PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Infrastructure Operations (IO) - Enterprise Service Management (ESM)

Enterprise Resource Planning (ERP)
Date: June 26, 2026
VA-26-000769
PWS Version Number: 1.0

DRAFT

Contents

1.0 BACKGROUND 5
2.0 APPLICABLE DOCUMENTS 5
3.0 SCOPE OF WORK 9
4.0 PERFORMANCE DETAILS 10
4.1 PERFORMANCE PERIOD 10
4.2 PLACE OF PERFORMANCE 11
4.3 TRAVEL 11
5.0 SPECIFIC TASKS AND DELIVERABLES 11
5.1 PROJECT MANAGEMENT 11
5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN 11
5.1.2 REPORTING REQUIREMENTS 11
5.2 ENTERPRISE SERVICE INTEGRATION, LICENSING, OPERATIONS, AND ACCOUNTABILITY MODEL 12
5.2.1 ENTERPRISE OPERATIONAL OUTCOME REQUIREMENTS 13
5.2.2 ENTERPRISE DELIVERY MODEL 14
5.2.3 ENTERPRISE LICENSING ACCOUNTABILITY AND TRANSPARENCY 15
5.2.4 ENTERPRISE OPERATIONAL ACCOUNTABILITY 17
5.2.5 PLATFORM OPERATIONS, SUSTAINMENT, AND MODERNIZATION... 19
5.2.6 CONTINUOUS SERVICE IMPROVEMENT AND BUSINESS VALUE REALIZATION 20
5.2.7 ENTERPRISE AVAILABILITY AND OPERATIONAL CONTINUITY 22
5.2.8 INCIDENT RESPONSE AND SERVICE RESTORATION 24
5.2.9 CHANGE , RELEASE, AND MODERNIZATION PERFORMANCE 25
5.2.10 INTEGRATION RELIABILITY AND DATA INTEGRITY 26
5.2.11 SECURITY AND OPERATIONAL RESILIENCE 27
5.2.12 USER EXPERIENCE, ADOPTION, AND SERVICE EFFICIENCY 29
5.2.13 SYSTEM INTEGRATOR TRANSITION-IN SERVICES 30
5.3 ENTERPRISE RESOURCE PLANNING PLATFORM REQUIREMENTS 31
5.3.1 ITSM 32
5.3.2 ITAM 34
5.3.3 ITOM 36
5.3.4 ITBM 37
5.3.5 DIGITAL WORKPLACE 39
5.3.6 CSM 40
5.3.7 SecOps 41
5.3.8 INTEGRATED RISK MANAGEMENT 42
5.3.9 INTEGRATION CENTER 44
5.3.10 REPORTING AND ANALYTICS 46
5.3.11 PLATFORM TOOLS 48
5.3.12 MOBILE 54
5.3.13 PRODUCTION INSTANCES 55
5.3.14 NON-PRODUCTION INSTANCES 57
5.3.15 PLATFORM PERFORMANCE TESTING INSTANCE 58
5.4 TRAINING 59
5.5 OPTION PERIOD ONE - FOUR 60

5.6 PLATFORM TRANSITION IN – TOOL REQUIREMENTS (OPTIONAL TASK 1) 60
5.6.1 IMPLEMENT CURRENT FUNCTIONALITY 61
5.6.2 MIGRATION FROM SERVICENOW 63
5.6.3 FedRAMP AUTHORIZED AND VA AUTHORIZED 63
5.7 ENTERPRISE ASSET MANAGEMENT (OPTIONAL TASK 2) 64
5.8 ENTERPRISE HRSD (OPTIONAL TASK 3) 66
5.9 ARTIFICIAL INTELLIGENCE (OPTIONAL TASK 4) 66
5.9.1 GENERATIVE AI CAPABILITIES 67
5.9.2 AGENTIC AI CAPABILITIES 67
5.9.3 COMBINED GENERATIVE AI AND AGENTIC AI USE CASES 68
5.10 DATA LAKE SOLUTION (OPTIONAL TASK 5) 68
5.11 GREENFIELD SOLUTION - Out of the Box (OPTIONAL TASK 6) 70
5.12 VENDOR RISK MANAGEMENT (VRM) (OPTIONAL TASK 7) 72
5.13 FIELD SERVICE MANAGEMENT (OPTIONAL TASK 8) 73
5.14 Cloud Cost Management & FINANCIAL operations (finops) (optional task 9) 74
5.15 DISTRIBUTED DEVELOPMENT AND SUSTAINMENT (OPTIONAL Task 10) 77
5.15.1 ORDERING AND AUTHORIZATION MODEL 78
5.15.2 OUTCOME-BASED SCOPING AND SOLUTION ASSESSMENT 79
5.15.3 SCOPE DEFINITION AND WORK PACKAGE REQUIREMENTS 80
5.15.4 STANDARDIZED PRICING AND CONSUMPTION MODEL 81
5.15.5 ENTERPRISE DEMAND MANAGEMENT AND FORECASTING 83
5.15.6 ENTERPRISE ARCHITECTURE, REUSE, AND STANDARDIZATION 84
5.15.7 DELIVERY ACCOUNTABILITY AND OPERATIONAL READINESS 85
5.15.8 SUSTAINMENT AND LIFECYCLE ACCOUNTABILITY 86
5.15.9 PERFORMANCE OUTCOMES AND KEY PERFORMANCE INDICATORS 87
5.16 TRANSITION OUT (OPTIONAL TASK 11) 88
6.0 GENERAL REQUIREMENTS 90
6.1 ENTERPRISE AND IT FRAMEWORK 90
6.1.1 VA TECHNICAL REFERENCE MODEL 90
6.1.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS 90
6.1.3 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 90
6.1.4 INTERNET PROTOCOL VERSION 6 (IPv6) 91
6.1.5 TRUSTED INTERNET CONNECTION (TIC) 92
6.1.6 STANDARD COMPUTER CONFIGURATION 92
6.1.7 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM) 93
6.1.8 PROCESS ASSET LIBRARY (PAL) 93
6.1.9 AUTHORITATIVE DATA SOURCES 94
6.1.10 SOCIAL SECURITY NUMBER (SSN) REDUCTION 95
6.1.11 SOFTWARE AND LICENSING REQUIREMENTS 95
6.1.12 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS 95

