel supporting each Time and Material (T&M) task and the supporting activities for each Contractor personnel, as well as the impact to the T&M budget. The Monthly Task Order Report shall comply with Activity Based Costing Labor Tracking methodology per PWS section 5.1.7.

Deliverable:

A. Monthly Task Order Report

5.1.4 KEY PERSONNEL

FMBT uses Agile approach for the operations of the program. Agile principles and scrum practices will be applied to complete FMBT work where appropriate.

Program Manager:
The Contractor Program Manager shall be responsible for managing the overall performance, quality, schedule, and cost for the contract. Among other responsibilities, the Program Manager shall support the FMBT Program in executing the systems integration activities. The Program Manager shall have successful experience in implementing a large complex Momentum based financial and acquisition management cloud-based solution for a Cabinet Level Agency. The Program Manager shall have extensive experience with agile and traditional project management methodologies. The Program Manager shall have experience including finance, acquisitions, and technology. The Program Manager shall hold current agile certification and project management professional certifications. The Program Manager should have at minimum:

- Active PMP certification
- Experience managing a large program at VA.
- 15 years' experience in areas related to finance, acquisition, and technology.
- Experience leading a large financial and acquisition Momentum implementation.

Deputy Program Manager:
The Contractor Deputy Program Manager shall be responsible for supporting the Program Manager in managing the overall performance, quality, schedule, and cost for the contract. Among other responsibilities, the Deputy Program Manager shall support the FMBT Program Office in executing their program management activities, planning the Department's transition to the iFAMS solution, preparing for governance process reviews, and assisting with communications across the capabilities of the iFAMS solution. The Deputy Program Manager shall have successful experience in implementing a large complex financial and acquisition management cloud-based solution for a Cabinet Level Agency. The Program Manager shall have extensive experience with agile and traditional project management methodologies. The Deputy Program Manager shall have experience including finance, acquisitions, and technology. The Deputy Program Manager shall hold current agile certification and project management professional certifications. The Deputy Program Manager should have at minimum:

- Active PMP certification
- Experience managing a large program at VA.

- 15 years' experience in areas related to finance, acquisition, and technology
- Experience leading a large financial and acquisition Momentum implementation.

The Contractor key personnel for Program Manager and Deputy Program Manager shall have prior experience in large-scale financial management business transformation, SaaS delivery model adoption, shared service implementation including customer and provider side implementation, and large-scale program integration. The Contractor shall provide the titles, and a description of the duties of key personnel to be assigned to these tasks. The Contractor shall submit a resume for each key person. Each resume shall provide information with respect to:

1. Subject matter expertise and knowledge of financial management and acquisition business transformations.
2. Expert knowledge on SaaS delivery model adoption.
3. Demonstrated project management expertise on similar complex Federal Department-wide financial and acquisition system implementations.
4. Demonstrated experience and expertise, including certification when applicable for all FMBT tools in support of the Knowledge Management efforts (reference Section 5.2.2.3).
5. Subject matter expertise in Momentum is required.

Momentum Technical SMEs:
The Contractor shall provide Momentum Technical Subject Matter Experts as key personnel. The Contractor SMEs resume shall include:

1. Experience implementing in a financial and acquisition management system for a Cabinet Level Agency;
2. Experience providing technical direction and guidance in the performance of analysis, requirements development, and implementation of Momentum;
3. Experience making recommendations on system improvements in the following specialties as they pertain to Momentum: information systems architecture, networking, automation, security, communications, software life-cycle management, modeling and simulation;
4. Experience providing technical, managerial, or administrative direction for functional domains related to IT systems and projects.

The Contractor shall provide resumes for any Key Personnel positions identified above. All submitted resumes are to be redacted to prevent disclosure of personally identifiable information (PII). Examples of PII include but are not limited to names, addresses, phone numbers, social security numbers, and birthdays/dates. For those individuals proposed as Key Personnel who are not current employees of your company, a signed a Letter of Intent will be required. The Key Personnel positions and redacted resumes of individuals who shall fill the Key Personnel positions shall be included as an attachment to the contract/order in Section D upon award.

Letters of Commitment: The Offeror shall provide written Letters of Commitment signed by the individuals concerned that are included in the Offeror's proposal as Key

Personnel. The Letters of Commitment shall indicate, at a minimum, that each individual proposed as Key Personnel was contacted after the issue date of the solicitation, that each proposed individual has consented to the submission of their Letter of Commitment by the Offeror with its proposal, and that each individual has confirmed that he/she is available for order performance. Offerors are advised that in the event it may become necessary to replace any of the proposed Key Personnel prior to and/or during the course of contract performance, the Offeror must, prior to conducting the replacement, provide the cognizant Contracting Officer with assurances that the agency will receive replacements with equal or better qualifications as compared to those Key Personnel being replaced.

During the first 90 calendar days of performance, the Contractor shall not replace or substitute Key Personnel who the Contractor proposed pre-award unless the replacement is necessitated by illness, death, or termination of employment. The Contractor shall notify the Contracting Officer within 15 calendar days after the occurrence of any of these events and provide a detailed explanation of the circumstances necessitating the proposed substitution and shall demonstrate that the proposed replacement personnel are of at least substantially equal ability and qualifications as the individual originally proposed for that position. The proposed replacement personnel shall be approved by the CO or COR prior to final determination.

After the initial 90 calendar days, any personnel the Contractor offers as substitutes for the above identified key personnel positions shall have the ability and qualifications equal to or better than the key personnel which are being replaced and shall meet or exceed the qualifications designated for that Key Personnel position. If any change to a key personnel position becomes necessary, the Contractor shall immediately notify the VA PM and COR in writing, but whenever possible Contractor shall notify the VA PM of substitutions in personnel in writing 30 calendar days prior to making any change in key personnel, and provide a detailed explanation of the circumstances necessitating the proposed substitution and shall demonstrate that the proposed replacement personnel are of at least substantially equal ability and qualifications as the individual originally proposed for that position and that the proposed replacement meets or exceeds the qualifications designated for that Key Personnel position.

The Contractor agrees that it 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. Failure to replace a Key Personnel pursuant to this clause and without a break in performance of the labor category at issue shall be considered a condition endangering contract performance and may provide grounds for default termination.

5.1.5 QUALITY ASSURANCE AND QUALITY CONTROL

The Contractor shall deliver an update to the Quality Assurance and Quality Control (QA/QC) Plan to the Government for approval and implement a QA/QC program which

establishes, implements, and maintains QA/QC as it relates to technical quality for deliverables, work products, and services performed under this task order.

The QA/QC Plan shall document the Contractor's QA/QC process, which will meet and comply with quality standards established in this PWS and are compliant with ISO 9001/IEC 90003 and include a monitoring and controls process.

The QA/QC Program shall address all requirements within the PWS and incorporate all processes required to develop, document, monitor, review, analyze, and conduct the Contractor's execution of the PWS It shall ensure that all developed application software and associated materials meet accepted industry standards, best practices for quality, and Federal Financial Management System requirements as detailed in OMB Circular A-127, Financial Management Systems. It shall ensure adherence to the performance measures specified in the Performance Requirements Summary (PRS) defined in the task order a Quality Assurance and Surveillance Plan (QASP). The Government will use this QASP to measure Contractor performance against the metrics defined in this PWS.

Consistent with QA/QC plan, the QA/QC program shall include management and technical reviews and audits to validate the quality of the work performed by the Contractor's personnel and of the work performed by its sub-contractors. Management and technical reviews and audits will be performed by personnel/sub-contractors not directly responsible for the work performed.

The Contractor shall maintain records documenting all corrective actions and process improvements undertaken during contract performance. The records shall validate the Contractor's compliance with the processes contained in the QA/QC plan. The Contractor shall make the records available to the Government during contract performance.

The Government has the right to perform periodic surveillance of the Contractor to assure that the Contractor's work products and QA processes are in compliance with the contract requirements, including performing root cause analysis on specific problems and/or issues.

Deliverable:

A. QA/QC Plan
B. Monthly Updates to QA/QC Plan

5.1.6 PRIVACY AND HIPAA TRAINING

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task. The status reporting shall identify; a single Contractor Security Point of Contract, the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. This information shall be submitted as part of the Weekly/ Progress Status Report.

The Contractor shall submit Talent Management System (TMS) training certificates of completion for VA Privacy and Information Security Awareness training. The Contractor shall also provide VA Privacy and Information Security Awareness Signed Rules of Behavior, and VA Health Insurance Portability and Accountability Act (HIPAA) Certificate of Completion in accordance with Section 9, Training, from Appendix C ofthe VA Handbook 6500.6, “Contract Security”.

Deliverable:

A. TMS Training Certificates of Completion for VA Privacy and Information Security Awareness Training
B. Privacy and Information Security Awareness Signed Rules of Behavior
C. VA HIPAA Certificate of Completion

5.1.7 ACTIVITY BASED COSTING

The Contractor shall comply with Activity Based Costing (ABC) Labor Tracking. ABC Labor Tracking is used as a driver quantity to assign resource cost to activities and activity cost to products and services within the organization. The quantities from ABC Labor Tracking makes activity cost visible throughout the organization, incentivizes cost reduction, increases precision of overhead allocation, and enables informed pricing decisions.

5.1.8 SCALED AGILE FRAMWORK

The Contractor shall use the existing FMBT Scaled Agile Framework and make recommendations for improvement based on lessons learned to the Government for approval. The objective of the Scaled Agile Framework is to provide a governing set of Agile best practices critical to the successful implementation of iFAMS in alignment with the Department of Veterans Affairs Digital Transformation Strategy. These key practices have been defined, at a high level, to enable the FMBT program and FSC to satisfy GAO and OIG audit requirements.

iFAMS Agile teams are expected to adhere to FMBT Scaled Agile Framework practices and work with the Government Agile Council for advice, strategy, and feedback to improve agile practices and backlog management.

Contractor will also be responsible for:

- Managing agile release trains following FMBT SAFe principles and practices
- Create, coordinate and lead, with VA team and agile release trains, backlog of technical and business aligned requirements utilizing FMBT EAP/Agility tool and following FMBT/iFAMS Agility guidance and standards.
- Continuous backlog refinement, prioritization, implementation, and monitoring/reporting of backlog at every stage of program lifecycle with VA team and agile release trains
- Assessing and reporting backlog metrics and health and data integrity checks through continuous backlog monitoring following FMBT/iFAMS Agility guidance and standards.
- Coordination with project scheduling team to track agile epics and features in the Integrated Project Schedule
- Supporting and participating in Agile Council meetings, Agile/Agility Community of Practice, program retrospectives, lessons learned and continuous process improvement efforts.

Deliverable:

A. FMBT Scaled Agile Framework Updates
B. Backlog
C. Backlog health metrics and data integrity checks

5.2 PRODUCT SUPPORT

The Contractor shall be responsible for the sustainment of the Momentum application, including baseline integrations, through support of the Program's Incident, Problem, and Change Control processes; the performance of regular maintenance activity, including configuration control, patch testing and deployment; and by advising Program leadership on future enhancements aligned to the published Momentum product roadmap.

5.2.1 Service Desk Support Incident and Service Request Support Tickets

Aligned with the Program's Incident and Problem Management processes, the Contractor shall address all Momentum-related concerns, in accordance with the government's prioritization of related tickets. This activity may include triaging and Incident validation; Root Cause Analysis (RCA), identification, execution and unit testing of remediations or work-arounds; coordination with government and other contractors, deployment of appropriate solutions through the Program's Change Control processes, and timely documentation of all steps taken in the appropriate ticketing system or registry. Unless explicit permission is granted by the government, the Contractor shall complete all relevant documentation by the close of business of the full resolution of the

Incident. Support for critical Incidents ("Break Fixes") requiring immediate action, as determined by the government, shall be provided by the Contractor 24 hours/day, seven days/week, 365 days/year. This support shall be provided:

- Less than one-hour response at the "engineer level" response (not just a service desk trouble ticket entry)
- Ongoing communication with government-designated PoCs on regular intervals not to exceed one hour to provide status updates and next steps
- Ongoing coordination with the government and other supporting Contractors, including the Momentum system vendor, as appropriate to fully restore service and communicate to users and other stakeholders
- Four-hour response time for dispatches, and eight-hour time-to-repair for critical severity issues
- Documentation in the appropriate registry of the incident, the Contractor's steps to resolve it, and, when appropriate, the steps the Contractor will take to mitigate future related risks

The government will dictate the expected turnaround time for these activities related to all other Incidents not deemed 'critical'. When appropriate, the Contractor shall recommend fixes for the Momentum product that will address Known Errors (derived from Problem Management), Risks (derived from Incidents or proactive monitoring), or other sources for the government to potentially escalate to the Momentum system vendor for future Momentum Product baselines.

- Less than one-hour response at the "engineer level" response (not just a service desk trouble ticket entry)
- Ongoing communication with government-designated PoCs on regular intervals not to exceed one hour to provide status updates and next steps
- Ongoing coordination with the government and other supporting Contractors, including the Momentum system vendor, as appropriate to fully restore service and communicate to users and other stakeholders
- Four-hour response time for dispatches, and eight-hour time-to-repair for critical severity issues
- Documentation in the appropriate registry of the incident, the Contractor's steps to resolve it, and, when appropriate, the steps the Contractor will take to mitigate future related risks

The Government will dictate the expected turnaround time for these activities related to all other Incidents not deemed 'critical'. When appropriate, the Contractor shall recommend fixes for the Momentum product that will address Known Errors (derived from Problem Management), Risks (derived from Incidents or proactive monitoring), or other sources for the government to potentially escalate to the Momentum system vendor for future Momentum Product baselines.

The Contractor shall recommend fixes for the Momentum product that will address Known Errors (derived from Problem Management), Risks (derived from Incidents or proactive monitoring), or other sources for the government to potentially escalate to the Momentum system vendor for future Momentum Product baselines.

The Contractor will either provide defect resolution or provide VA a manual workaround to minimize disruption to VA operations. Once the Contractor provides a workaround that accepted by the Government, the Contractor shall document the workaround, coordinate with other Contractors to communicate the workaround steps to appropriate stakeholders, and close out the Incident, transferring the Known Error to the Problem Management process with appropriate documentation to support later understanding, including history of the error, attempted/recommended remediation steps, and known level of effort compared to the workaround, and prioritization.

The Contractor shall provide vendor management for those vendors that are providing direct support to Momentum components. The Contractor shall track, analyze, and resolve customer issues including the ability to directly access Momentum Product Development resources and the Momentum defect repository. The Contractor shall provide a Weekly Report indicating ticket workload broken out by tier.

Metric Description	Metric Standard
Baseline bug defects: system design flaws or software coding errors that are resolved with Momentum Baseline changes.	• 95% of baseline tickets resolved or a VA approved work-around implemented within 23 calendar days from receipt by Momentum baseline team. • 95% of workarounds will have a permanent solution implemented within 6 months from receipt by Momentum baseline team.

The Contractor shall produce a Monthly Product Baseline Report demonstrating the time to resolve baseline tickets including delivery of workaround and final ticket resolution.

Deliverable:

A. Weekly Product Baseline Defect Report
B. Monthly Product Baseline Report

5.2.1.1 Baseline Enhancements

The Contractor shall provide support for baseline enhancements for the Momentum product. The Contractor shall assess the request and provide VA with the prioritization of enhancements along with the level of effort required.

Deliverable:

A. Weekly Product Baseline Enhancement Report

5.2.2 Product and Baseline Enhancements

Enhancements are proposed changes to improve product performance, address new or changed business needs, or otherwise modify the application unrelated to any documented Incident or Problem. Enhancements may reflect changes to the baseline Momentum product ("baseline enhancements," which are developed and deployed by the Momentum system vendor) or changes to the iFAMS-specific configuration of the product ("product enhancements," which are developed and deployed under this contract). The Contractor shall receive direction from the government for enhancements and is expected to proactively recommend product performance improvements. Once a possible enhancement is identified the Contractor shall perform deeper analysis into the value and level of effort of any enhancements at the direction of the Government. The

For any iFAMS enhancement that is requested, the Contractor shall conduct the following:

- Initial Requirements supporting the development of the requested enhancement
- Coordination with the government and other vendors to prepare a business case/justification for the enhancement
- Assessment of published Momentum product roadmap documents to validate whether the enhancement is already planned within a future release
- Coordination with the government and other vendors to identify enhancement paths as alternatives to modifications to the Momentum product
- Initial development of wireframe and process flows to demonstrate the enhancement.
- Development of a Level of Effort including the estimated hours and proposed timeline required to complete the development of the enhancement including:
    - Development of any changes to the VA implemented version of Momentum (iFAMS) that the Government requests the functionality to be available.
    - Full testing to ensure no bugs are introduced into the VA implemented version of Momentum (iFAMS)
    - Implementation of the enhancement into the Government requested VA implemented version of Momentum (iFAMS)
    - Testing of the enhancement during the next VA implemented version of Momentum (iFAMS).
- For Baseline Enhancements, participate with the government in discussions with the Momentum product vendor
- Provide supporting documentation aligned with the above steps

The Contractor shall track the status of product and baseline enhancements, if known and report status to the Government within the Monthly PMR Report IAW PWS section 5.1.3.4. The enhancements shall include, but not limited to:

- Enhancement to the VA Momentum (iFAMS) instance
- Enhancement to the Momentum underway or planned by the Momentum product vendor (vendor status)
- Enhancement to the next selected VA Momentum (iFAMS) upgrade

Deliverables:

A. Monthly Enhancement Report to the PMR

5.2.2.1 Enhancement Implementation (OPTIONAL)

Upon Government approval, the Contractor shall execute the enhancements in the Monthly Enhancement Report. The Contractor shall ensure that enhancements are delivered within budget, and on time. The Contractor shall execute all enhancements through the Program's Operations and Management Build and Release Process.