6.1.12.1 AI SYSTEM/LLM DEVELOPMENT AND OPERATION DOCUMENTATION REQUIREMENTS 97
6.1.12.2 MONITORING, REPORTING, AND CORRECTIVE ACTION 98
6.1.12.3 AI MODEL UPDATES AND CHANGE DISCLOSURES 98
6.1.13 SOURCE CODE HARMONIZATION AND REUSE IN INFORMATION TECHNOLOGY (SHARE IT Act) 99
6.2 SECURITY AND PRIVACY REQUIREMENTS 99
6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 99
6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 100
6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 102
6.4 PERFORMANCE METRICS 102
6.5 FACILITY/RESOURCE PROVISIONS 103
6.6 GOVERNMENT FURNISHED PROPERTY 104
6.7 SHIPMENT OF HARDWARE OR EQUIPMENT 104
ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED 105
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE 110

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information and Technology (OIT), Infrastructure Operations (IO) Enterprise Service Management (ESM) requires the acquisition of cloud-based Enterprise Resource Planning (ERP) solution delivered via a multi-instance Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) subscription model. The Government requires a fully integrated enterprise operating model in which the Contractor served as Enterprise System Integrator, is accountable for the service delivery, performance, reliability, maintainability, scalability, supportability, and continuous improvement of the enterprise IT Service Management platform and associated enterprise services.

This requirement supports the VA mission to enhance IT service delivery, strengthen operational efficiency, and advance digital transformation across the enterprise. The required solution must provide enterprise-wide integration and functionality consistent with leading ERP in the marketplace

VA OIT currently leverages a SaaS platform to manage critical enterprise operational practices, including enterprise service desk operations, incident and event triage, request fulfillment, change enablement, and problem resolution. Additionally, the platform supports application provisioning, clinician support, and telehealth availability. The SaaS platform is central to maintaining uptime for essential systems, including Veterans Health Information Systems and Technology Architecture (VistA) and the new Oralce/Cerner Electronic Health Record Management (EHRM) platform.

As demand increases for real-time support, automation, cybersecurity compliance, and adaptability to evolving legislative and policy requirements, VA requires acquisition of a next-generation ERP solution with capabilities that meet or exceed industry standards for federal environments. This solution must span across IT Service Management (ITSM), IT Asset Management (ITAM), IT Operations Management (ITOM), IT Business Management (ITBM), Human Resource Service Delivery (HRSD), and other service domains.

2.0 APPLICABLE DOCUMENTS

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

1. “Federal Information Security Modernization Act of 2014”
2. Federal Information Processing Standards (FIPS) Publication 140-3, “Security Requirements for Cryptographic Modules”, March 22, 2019
3. FIPS Pub 199. “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
4. FIPS Pub 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
5. FIPS Pub 201-3, “Personal Identity Verification of Federal Employees and Contractors,” January 2022
6. 10 U.S.C. § 2224, "Defense Information Assurance Program", as amended
7. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”

8. Public Law 109-461 (P.L. 109-461), Veterans Benefits, Health Care, and Information Technology Act of 2006, as amended, Title IX, Information Security Matters
9. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964", as amended
10. VA Directive 0710, "Personnel Vetting Program," September 8, 2025, https://www.va.gov/vapubs/index.cfm
11. VA Handbook 0710, "Personnel Vetting Program," September 8, 2025, https://www.va.gov/vapubs/index.cfm
12. VA Directive 6102, "Internet/Intranet Services," August 5, 2019
13. 36 C.F.R. Part 1194 "Information and Communication Technology Standards and Guidelines," as amended
14. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
15. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)", as amended
16. NIST SP 800-66 Rev. 2, "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," February 2024
17. 45 C.F.R Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 C.F.R. Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"); as amended
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, "VA Cybersecurity Program," February 24, 2021 (see VA NOTICE 24-18, dated September 27, 2024, "Update to VA Directive 6500 Cybersecurity Program", and VA Notice 25-07, dated 3/18/25, "Amending VA Directive 6500 to incorporate M-24-15")
21. VA Handbook 6500, "Risk Management Framework for VA Information Systems VA Information Security Program," February 24, 2021 (see VA Notice 25-01, dated October 15, 2024, "Update to VA Handbook 6500 Risk Management Framework for VA Information Systems VA Information Security Program", and VA Notice 25-06, dated 3/18/25, "Amending VA Directive 6500 to incorporate M-24-15", VA Notice 25-16, dated September 15, 2025, "Amending VA Handbook 6500 to Replace Enterprise Mission Assurance Support Services Tool With Office of Information Technology Governance Risk Compliance Tool, and VA Notice 25-17, dated September 22, 2025, "Rescission Of Office Of Information Security (OIS) Deputy Assistant Secretary (DAS) Memorandum – Requirements of Proper Plan of Action and Milestones (POA&M) Completion)
22. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)," June 30, 2023
23. VA Handbook 6500.6, "Contract Security," March 12, 2010 (see VA Notice 24-12, dated 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")