Upon the government's direction, the Contractor will begin development of product enhancements or begin review of baseline enhancements received from the Momentum system vendor. Upon completion of development (product enhancement) or receipt (baseline enhancement) the Contractor shall conduct unit testing of the enhancement and implement the enhancement into the VA instance of Momentum (iFAMS) utilizing the standard O&M build and release process.

Anytime enhancements are implemented all related processes and documentation shall also be updated, and the updated documentation provided to the Government. The documents updated shall include, but not limited to:

- System Design Document
- Network Topology Diagram
- Interface Control Document
- Table and Code Documentation
- Updated Data Dictionaries
- Updated Knowledge-based Help Desk Documents
- Release notes to support training documentation updates
- Updated Training Documentation

Deliverables:

A. Updates to Enhancement Documentation

5.2.3 Supplemental Service Management (Help Desk) Design (OPTIONAL)

The Contractor shall provide managed services to support the successful operation of the financial and acquisition management ecosystems hosting environment including, license management, incident management, disaster recovery, Tier 3 help desk support, and documentation services. Prior to the go-live date for each wave, the Contractor shall provide a service management approach that complies with the Service

Desk Integrated Conceptual Design and Roadmap and shall provide the following details:

- Hours of operation
- Escalation management
- Resolution management
- Tool necessary to track all service requests, change requests and incidents

Roles and responsibilities

5.2.4 Supplemental Tier 2 Support (OPTIONAL)

The Contractor shall support resolution of Tier 2 tickets. Including but not limited to: Security administration issues

- iFAMS reference table updates
- User security issues
- iFAMS transactional error handling
- Policy questions
- General inquiries from users
- Coordination with interface stakeholders
- SQL extracts
- VA infrastructure-related issues
- Other issues related to the iFAMS Product that Tier 1 Support is unable to resolve

Metric Description	Metric Standard
Inquiries: Customer issues submitted through VA approved ticketing solution with non-system impact responses	• 95% of inquiry tickets will be returned to VA with a recommended resolution within 3 business days of Contractor receipt.

5.3 INFRASTRUCTURE OPERATIONS AND MAINTENANCE

5.3.1 OM Disaster Recovery Testing

The Contractor shall conform to requirements set forth in NIST 800-34.

The Contractor shall provide backup and recovery support as identified. The Contractor shall provide a DR Test Report each year to include root cause analysis on issues and recommendations for the following and/or improving responses to disasters.

The Contractor shall perform a six-month rotating DR/Failover exercise between two different physical sites along with a Report summarizing the results of the exercise and identifying areas for improvement.

- Revamp DR procedure to full cutover to complementary environment every 6 months, running all environments for 6 months in each complimentary environment
- Coordinate all DR activity with FSC and all impacted VA affiliated organizations
- Identify accreditation boundary between our infrastructure and Azure
- Snapshots of VMs at a determined frequency (applicable to individual systems).
- Identify appropriate storage mediums and implement backup plans customized to the business requirements of the information owner
- Active Directory
    - AD objects (groups, OUs, users, permissions, security policies, etc.)

Deliverable:

A. Disaster Recovery Test Report
B. DR Exercise Report

5.3.2 Technical Operations/Administration

The Contractor shall provide technical administration and maintenance support for The VA's databases, servers, and networks. The Contractor shall:

- Meet the required availability requirements for single components. The Contractor must notify the VA when restoring loss of service from single component failures that could result in customer impacts.
- The Contractor shall propose designs and implement at the direction of the VA
- Provide preventative maintenance services and troubleshoot each physical and virtual server and any associated software or hardware to ensure all servers and associated components that comprise VA-FSC IT Infrastructure are operational.
- Uptime computation excludes scheduled, pre-agreed outages and outages caused by VA other accreditation boundaries to include both application and infrastructure boundaries. No data points will be filtered

on uptime calculations. Downtime will be annotated for communications such as partial available and/or maintenance, etc.

- Configure similar/like components load-balancing/load-sharing/dual-routing
- Design all production hardware, software, and network components for high availability, minimizing single points of failure where necessary to meet applicable SLRs. The Contractor shall propose architectural changes toward an increasing high-availability model by request or annual.
- The Contractor shall evaluate architecture alternatives at the request of the VA.
- Configure components for automatic failover where load-balancing/load-sharing/dual-routing is not possible
- Monitor and report all facility, hardware, software, and network components for failure and clearly defined performance parameters
    - Define partial outages and report on them
        - Customer experience/impact
        - Interface handling and its influence on up time
        - Need to discuss component outages and their relative importance
- No data points will be filtered out
- Include ALL downtimes (including planned and unplanned maintenance windows, outages, slowdowns, etc.)
- Downtimes outside of a pre-approved maintenance window must include a root cause report
- Develop and maintain standard baseline configuration documentation or “build- books”
- Identify VA’s hardening standards
- Ensure that all installed product version levels are in compliance with the TRM

The Contractor shall operate and maintain the data network infrastructure by providing full engineering lifecycle support including:

- House the appropriate VA-owned network hardware (switch and routers) to provide wide area network (WAN) connectivity to VA private network users
- Provide user access to VA resources via The VA backbone network only. Per VA policy, Internet traffic to and from the data center facility will be routed by The VA’s Internet Gateways unless otherwise approved
- Support virtual private network (VPN) tunnels

- Ensure there are no single points of failure in the WAN/LAN architecture unless otherwise approved
- Help resolve or respond to network issues or trouble calls from The VA WAN network operations center and security operations center
- Provide protected external communication for Contractor personnel to access VA resources by configured and monitored stateful and application-layer firewalls and network intrusion/prevention systems and/or VPN connections with two-factor authentication mechanisms, and must be approved
- Provide change management and configuration support for Internet Protocol (IP) address and domain name system (DNS) name changes required as part of a network request change in support of The VA's infrastructure

The Contractor (and their network service provider[s]) must adhere to The VA's guidelines and security policy for network connectivity. Changes made on the Contractor site(s) must be coordinated and approved by The VA prior to implementation.

The Contractor shall provide technical, administrative, and operational support services for server management infrastructure supporting the full lifecycle of server deployment, operations, and applications systems across the hosted environment. The scope of this lifecycle support includes but is not limited to:

- Establish and maintain configuration and system parameters across like server environments, in conformance with established OIT security and configuration baselines/benchmarks.
- Execute processes for maintenance and functioning of tiered architecture systems (e.g., load balancing, tuning, configuration management, etc.)
- Execute authorized change requests
- Execute software/hardware maintenance, upgrade, refresh, as required, to maintain operation and meet SLRs
- Maintain non-sizing and non-platform specific presentation tier parameters and system settings across development, test, and production environments
- Implement and administer management tools to achieve monitoring capability of critical functions across all server instances operating in their respective zones
- Patch all software as needed according to VA policy
- Provide system software configuration, installation, and maintenance
- Provide deployment, testing, operation of software, development, test, and production servers

- Provide program and documentation support required to ensure systems are operating in compliance with applicable industry, VA, and agency requirements/standards
- Provide explanation, risk assessments, waivers/exceptions to VA standards for consideration of approval by the AO for all systems not in compliance
- Provide application software deployment as needed
- The Contractor shall also provide the following monitoring services:
- Develop, update, and document monitoring procedures that meet organization requirements and adhere to defined policies
- Provide console operations for centralized and remote CPU
- Provide console monitoring, troubleshooting, repair, and escalation of problems in the data center computing environment
- Provide preventative measures for monitoring and self-healing capabilities to limit outages that impact service delivery
- Monitor systems and respond to system messages
- Identify and report application problems
- Resolve or assist in resolving application problems. Escalate as required
- Support applications development-to-test-to-production migration activities The Contractor shall provide tier administration services in support of tier software services. Tiers include Presentation (Apache), Application (WebLogic), Middleware (Tuxedo), integration (webMethods or other), and Business Intelligence. Multi-tier administration also includes Secure FTP services.
- Support applications development-to-test-to-production migration activities

The Contractor shall provide tier administration services in support of tier software services. Tiers include Presentation (Apache), Application (WebLogic), Middleware (Tuxedo), integration (webMethods or other), and Business Intelligence (BI). The Contractor shall provide the following tier administration services:

- Install presentation, application, middleware, business intelligence and integration tier software and configurations required to support Momentum requirements
- Create, alter, and delete presentation, application, middleware, business intelligence, and integration tier objects
- Establish and maintain configuration and system parameters across like server environments
- Execute processes for the maintenance and functioning of tier services (e.g., cluster/load balancing, tuning, configuration management)
- Execute authorized change requests
- Execute tier creation, upgrade, and refresh

- Execute all tier system level changes (initialization and configuration parameters)
- Execute all object changes for all instances
- Maintain non-sizing and non-platform specific application tier parameters and system settings across all like instances according to established SDLC
- Implement and administer appropriate tier management tools, to be able to achieve holistic monitoring capability of all critical functions within this tier across all server instances operating in this zone
- Patch tier software according to established SDLC
- Provide tier communication software configuration, installation, and maintenance
- Provide technical support to application operators and developers involved in administration and tuning of application software components (i.e., Momentum Financials® and Acquisitions)
- Tune 3rd-party software and middleware component configurations to achieve and maintain adequate performance and proper operations of application software (i.e., Momentum)
- Implement 3rd party software and middleware component configurations per installation guides provided by the application software vendor
- Deploy and configure application software delivered by the application software vendor into test and production environments
- Perform password maintenance every 90 calendar days to change various 3rd- party software configuration parameters where passwords are embedded
- Monitor environments including review of audit logs, alert logs, trace files, etc., and generate automatic trouble tickets for problems
- Generate automated security notifications for security exceptions per VA security policy and procedures

The Contractor shall perform server patching activities, including:

- Patch server software as needed according to VA policy
- Ensure change management procedures are followed
- Provide a list of server patches being applied
- Apply all patches in development and test environments prior to implementing into production

The Contractor shall perform server disaster recovery activities, including server back-up and recovery activities in accordance with section 5.3.1.

5.3.3 Maintenance Support

The Contractor shall provide a maintenance schedule in conjunction and collaboration with the VA. The schedule will be published a year in advance. Depending on business and security requirements, exception will be requested in writing on approved by the VA. The schedule will support required patches, maintenance, and upcoming changes.

The Contractor shall perform the following maintenance and support activities:

- Define and update maintenance and repair policies, procedures, and schedules during upgrades
- Ensure appropriate maintenance coverage for all service components.

Provide maintenance and break/fix support in VA's defined locations, including dispatching repair technician to the point-of-service location

Deliverable:

A. Maintenance and Patching Schedule

5.3.4 Findings and Vulnerabilities

The Contractor shall close or mitigate open vulnerabilities in accordance with OIT guidelines.

5.3.5 Database Administration

The Contractor shall provide system-level database administration including software installation and maintenance, backup, and recovery, and writing and maintaining scripts to automate tasks in support of customer database environments. The Contractor shall perform the following tasks:

- Develop generic HELM, Terraform, or equivalent infrastructure as code scripts to assist to deploy infrastructure automatically.
- Provide access reports, on demand, as requested by the VA
- Provide database storage management and develop, maintain, and track database storage for reporting and trend analysis
- Retain database backups for an organizationally defined period.
    - Configuration
    - Image Backup
    - Data and Structure (RMAN)
    - Raw Data Backup (Exports)
- Assist VA in developing an off-site or off-Azure database backup strategy if required by Federal mandate or requested by VA

- Manage database communication software configuration, installation, and maintenance
- Open, track, and manage to resolution all database problems and incidents

The Contractor shall provide reference materials with respect to the compatibility of the enterprise software product in use by the VA product

- Execute all database system-level changes (initialization parameters)
- Execute database creation, configuration, and refresh
- Generate automated security notifications for security exceptions per VA security policy and procedures
- Monitor database(s) including, but not limited to, review of audit logs, alert logs, trace files, sql*net logs, etc., Problems will have trouble tickets created, preferably automatically, or submitted as enhancement stories when the work cannot be completed solely by database administrators.
- The Contractor shall provide recommendations on process improvements, annually at a minimum, to the VA seeking approval for implementation.
- Provide support to application database administrators for database performance tuning, index generation and maintenance, nonstandard backups, and non-RDBMS relational database components
- Implement and administer Enterprise Manager , or equivalent, and other appropriate database management tools across all database instances including ensuring the availability of performance metrics and historical data for trending and reporting over a minimum of 12 months
- Define and execute database performance and tuning scripts and keep database running at optimal performance for the agency’s workload
- Maintain consistency of non-sizing and non-platform specific database parameters and system settings across all like instances according to established software development life cycle (SDLC)
- Maintain documentation for all database instance parameters and system settings documenting exceptions to VA and STIG recommendations as per organization requirements
- Administer and monitor all redundant database server implementations; services including database mirroring, clustering, replication, or any similar database fail-safe implementations.
- Provide support for the COOP, through planning, documentation, testing, and execution for all COOP ISCP-related activities, which includes, but is not limited to disaster recovery and IT contingency, and create and maintain as needed, COOP ISCP documentation which includes a hardware/software list and configurations and system startup prioritization. This documentation shall be included in the COOP ISCP Plan.
- Participate in the ATO assessment and accreditation process.
- Review application queries and stored procedures for security-related vulnerabilities.

- Manage database data-level encryption, encrypted data security access to authorized applications and individuals.
- Administer and provide movement or migration of new and revised databases and applications to all databases as part of the SDLC.
- Establish libraries of scripts and stored procedures to assist developers and improve code reuse.
- Establish and maintain user access control appropriate to each database environment consistent with VA and FSC security policy.
- Monitor and administer user access, authentication, Single Sign on, logins and passwords for all databases.
- Ensure daily, weekly, and monthly jobs against all databases execute.
- Periodically test database backups, to include full restoration of one or more databases or entire database server.
- Monitor all databases for security breaches; investigate or support investigation of possible breaches with security personnel.
- Ensure test recovery procedures for databases and for web and application servers are accurate, and written recovery procedures tested at least once a year.
- Respond to callback and serve as the initial point of contact for failures of the database components and products and ensure and coordinate the resolution and correction of failures.
- Provide preventative maintenance services and troubleshoot each database instance to ensure database components that comprise IT Infrastructure are operational 99.99% of the time. Computation excludes scheduled, pre-agreed outages and outages caused by VA provided equipment, power, network, and/or user generated disruption of service.
- Provide Data Dictionaries and Db Schema/Configurations including maintaining the table, data elements, domains, and views for iFAMS databases.
- Update database specific sections of the Production Operations Manual (POM), Release Management SOP, and Configuration Management Plan.
- Ensure all configuration, schema, and data changes (where applicable) are deployed and tested in non-production environments prior to release to production.
- Demonstrate modifications to data showing evidence that appropriate testing has been done prior to seeking approval to execute said modifications in production.
- Support access reviews and advising the government when there are discrepancies between those who have and/or are requesting access and their role pursuant to the concepts of least privilege and zero trust.
- Participate in scrum and release planning activities.
- Follow all VA, FSC, and iFAMS change and configuration management (CM) processes.
- Ensure all configuration, schema, and data changes (where applicable) are documented following CM processes and synchronized between all non-production and production environments.

5.3.6 Database Patches and Upgrades

The Contractor shall perform database patches and upgrades when required to maintain vendor support and/or when requested by the VA, to include the following activities:

- Provide a plan for database patch and upgrades prior to commencing work.
- Perform assessments in the test environment for database upgrades and present a patch and upgrade plan for approval by the VA in alignment with Software Development Lifecycle (SDLC).
- Apply all patch and upgrades per configuration management plan.
- Apply all patch and upgrades as otherwise documented in a change request approved by the VA per configuration management plan.
- If environmental or third-party product conditions preclude maintaining database upgrades to the level required to maintain vendor support, Contractor shall document the reason and submit for a POAM with system steward(s), which shall include a mitigation and remediation plan and expected timeframe for returning to full compliance or risk acceptance as applicable.
- Support the VA selected database enterprise software package and version with an annual justification of selected package
- The section is intended to include the selected database enterprise software package as well as its database ancillary modules, functions, and accessories to include but not limited to synchronization, intrusion detection, backup, and high availability functionality.
- Provide monthly reports indicating database patch and upgrade execution

The Contractor shall perform database upgrades when requested to include the following activities:

- Perform assessments in the test environment for database upgrades and present an upgrade plan for approval by the VA

Deliverable:

A. Database Patch and Upgrade Plan
B. Database Patch and Upgrade Execution Report
C. Database Administration SOP

5.4 OPERATIONS AND MAINTENANCE SCALING SUPPORT (OPTIONAL)

At the direction of and upon optional exercise by the Government, the Contractor shall scale up additional operations and maintenance support in accordance with incremental increases in iFAMS users as defined under Section 5.3.

5.4.1 Initial Scaling Support (OPTIONAL)

At the time of the award, iFAMS user base is below 5,000 users. The Government anticipates an optional exercise once the user base exceeds 5,000 users, and subsequent additional exercises at each 5,000 user increments.

5.4.2 Mature Scaling Support (OPTIONAL)

Upon reaching 20,000 users, the Government will exercise option at 10,000 user increments to reflect economy of scale and maturity of experience in supporting additional users.

5.5 BUSINESS PROCESS VALIDATION SESSIONS (OPTIONAL)

The Contractor shall validate and document the migrating component's as-is end-to-end business processes at the activity level. As-Is documentation includes but not limited to, an inventory of interfaces, internal control activities, reports, existing as-is configuration guides, process maps, and data dictionary.

The Contractor shall conduct a gap analysis to identify the differences between the migrating component's legacy systems (e.g., financial management, acquisition management, reporting) and Momentum. Gap and impact analysis activities include but are not limited to:

- Migrating Agency's business processes and standard business processes.
- Accounting code structure variances.
- Validating specific business rules to setup document types.
- Validating gap solutions.
- Validating and refining Workflow/Workflow groups/Workload Managers/Approval Templates.
- Reference tables and data comparison.
- Standard report comparison.
- Interface comparison

The Contractor shall provide subject matter expertise to coach, mentor and/or consult with Government Program Managers on financial systems standards as prescribed by industry and Government best practices in Federal financial, budget, acquisition, grants, and asset management functionality. The Contractor shall provide subject matter expertise support in financial system standards, guidance, and processes including but not limited to:

- Financial Management Line of Business (FMLoB)
- Core Financial Systems Requirements as defined by the Office of Federal Financial Management
- Office of Management and Budget (OMB) Circular A-127

- OMB Circular A-123 and Appendices
- Digital Accountability and Transparency Act of 2011 or DATA Act.
- Federal Accounting Advisory Board (FASAB) Handbook of Federal Accounting Standards

The Contractor shall assist in facilitating activities associated with business process education and alignment. Activities include training subject matter experts on requirements processes and how to define, communicate and document requirements. The Contractor shall assist with the evaluation of requirements management tools to ensure a process is in place to manage requirements throughout the migration.

The activities should include but not be limited to the following:

- Finalize list of in-scope processes for migration and identify which processes will undergo re-engineering.
- Validate and update the Deep Dive.
- Validate and update process decomposition for in-scope processes based online of Business service catalogs.
- Develop Target State Process Flows for in-scope processes, considering internal control, segregation of duties, technology, handoffs, workloads, and manual workarounds.
- Review, validate, educate, and update processes with stakeholders.
- Develop and maintain Desk Guides/User Guide for customer and provider processes.
- The Contractor shall use best practices that include but not limited to the following:
    - Establish a standardized and common process decomposition to have consistency in terminology using guidance from the applicable business lines.
    - Perform business process alignment activities rather than traditional business process reengineering to avoid bad practices continuing in the new system.
    - Identify key functional process lead and subject matter experts to drive process ownership and decision making.

The Contractor shall create, refine and manage a backlog of epics, features and user stories using the prescribed Enterprise Agile Planning tool, currently Agility. Backlog management processes shall be documented the Requirements Management Plan (RMP). The RMP shall include an approach for identifying and prioritizing categories of requirements (e.g., mission critical, must-have requirements (operational, functional, technical, data, interface, security/cybersecurity, reporting, contact center, controls, and

performance)). Where applicable, the RMP shall cite regulation or policy source documents that will also be associated with the applicable to-be business processes.

The Contractor shall develop and maintain a Requirements Traceability Matrix (RTM) for all iFAMS releases that maps and traces backlog requirements from the enterprise roadmap, enterprise epics, epics, features, user stories and test cases (functional, IST, UAT). The RTM shall be used to validate that functional and technical (e.g., security, interfaces) requirements have been fully met and tested. The contractor shall utilize the EAP tool/Agility and other tools/documents as needed from partners and stakeholders to develop and maintain traceability.

Deliverable:

A. Gap and Impact Analysis by legacy system
B. Functional Requirements
C. Requirements Management Plan
D. Requirements Traceability Matrix for every iFAMS release
E. Desk Guides/User Guide

5.6 WAVE IMPLEMENTATION (OPTIONAL)

VA is implementing Momentum utilizing a Wave approach. Waves consist of the incremental delivery of the specific Momentum capability resulting in production use by the enterprise or for a subset of VA users, or updates to existing VA users. The Contractor shall support Wave implementation in accordance with this PWS. Wave implementation is the process of moving an entity at a government agency from legacy financial and acquisition systems (including interrelated system(s)) to the Momentum solution in iFAMS. The migration process typically includes business process and internal controls analysis, configuration, addition of interfaces, developing business intelligence reports, enabling access to VA personnel, conversion, testing, change management, and training.

5.6.1 Integrated Project Schedule (OPTIONAL)

The Contractor shall create and maintain an Integrated Project Schedule (IPS) in MS Project format that depicts the full scope of the project and deliverables. The IPS shall follow the established FMBT Schedule and include defined activities and all applicable Universal Project Milestones (UPM) for identifying and documenting discrete events necessary to complete the project. The Contractor shall identify task dependencies, estimate task durations, and assign required resources to each task. Any changes to the project schedule shall be reported per the requirements stated in IAW PWS paragraph 5.1.3.

The IPS shall clearly identify the critical path for the project. The Contractor shall obtain the necessary data and update the IPS at minimum on a weekly basis, or more frequently as required, for generating schedule reports that depict planned versus actual program, product/project performance and critical path.

Deliverable:

A. Integrated Project Schedule

5.6.2 System Test Plan (OPTIONAL)

The Contractor shall utilize previously created System Test Plans to create a unique test plan for each release/wave and subsequent testing event in both draft and final formats and deliver to the Government, or upon the COR's request. The Contractor shall describe in the test plan:

- Testing of enhancements to iFAMS software
- Testing of configuration for the event
- Testing of inbound and outbound interfaces to the system
- Testing of specific user configurations to ensure that workflow and approvals are complete
- Identification, disposition, and elevation of any gaps identified in the event.
- The System Test Plan shall also address all software testing for production and wave releases and development and configuration work for new interfaces and modules. The Test Plan shall document the following:
- Assumptions and considerations
- Specific approach to each testing event and how it will be performed
- Identification of Test Environments to be used in the event
- Documented Acceptance Criteria

The Contractor shall schedule and lead testing meetings to present the details of the plan to the government, present status of any testing event, address any concerns of the government with the quality of the software that is being tested.

Deliverable:

A. System Test Plan Updates

5.6.3 Wave Implementation Plan and Schedule (OPTIONAL)

The Contractor shall provide a Wave Implementation Plan and Schedule to the Government for review as soon as a Wave is formalized. The Wave Implementation

shall incorporate business process, organizational communications management, interfaces, release of products, access to Momentum subject matter experts, customer configurations, testing, ACS, data cleanse and migration support, internal controls, extensibility, scalability, updates to previously implemented waves, technical infrastructure, databases, and business intelligence reports.

Upon Government approval, the plan shall be implemented. The schedule for Wave implementation will be determined by the Government In collaboration with the Contractor.

The Contractor shall produce a price estimate for each wave and shall consider all tasks required for the successful go-live of the Wave including (each should be identified separately within the estimate):

- Wave Management
- Configuration and Process Design
- Conversion (note that conversion is designed and developed under a separate contract but should be tested with other components of the wave)
- Support for the Data Cleanse effort
- Interfaces (note that new interfaces are designed and developed under a separate contract but should be tested with other components of the wave)
- Testing, to include testing of all business processes, 508 testing, performance testing, systems integration testing, production simulation testing and support for UAT
- Training Material Development and Delivery
- Go-Live support including the period of Post Production Support (Hypercare) estimated at 90 days
- Reports Design and Development
- Planning for and execution of cut over to Production
- Release Management

For each Wave implementation, the Contractor shall assign a dedicated Project Lead to manage and staff each Wave implementation effort, execute the implementation tasks, and coordinate with agency management and the Program Management Office.

Deliverable:

A. Wave Implementation Plan per wave
B. Wave Implementation Schedule per wave
C. Wave Cost Estimate per wave

5.6.4 Business Operations Planning, Concept of Operations (CONOPS) (OPTIONAL)

The Contractor shall develop a Business Operations CONOPS and Production Operations Manual (POM) for Government approval. CONOPS shall cover all financial and acquisition business activities for iFAMS for daily monthly and yearly activities. The CONOPS shall include, at a minimum, the organizational design, business operations designs, and a RACI.

Deliverable:

A. CONOPS per Wave
B. POM per Wave

5.6.5 iFAMS Configuration (OPTIONAL)

Based on the results of the validation sessions with agency staff, the contractor shall configure the system to meet all requirements for each wave implementation.

5.6.5.1 iFAMS ACS Configuration

Based on the results of ACS working sessions with agency staff, the contractor shall develop the approach for system configuration to accommodate ACS requirements. The Contractor shall include documentation on the proposed ACS, the crosswalks/mappings necessary for the migration from old FMS ACS to new iFAMS ACS, any extensibility changes necessary to accommodate the changes made, the need for system edits, and documentation of all system and implementation areas impacted. In addition to the documentation, the Contractor shall provide support in the actual mapping of the ACS data elements from FMS and VA feeder systems to iFAMS.

The Contractor shall update the ACS Guidance provided by the Government in accordance with the changes because of the ACS Mapping and Federal policy and guidance for each FMBT Wave implementation.

The Contractor shall create a wave-specific Conversion Guide unique to each Administration or Staff Office in accordance with data requirements and conversion logic.

5.6.5.2 ACS Testing

In addition to unit testing the configuration, the Contractor shall support the testing of the ACS in iFAMS; including supporting the building of test scripts, testing, data validation and reconciliation. The Contractor will support the identification of modifications to the structure and support the remedial activities to incorporate the changes into the ACS.

5.6.5.3 Feeder System and Interface Support

The Contractor shall support the WAVE implementation by providing critical subject matter expertise on the Momentum solution for the identification of the data elements required for the mapping, import and export to/from VA feeder systems.

Key tasks include:

- Collaborate with Interface/Feeder Systems team to add accounting requirements during Technical Interface Assessment (TIA)
- Document the usability of accounting code structure for conversion of transactions from VA feeder systems to iFAMS
- Hold working group sessions with systems power users to evaluate business need
- Evaluate compliance of feeder system to federal accounting standards and requirement
- Reconcile GL cutoffs/timing differences in each system/interface to iFAMS
- Define and maintain tasks in wave IPS
- Coordinate with the Conversion/Interface Development Contractor for PI planning events
- Coordinate wave level status reporting to the program
- Communicate interface progress and impact on wave
- Participate in client meetings
- Develop high-level process for the new interface (process flow diagram)
- Participate in requirements and office hours as needed
- Review interface requirements and design
- Provide technical design reviews, code reviews
- Participate in transition meetings to receive hand-off of an interface to O&M team
- Collaborate with the Conversion/Interface Development Contractor and feeder system teams to optimize interface architecture and design
- Communicate and address configuration requirements
- Conduct System Integration testing, testing, issue tracking, resolution, retesting
- Support UAT activities
- Coordinate testing activities, reviewing test scenarios, environments, support configuration and security set up as needed to support test events
- Identify conversion topics that impact BI
- Coordinate with BI team to address impacts

5.6.5.4 Data Validation and Reconciliation

Validating the balances for each element in the ACS will be crucial during the Migration Phase. The ACS team will collaborate with the Data Management team to determine which balances will serve as the beginning balances in the target-state.

Key activities will include:

- Leverage Treasury guidance to create tie points that validate the reasonableness and completeness of FMS data
- Perform tie point analysis at the determined level (appropriation, fund, SGL etc.)
- Reconcile and investigate the reconciliation differences
- Upload the balances in the test environment and re-test the tie points
- Drill down to transaction detail levels to clean up tie point differences that exist
- Treasury Government Wide Treasury Account Symbol (GTAS) edit check validation
- Support data conversion and quality assurance activities during migration

Based on validation sessions, the Contractor shall align the as-is process with the individual migrating component's to-be model, where applicable, and develop additional to-be models as required.

Activities for the development of the business model include but are not limited to:

- Defining and validating the to-be business model.
- Defining extended functional requirements.
- Developing the business model

The Contractor shall support the development of an Interim State Environment for each migration wave utilizing outputs from various work streams across the program. The Contractor shall leverage the gap planning and analysis process activities outputs to ensure a consistent implementation approach for each wave. Activities include but are not limited to:

- Interim State Environments
- Design Interim State Processes

The Contractor shall identify and document all new functional and/or technical requirements and associated impacts identified during the Momentum Business Validation Sessions and throughout the project. Momentum functional requirements include, but are not limited to:

- Reference Table Configuration

- Workflow
- Interfaces
- Application Security
- Application Extension (Momentum Extensibility)
- Reports
- Business Intelligence
- Problem Definitions and Relationship Edits

5.6.5.5 Financial and Acquisition Management Segment Target State

The Contractor shall define and document the TO-BE operating models for each of the following components of the Financial and Acquisitions Management Segment Target State:

- Budget Formulation to Execution
- Request to Procure
- Procure to Pay
- Bill to Collect
- Reimbursable Agreements
- Record to Report
- Acquire to Dispose
- Grants Management
- Core Accounting and General Ledger

For each of the above Financial and Acquisitions Management Segment components, the Contractor shall develop the following at a minimum:

- Business Processes that match the Agency functions the Momentum solution functionality.
- Interfaces and Extracts that permit the solution to consume transactions from other sources systems, and convey needed information to target systems
- Momentum configuration documentation that supports how the Agency uses Momentum to execute the above components
- Conceptual views that include Process, Functional, Systems, and Data to depict the full operating capability

5.6.5.6 Treasury Financial Management

The Contractor shall support the analysis and configuration of Momentum necessary to remain in compliance with Treasury, OMB, and Federal regulation reporting requirements.

Key Tasks Include provide functional and technical support for the following external reporting processes:

- GTAS
- DATA Act
- 1099
- MINX
- SF-133
- TROR
- Cash Reconciliation
- Intragovernmental Eliminations
- Financial Statements

Deliverables:

A. ACS Conversion Guide ACS Element Updated Documentation (updated during the WAVE)
B. Documentation on iFAMS ACS Configuration
C. Reports on ACS Testing and Data Validation/Reconciliation
D. Documentation on Feeder System and Interface Support
E. To Be Operating Model by Component
F. Technical Requirements
G. Target State Environment
H. Interim State Environment for each migration wave

5.7 POST-IMPLEMENTATION SUPPORT (OPTIONAL)

The Contractor shall provide Post-Implementation Production Support, after go-live until the pre-defined exit criteria has been met to validate achievement of the initial level of stabilization, as applicable. General iFAMS FSC support and Help Desk support shall be included. Support will be structured and executed based on customer needs which may include on-site, virtual or a hybrid model. The Contractor will also attend and support recurring meetings such as, daily touchpoints, executive briefings, and tier coordination meetings. The Contractor will provide SME support for pre-planned and ad-hoc workshops, for each functional area to reduce ticket volumes and accelerate stabilization. Workshops may include system demonstrations and live troubleshooting of user issues. The Contractor will provide data for recurring briefings to stakeholders and executives, such as user log ins, transactions status reports, and inputs into trend analysis. The Contractor will work in collaboration with the Government and other support vendors to provide relevant inputs to post-implementation status briefings and reports.

5.8 ACCOUNTING CLASSIFICATION STRUCTURE (OPTIONAL)

Federal Financial systems must be maintained in accordance with the Common Government-wide Accounting Classification (CGAC) Structure. CGAC is a Financial Management Line of Business (FMLoB) initiative taken up by the Office of Management and Budget (OMB) to assist agencies with their financial management system modernization efforts, and to reduce the cost and risk of implementing and maintaining these systems.

The CGAC structure establishes a standard method for classifying the financial effects of Government business activities. Although several standards exist for classifying financial transactions, the CGAC standards provide latitude for each agency to develop its own classification structure. As a result, the classification structures used in agency systems vary from agency to agency and often from bureau to bureau within the same agency.

The CGAC structure increases standardization in the following ways:

- Identifies the elements to be used for classification
- Establishes standard names, definitions, and formats for the elements
- Aligns the values of similar codes used by OMB and Treasury

Additional information on CGAC is provided by the Treasury's Office of Financial Innovation and Transformation ("FIT") group.