24. VA Handbook 6500.8, "Information System Contingency Planning," March 25, 2025
25. VA Handbook 6500.10, "Mobile Device Security Policy," February 15, 2018 (see VA NOTICE 25-10, dated June 9, 2025, "Use of Personally Owned Mobile Devices Policy Amendment of Department of Veterans Affairs Handbook 6500.10", and VA Notice 25-15, dated August 22, 2025, "Update to VA Handbook 6500.10 Mobile Device Security Policy")
26. VA Handbook 6500.11, "VA Firewall Configuration," August 22, 2017
27. OIT Process Asset Library (PAL), OIT Process Asset Library.
28. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
29. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
30. VA Directive 6510, "VA Identity, Credential and Access Management," September 3, 2024
31. VA Handbook 6510, "VA Identity, Credential and Access Management," September 27, 2024
32. VA Directive and Handbook 6513, "Secure External Connections," October 12, 2017
33. VA Directive 6300, "Records and Information Management," September 21, 2018
34. VA Handbook, 6300.1, "Records Management Procedures," March 24, 2010
35. 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
36. 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)
37. VA Directive 0735, "Homeland Security Presidential Directive 12 (HSPD-12) Program," October 26, 2015
38. VA Handbook 0735, "Homeland Security Presidential Directive 12 (HSPD-12) Program," March 24, 2014
39. 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
40. OMB Memorandum M-19-17, "Enabling Mission Delivery Through Improved Identity, Credential, and Access Management," May 21, 2019
41. OMB Memorandum, "Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation," May 23, 2008
42. Federal Identity, Credential, and Access Management (FICAM) Architecture, June 30, 2023 (FICAM Architecture (idmanagement.gov))
43. NIST SP 800-116 Rev 1, "Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access," June 2018

44. NIST SP 800-63 Rev 4, 800-63A-4, 800-63B-4, 800-63C-4, “Digital Identity Guidelines,” August 1, 2025
45. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
46. 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)
47. 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)
48. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896
49. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, https://www.cisa.gov/publication/tic-30-core-guidance-documents
50. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019
51. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (P.L. 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (P.L. 109–58), August 8, 2005
54. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
55. Executive Order 14148, “Initial Rescissions of Harmful Executive Orders and Actions,” dated January 20, 2025
56. VA Directive 0057, “VA Environmental Management Program,” October 25, 2022
57. OIS VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
58. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
59. “Veteran Focused Integration Process (VIP) Guide 4.0,” March 2021, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
60. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
61. “Product Line Management Transformation Playbook” version 3.1, August 2023, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946
62. NIST SP 500-267B Revision 1, “USGv6 Profile,” November 2020
63. OMB Memorandum M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” November 19, 2020
64. Social Security Number (SSN) Fraud Prevention Act of 2017
65. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018
66. C.F.R Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, as amended

67. Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/
68. OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
69. NIST SP 800-52 Revision 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
70. OMB M-26-05, "Adopting a Risk-based Approach to Software and Hardware Security," January 23, 2026
71. OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," August 27, 2021
72. NIST SP 800-88 Revision 1 "Guidelines for Media Sanitization," December 2014
73. CISA Binding Operational Directive (BOD) 19-02: "Vulnerability Remediation Requirements of Internet-Accessible Systems," April 29, 2019, BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems | CISA
74. CISA BOD 22-01: "Reducing the Significant Risk of Known Exploited Vulnerabilities," November 3, 2021, BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities | CISA
75. CISA BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks." Cybersecurity & Infrastructure Security Agency (CISA), BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks | CISA
76. VA Directive 6550, Pre-Procurement Assessment and Implementation of Medical Devices/Systems, June 03, 2019
77. VA Memorandum, "VA Security Controls," January 17, 2025, https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010
78. E.O. 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," December 3, 2020
79. E.O. 14319, "Preventing Woke AI in the Federal Government," July 23, 2025
80. OMB Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," April 3, 2025
81. OMB Memorandum M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government," April 3, 2025
82. OMB Memorandum M-26-04, "Increasing Public Trust in Artificial Intelligence (AI) Through Unbiased AI Principles," December 11, 2025

3.0 SCOPE OF WORK

The Contractor shall serve as the enterprise System Integrator, responsible for performing enterprise service integration, providing and managing all necessary licensing, conducting operations and sustainment activities, executing modernization initiatives, and maintaining full accountabilities for all assigned tasks and outcomes. The

Contractor shall provide a single, unified product/platform to support an enterprise-wide ERP SaaS/PaaS solution with a subscription model that includes licensing and support. The Contractor shall ensure that no additional platforms or tools are required for the implementation and operation of the solution.

The Contractor shall also perform the following optional tasks when these tasks are exercised:

1. Enterprise Asset Management
2. Enterprise HRSD
3. Artificial Intelligence (AI)
4. Data Lake Solution
5. Greenfield Solution
6. Vendor Risk Management
7. Field Service Management
8. Transition Out

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The PoP shall be 12-month base period with four 12-month option periods with nine Optional Tasks. The overall Period of Performance shall not exceed 60 months.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

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

Under current definitions, five 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 Contractor facilities. The Contractor shall identify the Contractor's place of performance in their proposal submission.

4.3 TRAVEL

The Government does not anticipate travel under this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

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

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

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

The Weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall conduct an Annual Reporting Capability Review within the 4th quarter of the federal fiscal year. The review shall include comprehensive review of the platform's reporting and analytics capabilities, with recommendations for enhancements.