The Accounting Classification Structure Work Group (ACSWG) developed the FMBT Accounting Classification Structure (ACS). It is a comprehensive line of accounting which provides a standard methodology for classifying financial effects for federal business activities. The structure is based on the Common Government-wide Accounting Classification (CGAC) requirements and is compliant with Federal financial regulations and guidance.

The Contractor shall support the development of the ACS for each wave to identify wave-specific ACS data elements and reporting requirements.

5.8.1 ACS Element Mapping

The Contractor shall support the ACS element mapping effort. The Contractor shall attend and participate in the ACSWG mapping sessions, support the continual identification and coordination of the delivery and validation of the legacy data, and map VA legacy account code structures (of all VA Administrations and Staff Offices) to the account code structure available in the Momentum Financial System. This crosswalk will serve as a foundation for the migration of VA’s financial systems and will be the

basis for decisions on BPR configuration, data validation, and feeder system/interface re-design, training, and GL posting models.

The Contract shall also support the development and mapping of the payroll crosswalks unique to each Administration or Staff Office.

The Contractor shall support the following efforts related to ACS element mapping:

- Develop crosswalk and mapping files for 19 agency defined ACS elements
- Ensure iFAMS is compliant with the 58 OMB and Treasury-defined ACS data elements
- Facilitate working sessions with Administrative Offices (AO) and VA stakeholders to validate data mappings and gain user acceptance and approval, includes but not limited to developing presentations, developing, and presenting iFAMS demonstrations, providing expert Momentum functional capability knowledge, and researching and providing insight in industry best practices
- Tailor crosswalks/mapping/documentation to each AO to support respective wave implementations (Grants, Insurance, Budget Formulation, NCA, VHA, etc.)
- Develop and maintain a repository for non-ACS data elements
- Update ACS Guidance documentation to align to target and interim state business processes
- Develop the approach for system configuration to accommodate ACS requirements, including documentation on the proposed ACS, the crosswalks/mappings necessary for the migration from old FMS ACS to new iFAMS ACS, any Extensibility changes necessary to accommodate the changes made, the need for system edits, and documentation of all system and implementation areas impacted
- Assist VA with customer support and reorganizations, at the direction of the Government

The Contractor shall update the ACS Guidance provided by the Government in accordance with the changes because of the ACS Mapping and Federal policy and guidance.

5.8.2 ACS Training (OPTIONAL)

The Contractor shall provide support for ACS training to all VA Administrations and Staff Offices. This includes preparing the training materials and assisting with delivering the training.

5.8.3 ACS Timeline (OPTIONAL)

The ACS support will continue throughout the FMBT WAVE implementations for all VA Administrations and Staff Offices.

Deliverable:

A. FMBT ACS Guidance Document - updated per Wave
B. Preliminary ACS Data Mapping Files
C. Preliminary AO Approval Documents
D. Final ACS Data Mapping Files
E. Final AO Approval Documents
F. All ACS Facilitated Meeting Agendas and Meeting Minutes
G. All meeting agendas must be provided 24 hours in advance of the meeting based upon the work week
H. Auditor Required Documentation
I. ACS Element Mapping
J. ACS Training Material, including Job Aids

5.9 TRAINING SUPPORT (OPTIONAL)

5.9.1 Training Support Plan

The Contractor shall work with the Government to develop and implement the Training Support Plan. The Training Support Plan shall include a strategy and implementation plan for formal training, just-in-time training, knowledge transfer, remedial/refresher training, and solution rollout support activities for all identified impacted stakeholders. Additionally, the plan will include appropriate design/delivery methods (i.e., ADDIE) and curriculum such as eLearning, on-line tutorials, classroom sessions, and the development user friendly documentation such as on-line procedure manuals, job aids, videos, FAQ, and knowledge bases.

Deliverable:

A. Training Support Plan

5.9.2 Training Development (OPTIONAL)

The Contractor shall create training materials such as training slides with exercises, quick reference guides, and Computer Based Training (CBTs), and training surveys. The Contractor is responsible for developing and distributing (where applicable) materials to support the execution of training and rollout/post go-live support (e.g., training handouts, presentations, work aides, work reference sheets, etc.). The Contractor is responsible to produce a curriculum to improve and enhance professional knowledge, skills, and abilities along with improving performance in respective job-

related areas. This task encompasses the design and development of training and performance improvement solutions. Design and development will follow industry best practices for instructional system design along with software and technology. This task may involve new courseware and/or redesign of existing courseware based on appropriate methodologies.

Instructor Led Training

The Contractor shall create a design specification, stating the training approach, methods, and modalities to be used to close the gap between performance requirements and current performance levels. The specification shall include the following:

- Learning strategies, techniques, and activities.
- Pre-requisites and post training requirements.
- Enabling and terminal learning objectives.
- Storyboard or other descriptive content summary.
- Participant assessment and knowledge check.
- Test and quality management approach.
- Sequence and grouping of performance objectives and associated activities to promote learning, skills transfer, and competency.
- Description of specific deliverables which may include any or all the following:
    - Lesson/presentation/facilitation plans
    - Training Guides/Instructor Guides (Facilitator and Participant)
    - Supplemental resources (job aids, videos, website(s), CDs, etc.)
    - Practical Exercise materials and guide
    - Illustrations/ graphics/ presentation materials

The design specification shall be approved by the COR prior to proceeding to the development phase.

The Contractor shall develop the learning program or learning series per the approved design specification to include print ready, reproducible course materials and source files for course materials. Produce documents and materials needed as a facilitator for virtual classroom presentations.

Develop evaluation instruments to determine the feedback towards training and the pre-training skills, and post-training knowledge and performance as aligned to the stated training objectives in accordance with the approved design specification.

Web Based Training

The Contractor shall create a production specification, stating the training approach, methods, and modalities to be used to close the gap between performance requirements and current performance levels.

The production specification shall include the following:

- Learning strategies, techniques, and activities.
- Prerequisites and post training requirements.
- Enabling and terminal learning objectives.
- Storyboard, wireframe storyboard, scripts, shot lists and/or other descriptive content summary.
- Participant assessment and knowledge check.
- Sequence and grouping of performance objectives and associated activities to promote learning, skills transfer, and competency.

Performance Support framework including job aids and performance support resources to be available to the target audience just-in-time outside the formal training environment.

- Description of resources to be provided for synchronous use of media, such as facilitator guides, panel discussion recommendations and evaluation guides.
- List of production materials to be delivered with finished media. The purpose of delivering production materials is to facilitate future modifications, edits, and revisions. The following list provides examples:
    - Rough-cut video including video shot for source material at live presentations
    - Final cut edited video (via review tool)
    - Supplemental resources such as job aids and reference cards
    - Illustrations/ graphics/ presentation materials for web-based launch pages (for video vignettes)
    - Web-ready, fully compliant interactive supplemental materials editable format for modification by VA or other vendors.
    - Interactive functional prototypes and formatting for sandbox pre-release versions of supplemental materials

The production specification shall be approved by the COR prior to proceeding to the development phase.

The Contractor shall develop the learning program or learning series per the approved production specification. The Contractor shall package and deliver the production materials as described in the approved production specification.

The Contractor shall develop evaluation instruments to determine the feedback towards training and the pre-training abilities, and post-training knowledge and performance as aligned to stated training objectives in accordance with the approved production specification.

Deliverable:

A. Training Materials and Lab Exercises
B. On-line Training Evaluation
C. Training Summary Plan
D. Quick Reference Guides
E. Online Self-service Training
F. Training Curriculum
G. iFAMS Training Video Vignettes
H. Plan of Instruction
I. Production Specification

5.9.3 Training Execution (OPTIONAL)

The Contractor shall conduct training for the Functional Coordinators, Help Desk Staff, and User Community (in accordance with the format and type designated by the Government). The Contractor shall provide an instructor's laptop for each training class. The Government will provide training facilities and required connectivity will be in place for the scheduled training. The Government will provide the workstations, overhead projectors, flip charts, and other materials required to conduct training in the training facilities and the Government will establish connectivity between the instructor's laptop and the training environment. Anticipated type of training ranges between the following four levels:

Level 1: Passive-No Interaction: A linear sequence of presentation, commonly referred to as 'page-turners'. A Level 1 course is linear and could be considered basic training, in which the participant is an information receiver. The participant is limited to watch, read, and navigate.

In the fixed sequence of presentation, the participant does not choose the order of the content. Passive presentations do not permit return to a previous topic or browsing freely. Level 1 is the minimal level to be considered eLearning or class-based learning; however, it can be effective for communicating simple concepts, and is relatively inexpensive to develop. Level 1 includes:

a. Graphics, images, and simple animations
b. Rollovers

c. Basic quiz questions

Level 2: Limited Interactivity: Level 2 course interaction is basic, but the participant has limited control over their training. Level 2 is used for non-complex operations and maintenance lessons. Limited Interactivity includes resources such as:

a. Clickable animated graphics
b. Navigation via menus, glossaries, and links to external resources
c. Simple exercises (i.e., drag-and-drop, matching, and identification components)
d. Audio and video, typically referred to as video vignette

Level 3: Moderate Interactivity: Level 3 provides a high degree of complexity of the course presentation, providing multiple pathways and resulting in a wide range of duration.

From the standpoint of the participant the course is a dynamic activity and does not require presentation of all available content. Selection of content is typically based on questions or testing at the module level. The goal is an optimized balance between active learning and development time.

Moderate interactivity includes resources such as:

a. Animated videos or video development
b. Audio recording, such as panel discussions, where the participant can select specific questions to be answered
c. Strategies for explaining use of applications allowing data to be entered to appropriate fields, with predictable results
d. Highlighting or “white board” style ability to markup content for discussion.
e. Scenario-based cases with multiple possible outcomes
f. Ability to access performance support tools, references, and other resources from within the training scenario.

Level 4: Simulation and Game-Based Learning: Level 4 level gives the highest degree of participant interaction. The goal is to provide a real-time or near real-time mimicry of situations in a safe environment. Simulation and gaming are frequently used when practice of an activity would pose real risk to participants, or equipment. Gaming is frequently conducted to allow a single participant to act and react within a simulated group encounter. Simulation and gaming are also used when the group to be trained cannot be co-located. The Level 4 course includes simulation and gaming resources such as:

a. Real-time learning.

b. Use of simulation and other gaming technology.
c. Virtual conferences

The level of training shall be based on the requirements, learning objectives, target audience description, modalities, and duration of training to be provided. Training programs shall be offered in a wide variety of training modalities and methods including asynchronous eLearning and media-based training, synchronous webinar and virtual classroom facilitated, and face-to-face instructor-led group offerings. All eLearning solutions shall be compatible with access via the LMS or other identified technologies. During the design process, focus groups and meetings with all stakeholders and subject matter experts may be conducted to ensure full understanding of the training requirements and target audience. VA acknowledges that VA user groups will need appropriate financial and acquisitions management (i.e., core accounting) training as a pre-requisite, prior to engaging in the iFAMS training curriculum. The Contractor may provide eLearning solution recommendations as pre-requisite training so VA user groups can familiarize users with their roles within iFAMS. Training is dependent on the user's role and responsibilities. VA's diverse users and budgetary accounts may require introductory as well as in-depth classes in financial management and budget execution. The Contractor shall perform all work in compliance with the Government and/or Contractor's standard operating procedures for application of Government and industry best practices for instructional design.

The Contactor will provide onsite training (Trainers) and onsite support, Hypercare, after go-live (Support) until the pre-defined exit criteria has been met to validate achievement of the initial level of stabilization, as applicable. General iFAMS FSC support shall be included for all waves. Help Desk support shall be included. Requirements may change based on the agreed upon Training Support Plan.

Section 508 compliance (see section A 3.0) is mandatory as well as associated standards, such as SCORM conformance.

The Contractor will provide all resources for

- iFAMS System Training – iFAMS training will be tailored for the audience. A variety of methods will be utilized, including instructor-led training and eLearning. Training materials and supplemental documentation will be developed and available for end-user access
- Sustainment Training – Sustainment training will be available post Hypercare to support new employees, new system release, and refresher training and delivered as determined. See section 7 for additional information. Prepare users for the change by managing the people side of transformation in nine readiness elements:

Deliverable:

A. Training Attendance and Completion Report

5.9.4 Introduction to iFAMS Training Boot Camp (OPTIONAL)

At direction of the Government, the Contractor shall provide ad-hoc training that introduces likely users to iFAMS. The Contractor shall design, develop, and deliver the training that enables new iFAMS user to accomplish everyday tasks in the system. The course will include, but not limited to an overview of the Federal Accounting Process and the full iFAMS Product; Overviews to include topics, but not limited to Navigation, Reference Data (including Vendors), Funds and Budgets, Forms/Documents, General Ledger, and System Administration & Security. More in-depth lecture, demo and hands-on exercises will be given on modules such as Budget Execution, Purchasing/Acquisitions, Accounts Payable, Credit Card, Automated Disbursements and Accounts Receivable. Course exercises will utilize a pre-configured training environment. The Contractor shall work in collaboration with the Government to determine iFAMS Training topics, course length, planning, and training logistics needed to produce a course. The Government will determine the overall training approach and delivery including training format.

5.9.5 O&M Training Development (OPTIONAL)

The Contractor shall support iFAMS training development needs for all users at organizations already in iFAMS production. The training shall include both synchronous and asynchronous formats, a variety of training support materials including but not limited to cheat sheets, desk guides and micro learning videos, and should be tailored for the unique needs of office level user groups, including attention to processes and systems outside iFAMS but associated with iFAMS and are required for users to perform their roles in iFAMS (such as interfaces or related systems, and required manual steps that might be performed outside the system). Sustainment Training support will include but is not limited to:

- Transitioning and updating training materials that were used prior to go-live so that they may be used in production;
- A Production Training Needs Assessment - Prior to go-live of any wave group, the vendor shall deliver to the Financial Services Center (FSC) a training needs assessment of the group entering production, communicating any pressing or urgent training needs that must be addressed in sustainment as well as deficiencies noted during delivery of wave training. This assessment includes all the logistics that came out of wave training.
- Design, development and delivery of new training materials that may be needed for production
- Train the trainer support for the Contractor to train VA trainers to perform independent delivery of all iFAMS training courses

5.9.6 Sustainment Organizational Change Management Plan and Delivery (OPTIONAL)

The Contractor shall support training and user preparedness activities, including but not limited to demonstrations, labs and workshops, will be provided according to the FSC's production training schedule, or when a production release is determined to have a significant impact to users, per the FSC's Organizational Change Management framework. For every release that is determined to have a significant user impact, the Contractor should provide at a minimum the following:

1) A Change Impact Assessment - The vendor must evaluate all production releases to identify impacts to users. For any production release that is determined to have a significant user impact, as defined by the FSC Organizational Change Management framework, the vendor must conduct and deliver a Change Impact Assessment that outlines the impacts to users by role and/or affected organizational group.
2) Updating existing training materials and creating new ones as a result of production releases that have a substantive impact to users or substantively change existing training material;
3) A Production Organizational Change Management (OCM) Plan - When the Change Impact Assessment results in changes that require user training and preparedness, the vendor is expected to design and deliver a plan for how users should be prepared for the change, to include communications, training, and other preparedness events such as demos, walk-throughs.
4) Developing, tracking and delivering training satisfaction surveys for the delivery of every training or user preparedness event.

Deliverables:

A. Production Training Needs Assessment
B. Change Impact Assessment
C. Organizational Change Management Plan
D. Train the Trainer Plan

5.9.7 Sustainment Training Delivery (OPTIONAL)

The Contractor shall support the VA in developing and executing against the overall VA iFAMS production training schedule and catalogue. Training support will include but is not limited to training materials, training delivery, demos, question and answer sessions, FAQs, Quick Clips, and other blended learning approaches. The Contractor shall:

- Provide post-go live training support at the conclusion of each wave, as needed as soon as 90 days after go-live

- Provide train the trainer support for VA trainers to perform independent delivery of iFAMS training
- Provide training and communication support as needed for configuration changes, system upgrades and enhancements
- Developing, tracking and delivering training satisfaction surveys for the delivery of every training or user preparedness event.

5.9.8 Transition Plan (OPTIONAL)

The Contractor shall provide a training transition plan by wave for FSC trainers to assume the training functions. The plan shall include the approach to train FSC trainers, and include delivery of training materials (slide decks, etc.) to be utilized by FSC trainers.

Deliverable:

A. Transition Plan

5.10 PARALLEL ACTIVITIES (OPTIONAL)

For VHA implementation FMBT utilizes a Capability Build Agile Release Train to build and configure key capabilities/functional elements for identified VHA scope. These capability builds are completed outside of a wave but in such a way that the completed work can be included in any implementation wave to deliver the completed scope to the customer.

Contractor will also be responsible for:

- Managing agile release train following FMBT SAFe principles and practices
- Create, coordinate and lead, with VA team and agile release trains, backlog of technical and business aligned requirements utilizing FMBT EAP/Agility tool and following FMBT/iFAMS Agility guidance and standards.
- Coordination with project scheduling team to track agile epics and features in the Integrated Project Schedule
- Supporting and participating in Agile Council meetings, Agile/Agility Community of Practice, program retrospectives, lessons learned and continuous process improvement efforts.

The Contractor shall support the Capability Build release train by providing critical subject matter expertise on the Momentum solution for the identification of the data elements required for the mapping, import and export to/from VA feeder systems.

Key tasks include:

- Create, refine, and manage a prioritized backlog of requirements
- Collaborate with Interface/Feeder Systems team to add accounting requirements during Technical Interface Assessment (TIA)
- Document the usability of accounting code structure for conversion of transactions from VA feeder systems to iFAMS
- Hold working group sessions with systems power users to evaluate business need
- Evaluate compliance of feeder system to federal accounting standards and requirement
- Reconcile GL cutoffs/timing differences in each system/interface to iFAMS
- Define and maintain tasks in project schedule
- Coordinate with the Conversion/Interface Development Contractor for PI planning events
- Coordinate wave level status reporting to the program
- Communicate capability progress and impact on future and current waves
- Participate in client meetings
- Coordinate and support high-level process for the new capability (process flow diagram)
- Participate in requirements and office hours as needed
- Review requirements and design
- Provide technical design reviews, code reviews
- Participate in transition meetings to receive hand-off of an interface to O&M team
- Collaborate with the Conversion/Interface Development Contractor and feeder system teams to optimize interface architecture and design
- Communicate and address configuration requirements
- Conduct System Integration testing, testing, issue tracking, resolution, retesting
- Support UAT activities
- Coordinate testing activities, reviewing test scenarios, environments, support configuration and security set up as needed to support test events
- Identify conversion topics that impact BI
- Coordinate with BI team to address impacts

The Contractor shall produce a price estimate for each capability and shall consider all tasks required for the successful go-live with a Wave including (each should be identified separately within the estimate):

- Configuration and Process Design

- Interfaces (note that new interfaces are designed and developed under a separate contract but should be tested with other components of a wave)
- Testing, to include testing of all business processes, 508 testing, performance testing, systems integration testing, production simulation testing and support for UAT
- Training Material Development and Delivery
- Reports Design and Development
- Planning for and execution of cut over to Production
- Organizational Change Management
- Technical Architecture Management
- Release Management

Deliverable:

A. Project Schedule
B. Capability Test Plan
C. Capability Cost Estimate
D. Capability Backlog

5.11 OPERATIONS AND MAINTENANCE SYSTEM TESTING (OPTIONAL)

There are many types of testing in software development projects. Developers perform the first type of testing called unit testing. In unit testing, Developers test small pieces of code but not the entire system. This type of testing requires a coding background and skill set. The Contractor shall conduct unit testing.

The Contractor shall perform the second type of testing called functional testing or end-to-end testing.

In functional testing, testers conduct independent tests on the entire system to validate that the system performs as expected from a user's perspective. The Contractor shall provide Testing support to include manual and automated functional and integration systems testing; regression; integration or end-to-end performance, load, and stress testing; VA Section 508 conformance testing (see section A 3.0); security testing support; and other test types as applicable to ensure quality of iFAMS products.

The Contractor shall conduct test support activities in VA environments comprised of VA approved test and Software Development Life Cycle (SDLC) support tools that shall include, Pega Systems Business Process Management (BPM) and Customer Relationship Management (CRM), Microsoft Visual Studio, Team Foundation Server, Test Manager, Agility or other VA approved tool, Section 508 Accessibility Management Platform and related Section 508 Assistive Technology tools, where environment

configuration is driven by the unique or specific interface and database component requirements of the application or system under test. Testing support services shall apply to software, hardware, database, network, and associated applications as applicable. Testing support services shall include planning for, executing, providing test results and development of documents supporting VA Section 508 conformance Certification requirements in accordance with VA policies and guidance.

The Contractor shall provide test management and execution services to complete each assigned project. The Contractor's Test Manager shall provide management, direction, administration, quality assurance, and leadership of the execution of testing requirements.

The Test Manager shall ensure all Contractor Testing personnel are appropriately qualified to perform testing activities and:

- Manage team assignments for testing resources
- Perform quality assurance over testing deliverables
- Use VA approved tools (e.g., Agility)
- Maintain and improve testing process documents
- Proactively monitor testing performance and provide expert SME input to ITOS and iFAMS Services leadership that will improve the overall maturity of test activities

5.11.1 Operations and Maintenance Automated Testing Support (OPTIONAL)

At the discretion of the VA, the Contractor shall automate up to 75% of all test scripts that have been delivered for O&M. The Contractor and the Government will jointly select the test scripts that will be automated and agree upon the delivery time of the automated test scripts. Test automation by the Contractor must be accomplished with VA automated testing processes and tool solution. When the Contractor delivers working, automated test scripts to the Government, the corresponding test results shall also be provided. The Contractor shall report status of test automation during weekly/monthly reports.

The automated test scripts shall be available to use for any testing effort/event to ensure that iFAMS functionality is configured to meet the needs of the VA.

Deliverables:

A. Automation Test Plan
B. Automated Testing Scripts
C. Automated Test Execution Results
D. Automated Testing Report

5.12 WAVE TESTING (OPTIONAL)

5.12.1 Wave Test Plan

The Contractor shall develop a Test Plan in both draft and final format for systems testing and deliver to the VA, or upon the COR's request, use and/or update an existing Test Plan instead of developing a new plan. The Contractor shall build a set of test cases and scenarios that test:

- Enhancements to Momentum software
- Setup for the acceptance of interface inbound to and outbound from the system
- Agreed-upon customer accounts receivable and billing business processes
- Integration gaps
- Momentum configuration testing
- The Test Plan shall also address all software testing for service releases and development work for new interfaces and modules. The Test Plan shall document the following:
- How the Contractor shall support The VA in performing the acceptance and end-to-end testing
- Detailed Test Cases, including Test Case descriptions, setups, and expected results
- Detailed Performance Test Cases, including Test Case descriptions, setups, and expected result.

For tasks involving software development (e.g., new interfaces or modules), the Test Plan shall include a requirements traceability matrix (RTM) to ensure appropriate tests are performed as changes are made. Test Cases shall be based upon the functional and technical analysis and shall be developed with a thorough knowledge of customer data sets and performance requirements. The Test Plan and Test Cases shall be reusable throughout the life cycle of the application.

Deliverable:

A. Test Plan Update

5.12.2 Wave System Testing and Test Reporting (OPTIONAL)

In accordance with the established FMBT Test Plan, the Contractor shall conduct individual unit/module testing, system testing, and regression testing for the following:

- New interfaces
- New functionality
- All waves

- Upgrades and Service releases for Momentum
- New BI Tool or reports
- Monthly builds

The Contractor shall perform tests to (1) isolate suspected and confirmed defects and issues and (2) confirm software corrections. Testing should be planned and executed systematically. The systems test criteria are the responsibility of the Contractor. All functionalities shall be complete, with all failures addressed internally by the Contractor prior to submission to The VA.

All of Contractor's testing shall be documented in a test report to the extent that tests can be recreated. Contractor shall provide to The VA all test scripts, test related results and mitigation plans to resolve any issues arising from testing no less than 10 calendar days prior to all Contractor conclusion of testing.

Deliverable:

A. Test Report

5.12.3 Wave Regression Testing (OPTIONAL)

The Contractor shall perform Regression Testing to validate that software and interface functionality continues to work as desired after implementation of software changes. The Contractor shall perform Regression testing during the system testing phase of the project.

Regression Testing shall include full customer data and volume for processes in both the financial module and acquisitions module as requested. The Contractor shall deliver Regression Test Results to The VA.

Contractor shall provide a status of regression testing at the weekly/monthly status meetings.

Contractor shall provide all test results in a Document Format that demonstrates the step-by-step navigation utilized by the contract subject matter experts (SME's) and encompasses the data utilized for testing, as well as any mitigation that took place by the SME to correct issues and/or bugs.

Deliverable:

A. Regression Test Results

5.12.4 Wave User Acceptance Testing (UAT) Support (OPTIONAL)

The Government will coordinate the UAT with support from the Contractor. UAT will be executed on subsystems, integrations/ interfaces, functional configurations, workflows, custom development, and process testing. UAT will use converted data.

The Contractor will support the VA in the event of data cleanliness issues associated with converted data testing.

The Contractor shall update the test scripts/cases throughout the course of the UAT and submit the updates to the VA upon conclusion of the UAT.

Deliverable:

A. Updated Test Scripts

5.12.5 End-To-End/Production Simulation Testing (OPTIONAL)

The Contractor shall lead the end-to-end/production simulation testing activities. The Contractor shall participate with the Government in executing end-to-end testing via troubleshooting of incidents uncovered during the process. The Contractor shall track, and correct incidents reported in Momentum software and platform components. The Contractor shall provide dedicated support for the UAT end-to-end testing effort.

The Contractor shall provide a status of end-to-end testing support at the weekly/monthly status meetings.

Deliverable:

A. Production Simulation Test Results

5.12.6 Wave Automated Testing Support (OPTIONAL)

At the discretion of the Government, the Contractor shall automate up to 75% of all test scripts that have been delivered. The Contractor and the Government will jointly select the test scripts that will be automated and agree upon the delivery time of the automated test scripts. Test automation by the Contractor must be accomplished with VA automated testing processes and tool solution. When the Contractor delivers working, automated test scripts to the Government, the corresponding test results shall also be provided. The Contractor shall report status of test automation during weekly/monthly reports.

The automated test scripts shall be available to use for any testing effort/event to ensure that iFAMS functionality is configured to meet the needs of the VA.

Deliverables:

A. Automation Test Plan
B. Automated Testing Scripts
C. Automated Test Execution Results
D. Automated Testing Report

5.12.7 Wave Test Scripts/Cases (OPTIONAL)

After the Test Plan has been approved by The VA for new development, the Contractor shall develop Tests Scripts in support of User Acceptance Testing (UAT). Contractor shall provide all test scripts to support UAT – business testing requirements in a document format that demonstrates the step-by-step navigation utilized by the contract subject matter experts (SME's) and encompasses the data utilized for testing, as well as any mitigation that took place by the SME to correct issues and/or bugs. The Test shall include detailed testing steps. The Test Scripts shall be capable of supporting the UAT and meet The VA's decision to utilize for UAT purposes.

The Test Scripts, which will be used by The VA to perform UAT, must be agreed upon by The VA in advance and may be augmented with additional tests. At least 25% of the test scripts developed must be automated.

Deliverable:

A. Test Scripts/Cases

5.12.8 Wave Test Management (OPTIONAL)

For each Planned Release, the Contractor shall provide a Test Plan. The Test Plan shall include the level of testing to be performed, the objectives of the test, level of effort estimates, resources, schedule, and the evaluation criteria to be applied.

The Contractor shall base the level of testing and evaluation criteria on mission criticality, associated risks, and the level of project complexity. In addition, the Contractor shall describe in the Test Plan the overall testing strategy from development to implementation, requirements traceability to test coverage, and address functionality, integration, performance, test readiness review, and initial operating capabilities.

The Contractor shall develop and maintain currency of Release Requirements Traceability Matrix (RTM) for each application development, upgrade, and maintenance project. The RTM provides traceability between, and is comprised of entries delineating, the application's requirements, components developed for each requirement, test cases/scripts used to test the application/system requirements, and the corresponding test case execution results.

The Contractor shall ensure the Test Plan adheres to and addresses applicable process guidance as specified in approved VA templates and guidance.

The Contractor shall ensure the Test Plan includes and addresses testable requirements inclusions and exclusions, test cases, test scripts, test environment, test locations, test data, test staffing, test training requirements, test risks, test constraints, test metrics, and a listing of specific key procedures and installation verification tests across the entire system in order to enable a complete system testing approach to ensure all necessary system components are operating correctly from an end-to-end perspective.

The Contractor shall identify and deliver testability elements as specified in each project's VA approved Business Requirements, Requirements Specification, Design Specification, and RTM. The Contractor shall translate requirements into test plan development and development of test scenarios, cases, and scripts, along with supporting test data to develop and deliver the Test Cases and Test Scripts. The Contractor shall map test cases to the RTM. The Contractor shall create all necessary data to perform all testing activities. The Contractor shall not proceed with test activities until VA concurrence on the Test Plan.

The Contractor shall assess and develop strategy to evaluate each assigned project's Section 508 compliance (see section A 3.0) and system performance requirements. The Contractor shall document these requirements to support project Section 508 testing as well as Performance and Load testing.

The Contractor shall develop and deliver Test Evaluation Summary Document for each project that shall assess product quality from a test management perspective and report test execution results.

The Contractor shall ensure the Test Evaluation Summary Documents summarize status of the entire test activity for a given project. The Contractor shall ensure Test Evaluation Summary Document includes a complete system test execution log, system test evaluation metrics, system test defect log, functional, performance, Section 508, and security test results.

The Contractor shall perform the following test execution tasks for each assigned project:

1. Manage testing activities and provide test reporting for the results of testing.

2. Provide status updates for test activities, test schedule updates, and deliverables review with the VA Test and Development Managers, data center, iFAMS customers, and applicable interfacing functional areas.
3. Develop Test Automation scripts and conduct automated testing, as approved by the VA Test Manager and PM, to optimize effectiveness of regression and related test activities and to optimize manual testing activities.
4. Review the test deliverables of this section and conduct peer reviews to verify conformance with VA policy and guideline requirements and to demonstrate test coverage of defined business, functional, non-functional, and VA Enterprise system requirements.
5. Report on test progress in Scrum team and related meetings, test execution, triage meetings, and in test status reports.
6. Provide Test Results for each Test Case.
7. Provide guidance and support to VA development teams to facilitate steps for defect re- creation and resolution.
8. Contribute to documentation related to testing of application software, network and systems, and hardware components as applicable.
9. Document updates to test artifacts as required to test approved requirements related to requests for Change in response to evolving customer system needs and requirements identified through the VA formal change control process.
10. Lead and organize meetings that include agenda items such as test planning, peer reviews, test execution triage, defect management, resource planning, and test status

5.12.9 Wave Test Execution (OPTIONAL)

Based on VA Test Management guidance, the Contractor shall perform the following test execution services:

1. Verify the readiness of the test system.
2. Prepare test plan, test cases, test scripts and results documentation.
3. Design and prepare test data.
4. Execute IT software tests using agile best practices and evaluate results to ensure compliance with applicable requirements, performance and design specifications and VA Enterprise requirements and regulations.
5. Perform integration testing using agile best practices to ensure that all system modules operate as an integrated system.

Conduct specified functional, performance, Section 508 (see section A 3.0), regression, and security testing based on approved requirements and the RTM to verify that the system conforms to design documentation or specifications.

6. Log Testing events, findings, and incidents in a system test execution log and system test defect log.
7. Document test results and recommend and evaluate fixes and provide daily, or as required by VA, test status reports.
8. Provide guidance and support to system users for User Acceptance Test (UAT) activities and planning.
9. Conduct performance testing to determine a system's responsiveness and stability under a defined workload.
10. After a system has undergone enhancements, patches, or configuration changes, conduct regression testing to uncover bugs in existing functional and non-functional areas.
11. Perform Section 508 testing activities using automated tools such as Accessibility Management Platform (AMP), applicable 508 Assistive Technology tools, and manual processes to verify that a system conforms to all 508 compliance standards for accessibility. The Contractor shall document results in the Section 508 Test Summary Report and develop applicable documents in support of the VA 508 Self-Certification process.
12. Provide requested updated test documentation, such as test cases and test scripts, for Quality Assurance Inspections at unscheduled intervals.
13. Provide Execution Records and Project Test Execution Results in the Project Test Evaluation Summary Document, as outlined in Test Management section

5.13 INDEPENDENT VERIFICATION AND VALIDATION REVIEW SUPPORT (OPTIONAL)

5.13.1 Independent Verification and Validation Support

VA will assign an Independent Verification and Validation (IV&V) Team, under the direction of a VA IV&V Program Manager (PM) and IV&V Lead, to the systems and projects within scope of this PWS. The VA IV&V PM, IV&V Lead and IV&V Team is Systems Quality Assurance Service (SQAS), under the Office of Quality, Performance and Risk (QPR) within VA OIT. SQAS has overall responsibility for IV&V services and support on the FMBT program and may be supported by additional contracted IV&V resources. The IV&V scope of work is outlined and based on the approved FMBT IV&V Plan.

The IV&V Team will, at its discretion, review program, project, and product deliverables and provide IV&V comments, findings, and recommendations to be addressed by the Technology Product Management vendor and tracked to closure by the IV&V Team.

The IV&V Team will review Contractor deliverables, including but not limited to, requirements, requirements traceability, functional designs, interface control documents, test plans, test cases/scenarios, test scripts, test executions, specifications, and other documentation regarding delivered systems/software functionality, interfaces, conversions to ensure all deliverables are accurate and consistent.