Deliverable:

A. Weekly Progress Report

5.2 ENTERPRISE SERVICE INTEGRATION, LICENSING, OPERATIONS, AND ACCOUNTABILITY MODEL

The Contractor shall perform enterprise service integration, provide and manage licensing, conduct operations and sustainment, execute modernization, and maintain full accountability in its role as the enterprise System Integrator. The Contractor shall provide the management, operational capabilities, technical coordination, vendor coordination, sustainment support, licensing coordination, release management, integration support, and continuous improvement capabilities necessary to deliver a secure, scalable, resilient, and continuously supportable enterprise environment. The Contractor shall provide the enterprise licensing, service delivery, operational support, and sustainment support. The Contractor shall meet all Service Level Agreement (SLA) requirements applicable to the Contractor's enterprise System Integrator role. Where requirements overlap, this section shall be interpreted as establishing the Contractor's integrated enterprise accountability for achieving the operational outcomes, service performance levels, modernization outcomes, and lifecycle sustainment obligations described herein.

The Contractor shall ensure the enterprise platform supports VA mission operations by enabling reliable delivery of Veteran-facing and mission-support services, improving enterprise service delivery efficiency, reducing operational disruption, improving user experience, increasing automation and self-service adoption, and reducing duplicative or non-standard enterprise capabilities. The Contractor shall remain accountable for achievement of the outcomes required by this PWS regardless of dependencies such as subcontractor participation, original equipment manufacturer dependencies, cloud provider dependencies, third-party service relationships, or supporting infrastructure arrangements.

The Contractor shall not attribute performance failures, outages, service degradation, licensing deficiencies, integration failures, sustainment issues, or operational delays to subcontractors, software publishers, cloud providers, infrastructure providers, or other third parties as a basis for avoiding contractual responsibility. The Contractor shall manage and coordinate all such dependencies as part of its enterprise service integration responsibilities.

The Government shall retain ownership of all Government data, metadata, configurations, workflows, automations, integrations, reports, analytics, documentation, operational records, and associated information assets created, processed, stored, configured, or maintained under this contract. The Contractor shall ensure Government

access, portability, auditability, and transitionability of those assets throughout the Period of Performance.

5.2.1 ENTERPRISE OPERATIONAL OUTCOME REQUIREMENTS

The Contractor shall achieve measurable enterprise operational outcomes throughout the Period of Performance. These outcomes shall support VA mission priorities and shall improve the reliability, usability, scalability, interoperability, maintainability, and efficiency of enterprise IT service delivery.

The Contractor shall maintain the enterprise platform in a manner that improves operational resiliency, reduces recurring incidents, increases standardization, reduces unnecessary customization, improves integration reliability, improves data integrity, and supports continuous platform modernization. The Contractor shall also improve user-facing outcomes by increasing self-service utilization, improving customer satisfaction, reducing manual service fulfillment activities, and supporting more efficient completion of enterprise service requests.

The Contractor shall establish operational baselines within 90 calendar days of contract award. Baseline methodology shall be included in the Transition-In Readiness Assessment as indicated in 5.2.13 and approved by the Contracting Officer's Representative prior to finalization. The Contractor shall provide an Enterprise Operational Baseline and Improvement Plan which include baseline data sources, assumptions, known data gaps, data quality limitations, and measurement methodology. Performance improvement requirements under this section shall be measured against the approved baseline beginning in the first full contract year following baseline approval.
Baselines shall include, at a minimum, platform availability, incident trends, service restoration times, change success rates, release performance, integration performance, user satisfaction, self-service adoption, automation utilization, recurring incident rates, modernization delivery performance, and business value realization measures. The Contractor shall use these baselines to demonstrate measurable year-over-year improvement.

The Enterprise Operational Baseline and Improvement Plan shall include, at minimum: approved baseline values for each required metric; data sources and collection methodology for each metric; identified trends and known operational risks; year-one improvement targets for each metric; and proposed measurement and reporting cadence.

The Contractor shall maintain performance management capabilities sufficient to identify recurring service issues, modernization constraints, underutilized platform capabilities, automation opportunities, service delivery inefficiencies, and opportunities to reduce duplicative or non-standard functionality. The Contractor shall provide recommendations to the Government that support improved service reliability, enterprise reuse, platform standardization, operational efficiency, and mission-aligned

modernization. Upon Government approval, the baseline values in Enterprise Operational Baseline and Improvement Plan shall serve as the performance targets.

Standard	Acceptable Quality Level (AQL)	Measurement Method
Completeness	All required content elements are presented per PWS section requirements; no more than 3 minor deficiencies per submission.	COR review of deliverable.
Accuracy	Factual errors or data discrepancies in no more than 2% of reported data points per submission.	COR review of reported data and supporting documentation.
Timeliness	Submitted on or before the due date established in the Contract Deliverables Requirements List; no more than 1 late submission per contract year.	Deliverable schedule
Enterprise Operational Baseline Established	Baseline delivered within 90 calendar days of contract award.	COR review of deliverable.
Year-over-Year Recurring Incident Reduction	Minimum 10% reduction in recurring incident volume per contract year versus prior year baseline.	Monthly and annual incident trend analysis.
Enterprise Platform Standardization	No more than 3 unsupported customizations identified in annual modernization assessment.	Annual modernization assessment and configuration review.
Improvement Plan Submission	Submitted on time.	COR review of deliverable.

Failure to meet a performance standard shall require the Contractor to submit a written Corrective Action Plan to the COR within five business days and to implement corrective actions within the timeframe approved by the COR and the Contracting Officer (CO), not to exceed 30 calendar days for Priority 1 and Priority 2 deficiencies and 60 calendar days for Priority 3 and Priority 4 deficiencies as defined in the SLA at Attachment 001.