Contractor deliverables will also serve as inputs to IV&V activities, such as Test Readiness Reviews (TRR) and IV&V functional and systems integration testing.

The FMBT IV&V Team will execute independent tests of the systems and configurations to help ensure VA functional and technical requirements are being met, and specifications regarding delivered systems/software functionality, interfaces, conversions, and documentation are accurate and consistent.

The Contractor shall support the IV&V Team with review and response (within 1 business day) to IV&V identified bugs/defects, needed clarifications, findings and recommendations, deliverable comments, and submitted risk or issues.

The Contractor shall keep the IV&V Team informed of changes to its requirements management, change management, configuration management, test management, defect management, quality management, release management and risk management processes.

The Contractor shall work with and support the IV&V team on coordination and scheduling of all IV&V activities including independent testing and may include, at VA discretion, execution of either or both manual and automated test scripts. The VA anticipates IV&V independent test execution to occur in advance of User Acceptance Test (UAT) events.

The VA IV&V Team may, at its discretion, organize IV&V tasks utilizing Agile best practices.

The Contractor shall support the FMBT IV&V Team by providing the test plans, test scripts, test designs, test strategies, test data, test user profile and security permissions, test execution, test execution results, test defects and user stories, related to SI test events including but not limited to Wave, O&M release, special project, and Momentum upgrades. The Contractor shall provide additional documentation as needed for each test event such as finalized approved requirements, Requirements Traceability Matrix (RTM), finalized and approved Interface Control documents, Release Notes,

Configuration documentation and any identified risks or issues that impact test execution.

The Contractor shall support the VA led IV&V team by providing read access, and where agreed upon, additional access to the Technology Product Management vendor's test tool(s) for the purpose of entering IV&V identified bugs/defects, monitoring bug/defect and other testing status.

5.13.1.1 Independent Verification and Validation Environment (OPTIONAL)

The Contractor shall maintain a separate, fully configured IV&V Independent Test System environment to which VA specified VA personnel and, if any, designated VA support Contractors will have access. IV&V test environments will be required to support IV&V test execution related to implementation Wave, O&M releases, and special projects.

The Contractor shall ensure IV&V test environment setup, maintenance, configuration, test data, test user profile and security permissions are established and ready for test execution prior to the IV&V test event. The Contractor shall address application and environment issues in a timely manner as to not negatively impact the completion of the IV&V test event.

The Contractor shall ensure the VA led IV&V team is provisioned full access to designated Integrated System Test (IST) environments, otherwise, the Contractor shall ensure the IV&V Independent Test System is configured with the capability to generate all systems interfaces either configured for or utilized by VA.

The Contractor shall maintain the continuous availability of the IV&V Independent Test System(s) 5 business days per week (Monday – Friday, 6:00AM-6:00PM EST) and coordinate with the VA led IV&V team on scheduled data loads, updates, configurations, migrations, and release installations (O&M, Wave, special projects).

The Contractor shall designate the VA as owner of the IV&V Independent Test System hosted and supported by the Contractor. The Contractor shall ensure the Independent Test System is configured with the same security controls as applied to the UAT and production systems housing PII data.

5.14 BUSINESS INTELLIGENCE (BI) SUPPORT (OPTIONAL)

The Contractor shall institute methods of system assurance that validate that the Business Intelligence solution is generating accurate and complete financial and acquisitions management reports. The Contractor shall ensure that the BI solution is consistently available to users meeting unique expectations depending on the environment. The Contractor shall provide project management, report and data governance support, report development and support, infrastructure management, operational and maintenance support, product management, and training support within the BI solution.

The Contractor shall design and implement the BI solution using an approach that ensures consistent overall system performance.

The Business Intelligence (BI) Reporting and Data Estate is comprised of several components outside of the Momentum and iFAMS configurations/infrastructures. The BI and Data Estate infrastructure is comprised or shall include the following components:

- Virtual Machines, with either Microsoft or Linux operating environments
- Microsoft Synapse
- Report Development toolset, currently PowerBI
- Governance software
- Oracle Golden Gate
- Microsoft Synapse Analytics

The Contractor shall follow the policies, procedures, and practices identified by FSC, which may include the SAFe Agile Framework and VIP tailored to the needs of FSC. The Contractor shall adhere to the iFAMS Agile process.

The Contractor shall adhere to the iFAMS Configuration Management and Change Release Management activities identified in Tasks 5.2.4 and 5.2.5 and utilize the VA identified system(s).

5.14.1 Internal Momentum Reports

The Contractor shall provide support for all reports implemented in Momentum. The Contractor shall also provide support for changes to existing Momentum reports and forms and for other reports implemented during the life of the Task Order. Contractor shall provide an Annual Report listing all existing Momentum Reports and their purpose. Additionally, the Contractor shall provide a real time dashboard indicating the status of all implemented reports.

In support of Reporting the Contractor shall, at a minimum:

- Identify and ensure inclusion of internal Momentum reports not visible to the VA configuration
- Assist with release and change management activities for inclusion of the reports within the VA configuration

Deliverable:

A. Annual Report
B. Real Time Dashboard

5.14.2 BI Project Management (OPTIONAL)

The Contractor shall be responsible for providing all administrative and managerial resources necessary for the management of BI and the Data Estate. The Contractor shall:

- Develop project schedules and plans, to include deliverables in task areas
- Mobilize resources to execute the work represented in the plans
- Monitor progress against the plans
- Provide briefings and reports of activities
- Review deliverables to ensure conformance to the quality assurance plan
- Resolve support issues within its responsibility
- Serve as the primary point of contact for all project management issues and keep the VA fully informed both verbally and in writing of any concerns or problems that arise
- Provide meeting notes
- Post of record sessions and dissemination of meeting notes
- Maintenance of owned invites and groups
- Maintenance of agile and program artifacts in the VA identified toolset
- Manages all scrum activities, i.e. – Sprint Planning, Backlog session, Agile ceremonies
- Internal and External audit support

Deliverable:

A. Meeting Minutes
B. Agile Artifacts

5.14.3 Data and Reporting Governance Support (OPTIONAL)

The Contractor shall assist with reporting and data governance. The Contractor shall assist with research, review, documentation, support, and assessment of governance activities and tools that shall be used within the Data Estate and BI environments. These activities include, but not limited to, research activities on data conforming and

governance, report standardization and governance, documentation preparation, and meeting support and minutes.

Examples of governance artifacts are as follows, but not limited to:

- PowerPoint Presentations
- Documenting results of research performed
- Meeting minutes
- Meeting notes

Deliverable:

A. Governance Artifacts

5.14.4 Data Estate and BI Development (OPTIONAL)

The Contractor shall utilize the identified BI solution for design, development, and implementation of all reports using an approach that ensures consistent overall system performance, with reports completing in organizationally acceptable periods of time.

The Contractor shall provide support for all report, dataset, and data model activity within the Data Estate and BI solution. This activity includes, but not limited to, requirements gathering, development of new reports/data models/datasets, enhancements, bugs, system testing, regression testing, user acceptance test, 508 testing, report guides, support reconciliation activities, quality assurance activities, customer inquiries, and implementation of reports and data models outside of the internal Momentum system.

The Contractor in collaboration with the VA shall identify the contents of a package containing the documentation associated with a single report. A report documentation package can include, but not limited to:

- Identification and approval of documentation
- Wireframes
- Requirement documentation
- Meeting Notes
- Report guides
- PowerPoint presentations
- Customer-facing Data Layer Definitions
- Requirements Traceability Matrixes

The Contractor in collaboration with the VA shall identify the contents of a package containing the report code and documentation associated with testing of a release that

can include new reports, enhancements, and defects. The release package can include, but not limited to:

- Testing activities, as defined in section 5.3.16, focused on reports
  - User Acceptance Test plan, cases, scripts, and results
  - 508 Test plan, cases, scripts, and results
  - System Test plan, cases, scripts, and results
  - Regression Test plan, cases, scripts, and results
- All code utilized to implement the report, enhancement, or bug
- Database code
- Data models
- Update Requirements Traceability Matrixes

Deliverable:

A. Release Package
B. Report Documentation Package

5.14.5 Data Estate and BI Operations and Maintenance (OPTIONAL)

The Contractor shall perform operations and maintenance activities for both the PowerBI application(s) and the Data Estate. The support shall include both product and infrastructure layer activities. The support shall include all environments as approved and required by the VA.

The Contractor shall institute methods of system assurance that validate that the Business Intelligence and Data Estate solutions are generating accurate and complete financial and acquisition management reports. The Contractor shall ensure that the BI and Data Estate solutions are in accordance with the continuity of operations procedures for the Data Estate and Business Intelligence solutions. The Contractor shall maintain the Data Estate and BI solutions with activities outlined in Section 5.3.20.

The Contractor shall adhere to the iFAMS Configuration Management and Change Release Management activities identified in Tasks 5.2.4 and 5.2.5.

5.14.6 Data Estate and BI Product Management (OPTIONAL)

The Contractor shall support both Data Estate and BI solution product management. The Contractor shall provide:

- Assistance and support of any troubleshooting activities
- Change management documentation
- Management and documentation of implementation of new reports, enhancements, and fixes to existing content
- Migration of existing report activities to the Data Estate
- Perform and research updates in alignment with other increased functionality changes to interfacing systems or Momentum functionality

- Data model and security model creation and maintenance
- Management and documentation of implementation of the new datasets, enhancements, and fixes to existing content
- Management and documentation of the implementation of new data models, enhancements, and fixes to existing content
- Support and adherence to the change management and release management deployment activities
- Support and monitor daily, weekly, monthly, quarterly, and annual reports to include verifying the accuracy of underlying data
- Proactively ensure the accuracy and integrity of reports through an automated verification process

Deliverable:

A. Change Management Documentation
B. Installation Documentation
C. Technical Documentation Updates

5.14.7 Data Estate and BI Infrastructure Management (OPTIONAL)

The Contractor shall provide operation and maintenance support on the Data Estate and BI solution infrastructure. The Contractor shall plan and anticipate increase in data volume and user transactions for Data Estate and iFAMS BI.

VA anticipates technical and hardware upgrades shall be required throughout the life of this effort. The Contractor shall support upgrades as described in the below tasks; however, all hardware associated with any upgrades will be provided by the VA.

The Contractor shall provide:

- System administration support for Oracle Golden Gate for Big Data
- System administration support for Microsoft Synapse and associated tools
- System administration support for Power Platform activities that support the Data Estate and BI solution
- System administration and support for, the scalability and performance enhancements of the Data Estate and BI solution
- Support, documentation, and participation for and within Disaster Recovery activities
- Support for, documentation for, and participation in Authority to Operate (ATO) and Continuity of Operations (COOP) activities. Documentation is to align with the requirements outlined in the eMASS Authorization Requirements SOP Guide.

- Reconciliation and system assurance activities to ensure data replication and ETL functionality quality
- Participation, and support of deployment activities of Data Estate customers
- Technical Documentation creation and management of system administration activities
- Infrastructure installing, monitoring, patching and maintenance activities in line with the VA DevSecOps policies and procedures
- Maintenance of all datasets within environment

Deliverable:

A. ATO Documentation
B. Disaster Recovery artifacts
C. Operating Procedures guides
D. Architecture Plan
E. Systems Inventory
F. Wiki maintenance of operations and procedures
G. Performance metrics

5.14.8 Data Estate and BI Training (OPTIONAL)

The Contractor shall provide support for two different training activities: customer training and knowledge transfer for both the Data Estate and BI Reporting.

5.15 TRANSITION SUPPORT (OPTIONAL TASK)

The Contractor shall be responsible to provide all resources necessary for the smooth transition of work to or from other vendors related to this PWS. If issued multiple options, the Contractor shall make every effort to consolidate transition functions.

Transition Services tasks include at a minimum planning; training of Government personnel; developing processes, procedures, and system documentation; and migration activities.

5.15.1 Outgoing Transition Management

The Contractor shall deliver an outgoing Transition Management Plan to the Government for approval to ensure the smooth transition to a successor Contractor. The Contractor shall transition the required services of the task order without interruption to the Government. The Contractor shall implement its Transition Management Plan upon request by the Government. However, the Government may require changes to the plan after submission. Compliance with any Government requested changes or revisions to the plan are due within 30 calendar days of the request, or sooner as negotiated.

Deliverable:

A. Transition Management Plan

5.15.2 Hosting Transition and Migration Planning (OPTIONAL)

The Contractor shall develop a Transition Plan and other deliverables in support of the transition of the hosting infrastructure from the system integration provider to Federal and contract information technology staff, henceforth referred to as “IT Staff”. . The Transition Plan shall clearly identify and define the procurement, installation, configuration, and migration responsibilities and other dependencies for the Contractor and other vendors. The Transition Plan shall include coordination with application managers, system administrators, and database administrators to ensure adequate knowledge transfer testing prior to cutover. In addition, the Transition Plan shall include planning for database migration, account for potential issues relating to the size of the database, identify challenges and risks, identify resources, and prevent any unplanned outages of production application or services. The Contractor shall support the transition tasks listed below:

- Provide access to servers, databases, Azure, and applications including but not limited to Momentum, JBOSS, Control-M, OpenShift, webMethods, Golden Gate, and any others required for supporting iFAMS
- Document baseline integrations between Momentum and other government agencies sufficient for support tasks to be maintained by IT Staff
- Document tier 2 support tasks to be provided by IT Staff and tier 3 tasks to be performed by the product vendor
- Updated physical and logical architecture diagrams documenting servers, components, and integrations for all environments
- Training on patching, maintenance, release, deployments, data fixes, cycle processing and other routine administrative tasks
- IT Staff Acceptance of documentation and training
- Release Readiness Review
- Full support of all iFAMS environments by IT Staff including production

A project manager shall be responsible for overseeing all aspects of the approved plan. The Contractor’s Project Manager shall be responsible for managing the following transition activities:

- Meeting transition milestones by completing the infrastructure preparation and helping to integrate both the VA WAN and connect the new facility LAN to the current hosted environment
- Providing personnel to complete systems configuration and testing within the data center environment
- Meeting with VA representatives, immediately following request, to review the transition milestones and schedule, and other material required to support the

Transition Plan. VA representatives include the system owners, application and database administrators, and security officers

- Maintaining an action item list or issue log and developing risk mitigation strategies to prevent schedule delays; this can be integrated with existing VA issue and risk tracking or tracked independently based on agreement with VA leadership
- Providing weekly status reports and meet regularly (bi-weekly minimum) with VA management and staff to address transition schedules, issues, and action items
- Develop and implement knowledge transfer and transition procedures to ensure that Government technical staff understands all components of the business and technical environment

The Contractor will continue to provide operational support for the product at the request of the government for any functional tasks where IT Staff are unable to adequately perform independently due to staffing shortages. Contractor staffing levels during the transition period will be adjusted according to need.
g

Deliverable:

A. Transition Plan
B. Updated POM, patching plan, database SOP, system administration SOP(s)
C. Updated Architecture Diagrams
D. Weekly Status Reports
E. Training Sessions

5.15.3 Gap Planning and Analysis (OPTIONAL)

To successfully fulfill the migration and startup requirements described below, the Contractor shall perform a thorough gap planning and analysis process, as part of the pre-migration planning activities. The outcome of this process shall be the identification and documentation of existing systems bottlenecks, dependencies, constraints, and efficiencies that will be taken into consideration when designing and implementing the target infrastructure for the Momentum or related applications hosting services environment.

5.15.4 Migration and Startup (OPTIONAL)

In accordance with the approach identified in Section 5.12.2 Hosting Transition and Migration Planning above, the Contractor shall plan and execute the migration of hosted applications, middleware components, databases, and utilities installed on or associated with each hosted server instance or image, including backup and recovery scripts and schedules from the current environment to the new cloud environment. Archive tapes from the current environment will be transferred to the control of the Contractor and migrated as necessary to maintain the ability to restore. The Contractor shall be

responsible for making any changes to system and 3rd party software configuration, scripts and utilities, network, or any other item required for proper operation of Momentum or related applications in the new environment. Testing shall include the execution of load and performance test scripts via the Silk Performer tool (or an equivalent) to ensure adequate performance and to establish benchmark performance metrics for the application performance service level requirements. As required, VA database administrators will work to keep migrated data in the new environment in sync with production data prior to final cutover.

The migrated systems and environment will be subject to a System Test and Evaluation (ST&E) and require independent Assessment and Authorization (A&A) and SAS-70 Type II certification prior to full system operations. Continuity of Operations (COOP)/Disaster Recovery procedures must be tested prior to go-live. The Contractor shall leverage common controls, policies, and procedures to the maximum extent possible in support of system A&A.

The Contractor shall support the needs of component, integration, Quality Assurance (QA) and performance testing to ensure that the implemented system meets or exceeds all requirements and specifications set forth. This includes lower-level environments (development, system test and QA) availability and accessibility to VA, its interface partners and end users.

The Contractor shall work with VA personnel to measure the accountability and reliability of systems and components to ensure compatibility with the requirements and establish the system functional baseline. The Contractor shall work with VA personnel on the regression testing to ensure all components are operating and performing at an acceptable level. The Contractor shall provide a responsibility matrix and assumptions around the testing effort between the Contractor and Government personnel.

Additionally, the Contractor shall perform integration testing and performance testing. The Contractor shall support the continuity of essential services such as configuration management and IT security. The Contractor shall work with VA to develop transition/support plans and provide comprehensive Go-Live support. The Contractor shall be responsible for supporting the additional computational capabilities received by VA from external sources.

Additionally, the Contractor shall:

- Replicate data to a backup facility
- Conduct a disaster recovery test and provide a test repost based on established SLA in Attachment B.
- Demonstrate business functionality at the disaster recovery site

Deliverable:

A. Integration and Performance Testing Report

5.16 STAKEHOLDER SUPPORT (OPTIONAL)

This optional task may be exercised one-time, multiple times and from time to time during the Base and Option Period of Performance.

The Contractor shall provide program support to FMBT and iFAMS's Stakeholders including but not limited to Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA), and other VA Staff and Program Offices. The Contractor shall perform all activities and deliverables for FMBT Stakeholders as listed under the following tasks of this PWS:

- Section 5.4 Business Process Validation Sessions
- Section 5.7 Accounting Classification Structure
- Section 5.8 Training

5.17 SYSTEM REQUIREMENTS

The system shall adhere to GSA's Federal Integrated Business Framework (FIBF), Contract Writing System Information https://ussm.gsa.gov/fibf-cw/ and meet additional requirements, including but not limited to the following:

5.17.1 Acquisition Lifecycle Functionality

The system shall support, include, or allow for acquisition lifecycle functionality of VA acquisitions and acquisition business processes, including, but not limited to the following:

- Bi-lateral eSignature functionality
- Milestone functionality to support acquisition lifecycle milestone management, including but not limited: the ability to apply multiple milestones to a central contract file, post-award milestones, apply duplicate milestones plans without overwriting prior plan historical data, ability to associate a milestone plan to a specific modification transaction within the CCF, require the selection of a milestone template when a CCF is created, and retroactively evaluate milestones for completion.
- Document preview generation
- Unique Procurement Instrument Identifier (PIID) data elements identified in FAR subpart 4.16 for solicitations, contracts, agreements, and orders, to include the

ability to manually generate the PIID as necessary following the procedures set forth in VAAM M804.1603

- FAR and VAAR clause and provision management
- Configurable workflow management and document review/concurrence to support organizational business needs
- Compliant with FAR 4.805 for storage, handling, and disposing of contract files, retention of contracts and related documents based on National Archives and Records Administration (NARA) General Records Schedule
- Contract file creation for accessing, storing, and managing contract documents
- Access to GSAR clauses and provisions for use in applicable pre-award, award, post-award, and closeout activities related to VA's Federal Supply Schedule (FSS) contracts
- Display trade-ins as a negative dollar amount
- Full acquisition lifecycle functionality necessary to support VA acquisitions and acquisition business processes, including but not limited to:
    - Pre-award
        - announcement, request for information, solicitation and amendment creation, including contract line-item number (CLIN) and sub line-item number (SLIN), office addresses, period of performance dates, delivery instances, terms and conditions, and other key data points
        - compliant with establishing line items (4.1003), subline items (4.1004), and the data elements required (4.1005), solicitation line item and provisions (4.1007 & 4.1008)
        - upload attachments to the solicitation and solicitation amendment
        - route the solicitation and solicitation amendment for review
        - accomplish clause and provision selection using clause recommendation logic
        - include current FAR and VAAR clauses and provisions
        - include enterprise and agency terms and conditions
        - solicitation review to identify language that is duplicative, contradictory, missing, or potential protest risks using natural language processing
        - conformed solicitation view to include amendments
        - post open and continuous solicitations
        - streamline and flexible offer evaluation workflow process
        - phase zero collaborative planning tool, with real-time, simultaneous document creation/editing functionality, document management, including version history, and the ability to file and tag final documents in the Central Contract File and/or as an Attachment to

the Announcement, Request for Information, Solicitation, and Award
- creation of planning documents

- Award
  - award creation, including contract line-item number (CLIN) and sub line-item number (SLIN), office addresses, period of performance dates, delivery instances, terms and conditions, and other key data points
  - upload attachments to the award
  - route the award for review
  - accomplish clause selection using clause recommendation logic
  - include current FAR and VAAR clauses
  - include enterprise and agency terms and conditions
  - multiple award contracts (MACs), blanket purchase agreements (BPAs), blanket ordering agreements (BOAs), and government-wide acquisition contracts (GWACs)
  - system available award review to identify language that is duplicative, contradictory, missing, or potential protest risks using natural language processing
- Post-award
  - modification creation, including contract line-item number (CLIN) and sub line-item number (SLIN), office addresses, period of performance dates, delivery instances, terms and conditions, and other key data points
  - upload attachments to the modification
  - route the modification for review
  - accomplish clause selection using clause recommendation logic
  - include current FAR and VAAR clauses
  - include enterprise and agency terms and conditions
  - concurrent modifications
  - award surveillance
  - task order and delivery order processing
  - award tracking against established ceilings
  - system available modification review to identify language that is duplicative, contradictory, missing, or potential protest risks using natural language processing
  - manage MACs, BPAs, BOAs, and GWACs
  - ability to view certified invoice payments
  - conformed view to include modifications
  - mass modifications

- Closeout functions
  - closeout creation, including contract line-item number (CLIN) and sub line-item number (SLIN), office addresses, period of performance dates, delivery instances, terms and conditions, and other key data points
  - route the closeout for review
  - accomplish clause selection using clause recommendation logic
  - include current FAR and VAAR clauses
  - include enterprise and agency terms and conditions
  - system available closeout review to identify language that is duplicative, contradictory, missing, or potential protest risks using natural language processing
  - closed out status
- Real time checks of availability of funds commitment and obligation of funds against budget approvals

5.17.2 Data Integrity and Compliance

- The system shall be compliant and up to date with requirements set forth in the Federal Acquisition Regulation (FAR).
- The system shall be compliant and up to date with requirements set forth in the Veterans Affairs Acquisition Regulation (VAAR) and Veterans Affairs Acquisition Manual (VAAM).
- The system shall provide users with the ability to manually add deviations or updates to FAR clauses (e.g., from a common work area or similar functionality) until they have been permanently added to the system.
- The system shall include validations and checks to ensure valid data is entered and is appropriate to the specific field.
- The system shall meet all applicable federal security standards (e.g. Authority to Operation, NIST, FISMA, etc. as applicable).

5.17.3 Integrations

- The system shall successfully interface with external systems, such as, but not limited to: FPDS, SAM.gov, Invoice Payment Processing System (IPPS), Automated Acquisition Management Solution (AAMS), Budget Tracking Tool (BTT).
- The system shall validate funds availability for invoice payments in real-time and display accurate rejection reason in real-time.
- The system shall interface with the National Acquisition Center Contract Management (NAC-CM) and Denver Logistic Service (DLS), Remote Order Entry System (ROES).

- Federal Procurement Data System (FPDS)
    - The system shall provide bi-directional data transmission.
    - The system shall successfully create and finalize the Contract Award Record (CAR).
    - The system shall display an error message when finalization/approval failures occur.
- System for Award Management (SAM.gov)
    - The system shall include all active SAM.gov vendors.
    - The system shall provide bi-directional data transmission.
    - The system shall successfully create, publish, and amend all announcement types and attachments.
    - The system shall display an error message when there is a publishing error.
- Budget Tracking Tool (BTT)
    - The system shall provide bi-directional data transmission.
    - The system shall receive planning actions and associated data from BTT when ready for submission.
    - The system shall pass data back to BTT such as status, milestones, etc.

5.17.4 Reporting

- The system shall enable access to data and self-service reporting for the ability to develop custom reports.
    - The system shall provide user friendly ad-hoc reporting capabilities, with the ability to utilize all available acquisition data fields, that do not require backend SQL knowledge.
- The system shall include standard acquisition reports that include all necessary acquisition data fields needed for acquisition processes and shall provide export capabilities to Excel or PDF.
    - These standard acquisition reports shall be validated and accepted by the Enterprise Acquisition community.
- The system shall enable users to generate reports with the desired data from a single source.
- The system shall provide the ability to create/update/delete report subscriptions, for one or multiple users. Reports shall be auto generated at the date/time/frequency defined by the user and sent via email to the specific VA account recipient(s) identified to receive the reports.

5.17.5 Security & Access

- The system shall provide the minimum required access to procurement sensitive data.

    - The system shall provide administrations and staff offices with *only* need-to-know access to support *their own* contract actions.
    - The system shall prevent users from having access to all local data for a given Security Organization.
    - The system shall provide contracting users with the ability to manage access to the Central Contract File (CCF), to include specific folders within the CCF.
- The system shall offer clear and well-defined user roles that are validated and approved by the enterprise acquisition community. Additionally, roles shall:
    - Provide sufficient authority for Ordering Officers to place orders against IDV contracts individually by contract number.
    - Provide sufficient Application Coordinator/Local Administrator authority to execute their job functions (i.e., change a user's email address, de-provision staff, warrant management, etc.).
    - Be assigned via a quick and simple process.
- The system shall provide organizational hierarchy, to be managed by the Application Coordinator/Local Administrator, at the organization, division, team, and manager/subordinate levels. Functionality shall allow Application Coordinator/Local Administrator to make dynamic, real-time changes when organizational restructuring occurs.

5.17.6 Usability

The system shall be user friendly and intuitive to enable efficient use and streamline processes, including but not limited to the following functionality:

- Dynamic Data fields
- Configurable to align with standard VA acquisition business processes
- Increase efficiency of acquisition business processes
- Minimize the number of interactions required to complete acquisition tasks
- Include a Digital Adoption Platform to assist users with system usability/functionality
- Info tags for all mandatory data fields
- Ability to conduct acquisition activities during annual fiscal closeout
- Display applicable fields only (i.e., hide inapplicable fields from acquisition user view)
- Autosave
- The system shall have error messages that are detailed, user friendly, actionable, and include steps on how to resolve the issue
- Workload management, including but not limited to: workload assignment query, tiered data reporting, workload manager view of all work (contract files, workload assignments, other inbox tasks, etc.) of a specific assignee, team, and division,

display progress percentage and status fields, prior fiscal year summaries (e.g. awards and obligations), etc. Configurable customer views

- Include all data fields necessary for acquisitions
- Identify all critical data fields as necessary/required
- Use of clear, plain language consistent with FAR-based acquisition terminology
- Version history to track changes made by users to data fields, to include what was changed and by whom
- The system shall provide automated and dynamic dashboarding capabilities to allow Local Admins to develop/update/delete and display data/metrics within the system for specific users or groups of users. Once created or updated, the dashboards shall automatically and dynamically pull, update, and display data.

5.17.7 Support Requirements

5.17.7.1 Acquisition Sandbox Environment

- The contractor shall provide a dedicated acquisition sandbox environment which meets the following specifications:
    - Deliver 99.5% availability (except for scheduled maintenance and updates) 7am – 7pm EST during course preparation (approx. 1 week prior to a scheduled course) and course delivery.
    - Include a full-featured iFAMS experience that allows unfettered access to all functional aspects of the iFAMS acquisition lifecycle experience as configured for VA, including but not be limited to: modules, components, interfaces, and features that deliver and/or support the VA's acquisition lifecycle. (Note: This shall include all associated functionality such as requisitioning and finance, as they are intertwined with the direct acquisition lifecycle work stream.) All configurations available within the iFAMS production environment shall be available.
    - Deliver strong performance (calculated via processing and return speeds) and experience extremely limited interruptions outside of schedule maintenance windows. Performance will be satisfactory to not disrupt classes up to 500 concurrent users.
    - Not include production data.
    - Not delete, change, or purge data without coordination and consent.
    - Provide those designated by VA the ability to create, without limit, user accounts and to assign, without limit, functional permissions to user accounts. The ability to assign elevated permissions shall not be restricted.
    - Provide helpdesk support for system issues.
    - Functionality that mirrors the iFAMS production environment.

- Effectively support up to 500 concurrent users and be scalable.
- Ensure releases pushed to the iFAMS production environment are also pushed to the dedicated training environment except those releases which are mutually agreed to forgo. A release plan shall be established where advanced notice can be provided regarding upcoming releases. Such notices shall be used to determine the functional impacts to the system and the value (or lack thereof) of having the release in the dedicated training environment. All releases, updates, and maintenance shall be coordinated with the appropriate VA POC.
- During training events, VA personnel and additional designees shall be provided support in response to issues encountered with the dedicated training environment, application(s), and integrations. Reach back support during scheduled trainings shall be responded to in order of priority, but as soon as possible, with an escalation mechanism to help quickly resolve issues arising during training.
- All mutually agreed upon interfaces established for the iFAMS production environment shall also be delivered into the dedicated training environment and directed to the requisite training or test interface. This includes SAM, FPDS-NG, AAMS, IPPS, and any additional interfaces that may be identified in the future.

5.17.7.2 Acquisition Training

- The contractor shall ensure that trainers have iFAMS enterprise acquisition module knowledge, as well as operational FAR, VAAR and VA acquisition business process knowledge.
- The contractor shall have the ability to provide training for various acquisition roles and functions (e.g. contracting officer, contract specialist, application coordinator, ordering officers, etc.) upon request.

5.17.7.3 Reporting

- The contractor shall provide a streamlined, timely process to enhance existing reports and develop/configure new reports.

5.17.7.4 Security & Access

- The contractor shall ensure that, at the time of deployment, acquisition leadership is provided the opportunity to review the list of users who are given the ability to view/access acquisition data.
- The contractor shall collaborate with the program and the enterprise acquisition community to develop and receive approval for the appropriate user roles.
- The contractor shall include the enterprise acquisition community in all system-wide user provisioning, access, and security discussions.

5.17.7.5 Service Desk

- The contractor shall ensure that the service desk support team has sufficient federal and VA acquisition knowledge commiserate with each service desk Tier to ensure proposed resolutions take into consideration federal and VA acquisition regulations, policy, and acquisition business processes.

5.17.7.6 Testing

- Testing shall include validation, regression, and user acceptance of all major and minor finance and acquisition enhancements/upgrades/product releases to ensure new configuration does not impact existing configuration.
    - Testing shall ensure that configuration changes and updates do not impact existing functionality of interfaced systems.
- Testing shall include detailed test use cases covering all acquisition functionalities.
- Testing shall include test scenarios developed in collaboration with and approval from acquisition subject matter experts.
- The contractor shall identify and incorporate all business-essential processes and related interfaces, as defined by product owners, during validation sessions and user acceptance testing or equivalent procedures, to accurately present system capability. Related interfaces included but are not limited to eCMS, SAM.gov, and IPPS.
- Testing shall include all end-to-end acquisition business processes with all necessary interfaces and user administration.
- The contractor shall prioritize full Testing over demos during UAT.
- The contractor shall include end-users during the Testing cycles.
- The contractor shall include interfacing system owners during testing to confirm interface updates are being considered (e.g., EASS and IPPS)

5.17.7.6.1 Testing Environment

- Testing shall be conducted in a reliable test environment with reliable test data, servers, and adequate resources.
- The test environment shall be configured to include end-to-end acquisition business process testing.
- The test environment shall be configured to include all key interfaces (e.g., eCMS, IPPS, SAM.gov).
- The contractor shall ensure all business essential interfaces are available in the test environment.

5.17.7.6.2 Enhancements

- In coordination with Enterprise Acquisition, the Contractor shall identify, configure, test, and implement required acquisition enhancements to maintain compliance with GSA's Federal Integrated Business Framework (FIBF), Contract Writing System Information, and other federal regulation and policies related to contract writing systems, as well as necessary product releases, upgrades, bug/defect fixes, etc. to ensure continued usability and functionality of the system, to include interfaces.
- The Contractor shall provide training and training materials as necessary for new functionality or enhancements/releases/upgrades/fixes that change the use/processes of existing functionality.

6.0 GENERAL REQUIREMENTS *(PENDING)*

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OIT Technical Reference Model (VA TRM). The VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. Moreover, the VA TRM, which includes the Standards Profile and Product List, serves as a technology roadmap and tool for supporting OIT. Architecture & Engineering Services (AES) has overall responsibility for the VA TRM.

6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

<DRAFT>

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), https://www.ea.oit.va.gov/EAOIT/VA_EA/Enterprise_Technical_Architecture.asp, and

VA Identity and Access Management (IAM) approved enterprise design and integration patterns, https://www.oit.va.gov/library/recurring/edp/index.cfm. The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in VA Handbook 6510 VA Identity and Access Management, VA Handbook 0735 Homeland Security Presidential Directive 12 (HSPD-12) Program, and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-05-24, M-19-17, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-05-24 and M-19-17 can be found at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf, and https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's Master Person Index (MPI) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion-based authentication. Additional assertion implementations,

besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VIEWS 00155984, PIV Logical Access Policy Clarification https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896.