Deliverable:

A. Enterprise Operational Baseline and Improvement Plan

5.2.2 ENTERPRISE DELIVERY MODEL

The Contractor shall assume the operational and financial risk associated with normal enterprise growth, increased user adoption, transaction volume growth, expanded

platform utilization, routine modernization demand, and service scaling necessary to maintain required performance levels. For purposes of this section, normal enterprise growth means increases in licensed user counts, transaction volumes, platform utilization, or related operational demand. that do not exceed 15% above the baseline established at award in any contract year. Growth exceeding this threshold shall be subject to contract modification at the Government's discretion.

The Contractor shall not impose additional charges for routine operational scaling, standard platform upgrades, maintenance releases, support activities, or licensing adjustments required to maintain the contracted enterprise service levels, except where expressly authorized by the contract.

The Contractor shall submit the Annual Enterprise Pricing Integrity Certification within 30 calendar days of each contract year anniversary. The Certification will be accepted by the Government if it identifies all active cost components, 100% of licensing, sustainment, operational, and modernization costs separately identifiable with no undisclosed markups. Certifications failing Government acceptance shall be resubmitted within 15 business days.

Performance Standard	Acceptable Quality Level	Measurement Method
Annual Enterprise Pricing Integrity Certification Submission	Submitted within 30 calendar days of each contract year anniversary.	COR review of certification submission date and completeness.
Pricing Transparency	100% of licensing, sustainment, operational, and modernization costs separately identifiable with no undisclosed markups or bundled pricing structures.	COR review of pricing artifacts, invoices, and supporting documentation.
Invoice Reconciliation Accuracy	Pricing certification reconciles to invoiced amounts within no more than 2% variance.	Invoice reconciliation and financial review.
Operational Scaling Support	Contractor maintains required service levels during normal enterprise growth without additional charges.	SLA performance reports and operational trend analysis.

Deliverable:

A. Annual Enterprise Pricing Integrity Certification.

5.2.3 ENTERPRISE LICENSING ACCOUNTABILITY AND TRANSPARENCY

The Contractor shall provide, manage, coordinate, and maintain all licensing, subscriptions, entitlements, support agreements, and related licensing activities

necessary to sustain uninterrupted enterprise platform operations and approved modernization activities. The Contractor shall ensure all licensing remains current, valid, sufficient, and aligned with authorized enterprise usage.

The Contractor shall structure licensing to support enterprise scalability, phased deployment, module expansion, operational continuity, upgrade compatibility, and long-term maintainability. Licensing shall align to actual Government usage and adoption to the maximum extent practicable and shall avoid unnecessary purchase of unused capacity when phased deployment or usage-based consumption is available.

The Contractor shall provide the most cost-effective licensing model type, including named user, concurrent user, consumption-based, or enterprise licensing arrangements, that meet Government requirements. The Contractor shall document the basis for the selected licensing model in the Licensing Transparency Artifact and shall identify alternative models considered and reasons for their exclusion.

The Contractor shall provide a Licensing Transparency Artifact that shows licensing costs shall be separately identifiable from implementation, sustainment, modernization, operational support, and other professional service costs. The Contractor shall not obscure licensing costs through undisclosed markups, hidden fees, bundled structures that prevent cost validation, or packaging arrangements that prevent the Government from understanding what is being purchased and how pricing was calculated.

The Contractor shall maintain an enterprise licensing management capability that identifies license quantities, license types, modules, unit prices, discount structures, utilization levels, unused capacity, growth assumptions, and optimization opportunities. The Contractor shall recommend actions to reduce unnecessary licensing costs, improve utilization, and support future enterprise scalability and provide a Licensing Optimization Assessment capturing the above requirements.

The Contractor shall provide Enterprise Licensing Management that identify, at minimum, all active licenses by type, module, and vendor; unit prices and applicable discount structures; the basis for the selected licensing model; comparison of alternative models considered; utilization rates; unused capacity; growth assumptions; pending renewals; and expiration dates within the subsequent 12-month period.

Performance Standard	**Acceptable Quality Level**	**Measurement Method**
Licensing Transparency Artifact	Updated on schedule with all required licensing elements identified.	COR review of deliverable.
Unused Capacity Identification	Unused licensed capacity exceeding 15% identified and corrective recommendations provided quarterly.	Licensing Optimization Assessment review.

Performance Standard	Acceptable Quality Level	Measurement Method
Licensing Renewal Tracking	100% of licenses with expiration within 12 months identified in reporting.	License inventory and renewal audit.
Licensing Model Optimization	Contractor documents evaluation of alternative licensing models and justification for selected approach.	COR review of Licensing Transparency Artifact.

Deliverables:

A.
B. Licensing Optimization Assessment
C. Licensing Transparency Artifact

5.2.4 ENTERPRISE OPERATIONAL ACCOUNTABILITY

The Contractor shall serve as the single point of accountability for end-to-end enterprise operational performance. This accountability includes platform availability, application functionality, integration performance, service support, sustainment, security coordination, release management, vendor coordination, subcontractor performance, operational continuity, and lifecycle support.

The Contractor shall maintain operational governance capabilities sufficient to identify risks before they impact service delivery, coordinate resolution of enterprise issues, prevent recurring failures, manage dependencies, support release planning, and maintain continuity of enterprise services. The Contractor shall ensure that operational risks are tracked, prioritized, mitigated, and reported no less than monthly in a manner that supports timely Government decision-making. The Contractor shall add newly identified risks to the Enterprise Service Accountability Dashboard Enterprise Operational Risk Assessment within five business days of identification. Risks rated High or Critical as defined in the SLA at Attachment 001 shall be reported to the COR within two business days of identification.

The Contractor shall provide and maintain Risk Rating Methodology approved by the Government within 60 calendar days of contract award. The methodology shall define risk likelihood, consequence, and rating criteria at minimum. Risk ratings shall be applied consistently across the Period of Performance.