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support Internet Protocol Version 6 (IPv6) based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). IPv6 technology, in accordance with the USGv6 Program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 “USGv6 Profile” (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 “Guidelines for the Secure Deployment of IPv6” (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and dual stack (IPv6 / IPv4) operations.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative“ (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 “Secure External Connections”, and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/publication/tic-30-core-guidance-documents). Any deviations must be approved by the VA TIC 3.0 Working Group at vaoisesatic30team@va.gov.

6.1.5 STANDARD COMPUTER CONFIGURATION

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 particular client operating system being used.

6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM)

The Contractor shall support VA efforts IAW the updated Veteran Focused Integration Process (VIP) and Product Line Management (PLM). The major focus of the new VIP is on Governance and Reporting and is less prescriptive, with a focus on outcomes and continuous delivery of value. Product Line Management (PLM) is a framework that focuses on delivering functional products that provide the highest priority work to customers while delivering simplified, reliable, and practical solutions to the business, medical staff, and our Veterans. The VIP Guide is a companion guide to the PLM Playbook and can be found at: https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371 and the PLM Playbook can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946. The PLM Playbook pivots from project-centric to product-centric delivery and contains descriptive practices that focuses on outcomes. The PLM Playbook contains a set of "plays" that implement Development, Security, and Operations (DevSecOps) principles and processes such as automated development, continuous integration/continuous delivery, and release on demand. The PLM Playbook details how product lines implement Lean-Agile principles, methods, practices, and techniques through levels of maturity. VIP and PLM are the authoritative processes that IT projects must follow to ensure development and delivery of IT products.

6.1.7 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.

6.1.8 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.

6.1.9 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the ICN in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

6.1.10 SOFTWARE AND LICENSING REQUIREMENTS

<DRAFT>

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

6.2 SECURITY AND PRIVACY REQUIREMENTS

<DRAFT TBD>

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

<DRAFT TBD>

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:

<DRAFT TBD>

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☐	☐	☐
5.2	☐	☐	☐
5.3	☐	☐	☐
5.4	☐	☐	☐
5.5	☐	☐	☐
5.6	☐	☐	☐
5.7	☐	☐	☐
5.8	☐	☐	☐
5.9	☐	☐	☐
5.10	☐	☐	☐
5. 11	☐	☐	☐
5.12	☐	☐	☐
5.13	☐	☐	☐
5.14	☐	☐	☐
5.15	☐	☐	☐
5.16	☐	☐	☐
5.17	☐	☐	☐

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.

6.2.2 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

6.3 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).

6.4 PERFORMANCE METRICS

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

<DRAFT TBD>

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 5. Incorporates “ease of use” Human Centered Design principles in any software developed.	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate to perform tasks required 2. Personnel possess necessary knowledge, skills, and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion***<DRAFT TBD>*** A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.5 FACILITY/RESOURCE PROVISIONS

<DRAFT TBD>

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

<DRAFT TBD>

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 Progress Status Report as required by PWS. For purposes of 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

<N/A>

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 being 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 Contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 (Appendix C updated April 22, 2024) by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract, or order. 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/. If you do not have a TMS 2.0 profile, go to https://www.tms.va.gov/SecureAuth35/ 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's Web Governance if the Contractor's work includes building and maintaining VA's digital presence. This pertains, but is not limited to: websites, social media, 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

VA Web Governance website can be found at Home - VA Web Governance.

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

(Three standards listed in Section A3.1 below [E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines), E204 Functional Performance Criteria, and E208 Support Documentation and Services] always apply to the evaluation of ICT, and should remain marked as "x". The requiring activity should un-mark any of the other remaining standards below [E206 and/or E207] that do not apply to this effort. The Accessibility Requirements Tool (ART) is a web-based application that will help the requiring activity determine the Section 508 standards that apply to their specific acquisition. The ART tool is located at Accessibility Requirements Tool (ART)***.)***

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

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: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508

Standards and 255 Guidelines will be supplied upon request, or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

The Contractor shall comply with section 508 of the Rehabilitation Act of 1973 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 following technical standards:

- ☒ 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

E201 Application

E201.1 Scope. ICT that is procured, developed, maintained, or used by agencies shall conform to the Revised 508 Standards.

E205 Electronic Content

E205.1 General. Electronic content shall comply with E205.

E205.2 Public Facing. Electronic content that is public facing shall conform to the accessibility requirements specified in E205.4.

E205.3 Agency Official Communication. Electronic content that is not public facing shall conform to the accessibility requirements specified in E205.4 when such content constitutes official business and is communicated by an agency through one or more of the following:

1. A. An emergency notification;
2. B. An initial or final decision adjudicating an administrative claim or proceeding;
3. C. An internal or external program or policy announcement;
4. D. A notice of benefits, program eligibility, employment opportunity, or personnel action;
5. E. A formal acknowledgement of receipt;

6. F. A survey questionnaire;
7. G. A template or form;
8. H. Educational or training materials; or
9. I. Intranet content designed as a Web page.

E205.4 Accessibility Standard (WCAG 2.0). Electronic content shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (Incorporated by reference, see 702.10.1).

E206 Hardware

E206.1 General. Where components of ICT are hardware and transmit information or have a user interface, such components shall conform to the requirements in Chapter 4.

E207 Software

E207.1 General. Where components of ICT are software and transmit information or have a user interface, such components shall conform to E207 and the requirements in Chapter 5

Exception from E207.1 General: Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to the requirements in Chapter 5.

E207.2 WCAG Conformance. User interface components, as well as the content of platforms and applications, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

Exceptions from E207.2 WCAG Conformance:

10. Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to E207.2.
11. Non-web software shall not be required to conform to the following four Success Criteria in WCAG 2.0: 2.4.1 Bypass Blocks; 2.4.5 Multiple Ways; 3.2.3 Consistent Navigation; and 3.2.4 Consistent Identification.
12. Non-Web software shall not be required to conform to Conformance Requirement 3 Complete Processes in WCAG 2.0.

E207.3 Complete Process for Non-Web Software Where non-Web software requires multiple steps to accomplish an activity, all software related to the activity to be accomplished shall conform to WCAG 2.0 as specified in E207.2.

E208 Support Documentation and Services

E208.1 General. Where an agency provides support documentation or services for ICT, such documentation and services shall conform to the requirements in Chapter 6.

E301 General

E301.1 Scope. The requirements of Chapter 3 shall apply to ICT where required by 508 Chapter 2 (Scoping Requirements), 255 Chapter 2 (Scoping Requirements), and where otherwise referenced in any other chapter of the Revised 508 Standards or Revised 255 Guidelines.

E302 Functional Performance Criteria

302.1 Without Vision. Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that does not require user vision.

302.2 With Limited Vision. Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.

302.3 Without Perception of Color. Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.

302.4 Without Hearing. Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.

302.5 With Limited Hearing. Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.

302.6 Without Speech. Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.

302.7 With Limited Manipulation. Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.

302.8 With Limited Reach and Strength. Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.

302.9 With Limited Language, Cognitive, and Learning Abilities. ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier.

503 Applications

503.1 General. Applications shall conform to 503.

503.2 User Preferences. Applications shall permit user preferences from platform settings for color, contrast, font type, font size, and focus cursor.

Exception from E503.2 User Preferences: Applications that are designed to be isolated from their underlying platform software, including Web applications, shall not be required to conform to 503.2.

503.3 Alternative User Interfaces. Where an application provides an alternative user interface that functions as assistive technology, the application shall use platform and other industry standard accessibility services.

503.4 User Controls for Captions and Audio Description Where ICT displays video with synchronized audio, ICT shall provide user controls for closed captions and audio descriptions conforming to 503.4.

503.4.1 Caption Controls Where user controls are provided for volume adjustment, ICT shall provide user controls for the selection of captions at the same menu level as the user controls for volume or program selection.

503.4.2 Audio Description Controls. Where user controls are provided for program selection, ICT shall provide user controls for the selection of audio descriptions at the same menu level as the user controls for volume or program selection.

602 Support Documentation

602.1 General. Documentation that supports the use of ICT shall conform to 602.

602.2 Accessibility and Compatibility Features. Documentation shall list and explain how to use the accessibility and compatibility features required by Chapters 4 and 5. Documentation shall include accessibility features that are built-in and accessibility features that provide compatibility with assistive technology.

602.3 Electronic Support Documentation. Documentation in electronic format, including Web-based self-service support, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

602.4 Alternate Formats for Non-Electronic Support Documentation. Where support documentation is only provided in non-electronic formats, alternate formats usable by individuals with disabilities shall be provided upon request.

603 Support Services

603.1 General. ICT support services including, but not limited to, help desks, call centers, training services, and automated self-service technical support, shall conform to 603.

603.2 Information on Accessibility and Compatibility Features. ICT support services shall include information on the accessibility and compatibility features required by 602.2.

603.3 Accommodation of Communication Needs. Support services shall be provided directly to the user or through a referral to a point of contact. Such ICT support services shall accommodate the communication needs of individuals with disabilities.

A3.1.1 Instructions to Contractor:

The Contractor shall provide an Accessibility Conformance Report (ACR) for each commercially available Information and Communication Technology (ICT) item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template Version 2.1 or later, located at https://www.itic.org/policy/accessibility/vpat. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. Address each standard individually and with specificity, and clarify whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. Provide a description of the evaluation methods used to support Section 508 conformance claims. The Government reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

The Contractor Shall:

1. Describe how to incorporate universal design principles to ensure ICT products or services are designed to support disabled users.
2. Describe plans for features that do not fully conform to the Section 508 Standards.
3. Describe "typical" user scenarios and tasks, including individuals with disabilities, to ensure fair and accurate accessibility testing of the ICT product or service being offered.

Acceptance Criteria:

1. Prior to acceptance, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent an inaccurate level of conformance than what is actually delivered to the agency, the government shall, at its option, require the offeror to remediate the delivered item to align with the required Section 508 conformance claims prior to acceptance.

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 wear visible identification at all times 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 of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by 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.

A6.0 Information Technology Using Sustainable Products and Services

(Reference: 52.223-23, Sustainable Products and Services. If the requiring activity is procuring the following types of Information Technology Products delivered or furnished for Government use or for Contractor use at a Federally controlled facility (applicable to the work being performed and/or the solution requires) the requiring activity must include the products that fall into the categories of EPEAT, Energy Star, and FEMP within the requirements specifications for the products within this PWS that fall into the respective categories to indicate applicability to this contract. Please see the GSA Sustainable Facilities Tool website, and the categories within it for guidance and applicability determination of the products/services being acquired.

If the products/services do not involve the acquisition of products that fall into the EPEAT, Energy Star, or FEMP categories at all, this entire section can be indicated as “Not Applicable” and any references to ecolabels can be removed from the product requirement specifications within the PWS, If after consulting with the Contracting Officer and Contract Specialist, the requiring activity determines there is no EPEAT, Energy Star, or FEMP products that meet VA requirements and a written justification, or an exception, or an exemption has

been provided, this entire section can be indicated as "Not Applicable" and any references to ecolabels can be indicated as N/A within the product requirement specifications within the PWS.

Overarching Website:

The Green Procurement Compilation (GPC) website, Green Procurement Compilation - GSA Sustainable Facilities Tool (sftool.gov), provides a comprehensive list of sustainable Products and Services by Category, to include sustainable acquisition guidance. The Requiring Activity should review the GPC website to help determine which purchasing programs apply to a specific product or service (e.g., within the GPC website, find the "Office Equipment and Electronics" category, for instance, then drill down within the various Product Types in that category (e.g. Combination Units/Multi-Function Devices, Computers, Data Center Storage, etc.,) to determine the related Certification, Designation, and/or Ecolabel requirements for them, and then can also drill down to find various brand and model numbers of products that meet them, as necessary)

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, and products and services that meet EPA Recommendations of Specifications, Standards, and Ecolabels in effect as of October 2023 (e.g. Electronic Product Environmental Assessment Tool (EPEAT) registered products) in providing information technology products and/or services. The Green Procurement Compilation (GPC) website available at Green Procurement Compilation - GSA Sustainable Facilities Tool (sftool.gov) provides a comprehensive list of sustainable products and services and sustainable acquisition guidance.

The Contractor shall provide products that meet the definition of sustainable products and services if the products are delivered to the Government; furnished by the Contractor for use by the Government, incorporated into the construction of a public building or public work, or acquired by the Contractor for use in performing services under a Government contract where the cost of the products is a direct cost to a Government contract (versus costs which are normally applied to a contractor's general and administrative expenses or indirect costs).

Specifically, the Contractor shall provide sustainable products under this contract in accordance with FAR 52.223-23. The applicable products with their associated certification, designation, and/or ecolabel (e.g. Energy Star, FEMP, and/or EPEAT) are identified within the product specifications in this PWS. The Contractor shall ensure proposed products meet the certification(s) / designation(s) / ecolabel(s) specified at the time of submission of proposals and at the time of award.


DRAFT

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

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

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

(All Sections in this Addendum B must be reviewed to determine applicability to the requirements of the effort within the PWS. Any Sections (B1 through B14) which DO NOT apply should be removed from this Addendum B. Requiring Activities should see the inclusion instructions prior to each Section and remove any full Sections that DO NOT apply (indicating "N/A" underneath the Section Heading(s)). The language within these Sections MUST NOT be modified, except the removal of instructional text provided prior to each Section)

B1. GENERAL

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

B2. VA INFORMATION CUSTODIAL LANGUAGE

(This entire section applies to all acquisitions requiring any Information Security and Privacy language)

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter "contract") unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General. The primary clause used to define computer software license (not data/intellectual property first produced under this Contractor or order) is FAR 52.227-19, Commercial Computer Software License.

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

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

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of Contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The Contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to Contractor and Subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

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

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

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

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

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

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

k. Notwithstanding the provision above, the Contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality-assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the Contractor is in receipt of a court order or other requests for the above-mentioned information, the Contractor shall immediately refer such court order or other requests to the VA CO for response.

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

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

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

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The Contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the Contractor shall send via a trackable method (USPS, UPS, FedEx,

etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the Contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

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

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

(This section applies when any person requires access to information made available to the Contractor by VA for the performance or administration of this contract or information developed by the Contractor in performance or administration of the contract)

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

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

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

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

e. The Contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
    (1) Contractor/Subcontractor personnel no longer has a need for access to VA information or VA information systems.

    (2) Contractor/Subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

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

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

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

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

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

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

B4. TRAINING

(This entire section applies to all acquisitions which include section 3)

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

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

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

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

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

c. Failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the required training is complete.

B5. SECURITY INCIDENT INVESTIGATION

(This entire section applies to all acquisitions requiring any Information Security and Privacy language)

a. The Contractor, Subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711).

The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the Contractor, Subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:

(1) The date and time (or approximation of) the Security Incident occurred.

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

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

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

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

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

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

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

e. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

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

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

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

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

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

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

c. VA IT Contractors, Subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, Risk Management Framework for Cloud Computing Services and Information Security Knowledge Service specifications in delivered IT systems/solutions, products

and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the Contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

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

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

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

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

baseline needs to be created, the Contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository,

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

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

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

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

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

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

n. When the Contractor is responsible for operations or maintenance of the systems, the Contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as

Microsoft OS patches or Adobe Acrobat), the Contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

(This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (cloud and non-cloud) hosted, operated, maintained, or used on behalf of VA at non-VA facilities)

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

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

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

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned

Contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).

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

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

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

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

i. The Contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs

to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.

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

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

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

(This entire section applies whenever section 6 or 7 is included)

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

b. Any audits or tests of the Contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact Contractor operations; (b):

interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the Contractor uses to destroy, maintain, receive, retain, or use VA information.

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

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

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

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

(This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included)

a. The Contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

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

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

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

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

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

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

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

B10. VIRUSES, FIRMWARE, AND MALWARE

(This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included)

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

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

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

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

(1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA’s information networks, computer systems and information systems; and
(2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

B11. CRYPTOGRAPHIC REQUIREMENT

(This entire section applies whenever the acquisition includes section 6 or 7 is included)

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

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

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

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

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

B12. PATCHING GOVERNANCE

(This entire section applies whenever the acquisition includes section 7 is included)

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

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

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

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

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

d. The Contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

B13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING)

(This entire section applies when the acquisition includes one or more Medical Device, Special Purpose System or Research Scientific Computing Device. If appropriate, ensure selected clauses from section 6 or 7 and 8 through 12 are included)

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

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

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

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

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

f. The Contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting

application may be used when the Contractor cannot install an anti-virus / anti-malware application.

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

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

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

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

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

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

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

B14. DATA CENTER PROVISIONS

(This entire section applies whenever the acquisition requires an interconnection to/from the VA network to/from a non-VA location)

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

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

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

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

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

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