The Contractor shall maintain enterprise coordination capabilities sufficient to manage dependencies among software publishers, cloud providers, hosting providers, subcontractors, infrastructure providers, third-party integrations, and VA stakeholders. The Contractor shall ensure those dependencies do not degrade enterprise platform performance, delay modernization, impair sustainment, or reduce service quality.

The Contractor will not be responsible for performance failures solely attributable to Government-controlled systems, infrastructure, networks, or services outside Contractor

operational authority, provided the Contractor demonstrates timely escalation, documented coordination, and reasonable mitigation efforts.

The Contractor shall maintain the ERP solution in a current, secure, and fully supported state throughout the period of performance. The Contractor shall provide access to and implement all standard OEM platform enhancements, security updates, performance improvements, workflow automation capabilities, analytics capabilities, and AI capabilities included within the Government's licensed subscription at no additional cost to the Government. The Contractor shall provide a quarterly Technology Modernization Report identifying newly available capabilities, recommended adoption actions, implementation impacts, and anticipated business value. The Contractor shall maintain upgrade readiness and support implementation of OEM-supported releases within Government-approved timelines.

The ERP solution shall support secure, near real-time integration and data sharing across all authorized ERP instances and environments. The Contractor shall ensure enterprise data synchronization, interoperability, and reporting capabilities are maintained with a minimum availability of 99.9% and without duplicate data repositories or manual data re-entry processes. The Contractor shall support standard APIs, integration services, and data exchange mechanisms necessary to enable enterprise-wide visibility, governance, reporting, and workflow orchestration across multiple instances.

Performance Standard	**Acceptable Quality Level**	**Measurement Method**
Enterprise Risk Register Maintenance	Newly identified risks entered into the register within 5 business days of identification.	Monthly risk register review.
High/Critical Risk Escalation	High and Critical risks reported to COR within 2 business days of identification.	COR review of escalation records and risk logs.
Government-Approved Risk Methodology	Risk methodology submitted and approved within 60 calendar days of contract award.	COR approval of methodology deliverable.
Dependency Coordination Effectiveness	No recurring unresolved dependency issue remains open longer than 30 calendar days without approved mitigation plan.	Operational governance meeting minutes and dependency tracking reports.
Monthly Operational Risk Reporting	Operational risk assessment submitted monthly, complete, and accurate.	COR review of monthly reports.

Deliverables:

A. Enterprise Operational Risk Assessment
B. Risk Rating Methodology

5.2.5 PLATFORM OPERATIONS, SUSTAINMENT, AND MODERNIZATION

The Contractor shall provide full lifecycle platform operations and sustainment services necessary to maintain a secure, stable, resilient, performant, scalable, interoperable, and continuously supportable enterprise environment. The Contractor shall operate the platform in a manner that supports current enterprise service requirements and future modernization needs.

The Contractor shall maintain capabilities for continuous monitoring, capacity management, performance management, vulnerability remediation, operational recovery, security coordination, release management, upgrade management, integration support, environment management, and lifecycle sustainment through an Enterprise Platform Health Dashboard. These capabilities shall be performed in a manner that preserves enterprise functionality, minimizes operational disruption, maintains security compliance, and supports future platform evolution.

The Contractor shall implement security patches and vulnerability remediations within the following timelines from vendor release or Government notification, whichever is earlier, unless a documented exception is approved in writing by the COR or CO: Critical severity within 15 calendar days; High severity within 30 calendar days; Medium severity within 60 calendar days; and Low severity within 90 calendar days in accordance with the SLA. The Contractor shall implement security patches and vulnerability remediations within the following timelines from vendor release or Government notification, whichever is earlier, unless a documented exception is approved in writing by the Contracting Officer: Critical severity within 15 calendar days; High severity within 30 calendar days; Medium severity within 60 calendar days; and Low severity within 90 calendar days in accordance with the SLA. The Contractor shall compile to VA security policy, emergency directive, binding operational directive, or Government-directed remediation timeline shall control. The Contractor shall notify the COR within two business days of identifying any patch or remediation action that cannot be implemented within the required timeline and shall provide a risk acceptance recommendation and interim mitigation plan.

The Contractor shall implement vendor-supported releases, maintenance updates, and platform upgrades within Government-approved timelines and in accordance with approved change and release governance processes. The Contractor shall ensure upgrades and releases do not introduce unsupported customizations, unnecessary technical debt, avoidable integration conflicts, or operational dependencies that negatively impact future maintainability and shall provide the Government with a Modernization and Upgrade Readiness Assessment.

The Contractor shall maintain modernization readiness by ensuring the platform remains supportable, upgrade-compatible, and aligned with enterprise architecture and security requirements. The Contractor shall identify technical debt, unsupported configurations, performance constraints, and modernization risks and shall recommend corrective actions to preserve long-term platform viability.

Performance Standard	Acceptable Quality Level	Measurement Method
Vulnerability Remediation Timeliness	Critical vulnerabilities remediated within 15 days; High within 30 days; Medium within 60 days; Low within 90 days unless otherwise directed.	Vulnerability management reporting and security audit review.
Upgrade and Release Currency	Vendor-supported releases and upgrades implemented within Government-approved timelines.	Release management records and change review.
Unsupported Customization Reduction	No increase in unsupported customizations from approved baseline year-over-year.	Annual modernization assessment and configuration review.
Platform Health Monitoring	Enterprise Platform Health Dashboard updated monthly with complete operational metrics.	COR review of dashboard submissions.
Technical Debt Identification	Technical debt and modernization risks identified and documented quarterly with remediation recommendations.	Modernization and Upgrade Readiness Assessment review.

Deliverables:

A. Modernization and Upgrade Readiness Assessment

5.2.6 CONTINUOUS SERVICE IMPROVEMENT AND BUSINESS VALUE REALIZATION

The Contractor shall maintain a formal Continuous Service Improvement capability focused on measurable improvement in enterprise operations, service reliability, automation adoption, modernization effectiveness, user experience, and business value realization.

The Contractor shall demonstrate measurable year-over-year improvement in operational areas such as recurring incident reduction, Priority 1 incident reduction, mean time to restore service, change success rates, release quality, automation utilization, self-service adoption, first-contact resolution, customer satisfaction, enterprise reuse, reduction of duplicate functionality, and reduction of manual operational effort.

The Contractor shall demonstrate year-over-year improvement against the approved operational baseline for each of the following metrics at minimum, unless otherwise approved by the Government based on achieved steady-state performance, documented data limitations, or Government-approved constraints outside the Contractor's control. The Contractor shall tabulate these improvements with the Continuous Improvement Metrics Dashboard.

Minimum Annual Improvement Requirements:

Metric	Minimum Annual Improvement
Recurring incident volume	10% reduction year-over-year.
Priority 1 incident reduction	15% reduction year-over-year.
Mean time to restore service	10% reduction year-over-year.
Change success rates	Maintain minimum 95% successful change rate and improve toward 98%.
Release quality	10% reduction in post-release defects year-over-year.
Automation utilization	5 percentage point increase in automated transaction share year-over-year.
Self-service utilization	5 percentage point increase year-over-year.
First-contact resolution	5 percentage point increase year-over-year.
Customer satisfaction	Maintain minimum 4.5 out of 5.0 and improve trend toward 4.7.
Enterprise reuse	10% increase in reused versus newly created components year-over-year.
Reduction of duplicate functionality	Net reduction of 5 duplicative capabilities per contract year, where duplicative capabilities exist and are within Contractor control.
Reduction of manual operational effort	10% reduction in manual fulfillment transactions year-over-year.

The Contractor shall provide a Business Value Realization Assessment to measure business value resulting from platform operations and modernization activities. Business value measurements shall include, as applicable, reductions in process completion time, reductions in manual touchpoints, increased workflow automation, increased utilization of delivered capabilities, improved operational throughput, improved service request fulfillment efficiency, and improved user adoption of standardized enterprise services.

The Contractor shall provide recommendations for improvement when performance trends indicate degradation, stagnation, avoidable manual work, underutilized platform capabilities, or recurring operational issues. The Contractor shall provide an Operational Efficiency Assessment, recommendations that include expected operational benefit, implementation considerations, dependencies, and measurable target outcomes.

Performance Standard	Acceptable Quality Level	Measurement Method
Automation Utilization	Minimum 5 percentage point increase in automated transaction share year-over-year.	Automation utilization reporting.
Business Value Recommendations	Improvement recommendations submitted quarterly with measurable operational benefit identified.	COR review of Continuous Improvement submissions.

Deliverables:

A. Business Value Realization Assessment
B. Operational Efficiency Assessment

5.2.7 ENTERPRISE AVAILABILITY AND OPERATIONAL CONTINUITY

The Contractor shall maintain monthly production availability of no less than 99.99%. Availability shall apply to all ERP production instances of the platform, required production integrations, core platform services, hosting dependencies under Contractor responsibility, and operational services necessary for users to perform intended business functions. The Contactor shall provide an Enterprise Availability Dashboard to allow the Government to review and monitor platform availability.

Availability shall be calculated as total scheduled operational minutes minus verified unplanned outage minutes, divided by total scheduled operational minutes, multiplied by 100. Government-approved maintenance windows, Government-directed outages, and force majeure events shall be excluded from the calculation.

An unplanned outage means an unscheduled interruption or material degradation of production service functionality that prevents users from performing intended business operations. Material degradation includes severe performance impairment, failed integrations, transaction processing failures, or service instability resulting in loss of operational usability. For purposes of this section, severe performance impairment means response times exceeding three times the established performance baseline, or transaction error rates exceeding 5%, sustained for a period of 15 minutes or more, or other Government-approved operational threshold based on the monitored service or business function.

Outages or degradations attributable to subcontractors, cloud providers, OEM vendors, integrations, infrastructure dependencies, or supporting services under Contractor responsibility shall count toward availability calculations. Exclusions from availability calculations shall be documented by the Contractor in the applicable monthly performance report with supporting evidence. Exclusion requests shall be reviewed and approved by the COR. The COR will refer exclusion determinations to the CO where the requested exclusion involves a pattern of recurring third-party dependency failures or where the requested exclusion would affect credit calculations.

The Contractor shall not be responsible for performance failures solely attributable to Government-controlled systems, infrastructure, networks, or services outside Contractor operational authority, provided the Contractor demonstrates timely escalation, documented coordination, and reasonable mitigation efforts.

The Contractor shall provide immediate escalation, restoration coordination, corrective action, and recurrence prevention for any availability event that threatens enterprise operations or mission-support services.

For each monthly measurement period in which availability falls below 99.99%, the Contractor shall submit a Availability Trend and Corrective Action Metrics Package that includes Root Cause Analysis within five business days and a Corrective Action Plan within 10 business days. For availability below 99.9% in any measurement period, the Government may assess service credits in accordance with the SLA. For availability below 99.5% in any measurement period, the Government may, at its discretion, issue a cure notice in accordance with applicable contract terms and clauses.

Performance Standard	**Acceptable Quality Level**	**Measurement Method**
Production Platform Availability	Minimum 99.99% monthly availability.	Monthly SLA availability calculation and monitoring reports.
Availability Event Root Cause Analysis	RCA submitted within 5 business days for all availability failures below AQL.	COR review of RCA submissions.
Corrective Action Plan Submission	CAP submitted within 10 business days for availability below AQL.	COR review of CAP submission and implementation tracking.
Unplanned Outage Documentation	100% of outages documented with impact, duration, cause, and corrective action.	Monthly outage reporting review.

Performance Standard	Acceptable Quality Level	Measurement Method
Availability Exclusion Validation	All exclusion requests supported with documented evidence and Government approval.	COR review of SLA exclusion documentation.

Deliverables:

A. Availability Trend and Corrective Action Metrics Package

5.2.8 INCIDENT RESPONSE AND SERVICE RESTORATION

The Contractor shall maintain incident management capabilities sufficient to minimize operational disruption, restore affected services, communicate status, identify root cause, and prevent recurrence. Incident response and resolution requirements shall apply to incidents affecting the production platform, integrations, operational services, security posture, or user ability to complete intended business functions. The Contractor shall provide an Incident Performance Dashboard to monitor incident performance.

Incident priorities shall be assigned in accordance with the following definitions, subject to Government review and reclassification. The Government may raise incident priority based on mission impact, operational criticality, data sensitivity, executive direction, or impact to a critical business function, regardless of the number of users directly affected.

Priority	Definition	Response Time	Resolution Target
P1	Complete loss of production platform availability or loss of a critical business function affecting 1,000 or more users, with no workaround available.	15 minutes	4 hours
P2	Significant degradation of a production service or loss of a major function affecting 250 or more users, with limited workaround available.	30 minutes	8 hours
P3	Partial loss of non-critical functionality affecting limited users, with an acceptable workaround available.	1 hour	2 business days
P4	Minor issues, cosmetic defect, service question, or low-impact condition with no material operational impact.	1 business day	5 business days

SLA compliance shall be calculated as the number of SLA-applicable incidents resolved within the applicable target divided by the total number of SLA-applicable incidents during the measurement period, multiplied by 100.

The Contractor shall provide a Root Cause and Corrective Action Package that maintains escalation procedures, root cause analysis procedures, restoration procedures, and recurrence prevention processes. For Priority 1 and recurring Priority 2 incidents, the Contractor shall identify cause, operational impact, corrective action, preventive action, and target completion dates for remediation. For purposes of this section, recurring Priority 2 incidents means two or more Priority 2 incidents with the same or substantially similar root cause within a 30-calendar-day measurement period.

Performance Standard	Acceptable Quality Level	Measurement Method
Recurring Incident RCA Completion	Root cause analysis completed for 100% of recurring Priority 1 and Priority 2 incidents.	RCA review and incident tracking audit.
Escalation Procedure Compliance	100% adherence to documented escalation procedures for major incidents.	Operational review and ticket audit.

Deliverables:

A. Root Cause and Corrective Action Package

5.2.9 CHANGE , RELEASE, AND MODERNIZATION PERFORMANCE

The Contractor shall maintain change and release capabilities sufficient to support enterprise modernization while preserving operational stability. The Contractor shall ensure changes and releases are planned, tested, traceable, approved, recoverable, and aligned with enterprise governance requirements. The Contractor shall provide a Change Performance Dashboard to monitor Change performance.

The Contractor shall achieve a minimum 95%successful production change implementation rate and a minimum 95% successful major release deployment rate. A successful change or release is one that is implemented as approved, does not require emergency rollback due to Contractor error, does not introduce a Priority 1 or Priority 2 incident within 24 hours of implementation for standard changes or within 72 hours of implementation for major releases, and does not result in unauthorized unplanned degradation of production services. The Contractor shall provide a Release Readiness and Outcome Assessment to the Government for review of release outcomes.

The Contractor shall not implement unauthorized production changes. All production changes shall be implemented in accordance with the approved change management process.

The Contractor shall reduce failed change trends, improve release quality, and identify opportunities to increase deployment efficiency without degrading platform stability or security compliance.

Performance Standard	Acceptable Quality Level	Measurement Method
Successful Change Rate	Minimum 95% successful production change rate.	Change management reporting.
Successful Release Deployment Rate	Minimum 95% successful major release deployment rate.	Release performance reporting.
Unauthorized Production Changes	Zero unauthorized production changes implemented.	Change audit and governance review.
Failed Change Trend Reduction	Year-over-year reduction in failed changes attributable to Contractor actions.	Trend analysis of change outcomes.
Post-Release Incident Reduction	Minimum 10% reduction in post-release defects year-over-year.	Release defect tracking and incident review.

Deliverables:

A. Release Readiness and Outcome Assessment

5.2.10 INTEGRATION RELIABILITY AND DATA INTEGRITY

The Contractor shall maintain integration reliability and data integrity sufficient to support uninterrupted enterprise operations and business-process continuity. The Contractor shall ensure integrations are monitored, failures are detected, data synchronization is validated, and integration issues are resolved within applicable SLA timelines.

The Contractor shall achieve a minimum 99% successful integration transaction processing rate for production integrations under Contractor responsibility. Integration transaction success shall be calculated as successfully completed integration transactions divided by total attempted integration transactions during the measurement period. Transactions executed within approved test windows and transactions affected by Government-directed outages shall be excluded from the calculation, provided the Contractor documents those transactions and the basis for exclusion in the applicable performance report. The Contractor shall provide an Integration Reliability Dashboard to allow the Government to review compliance with the above requirements.

The Contractor shall preserve Change Management Data Base (CMDB) integrity, reduce duplicate or conflicting enterprise data, maintain synchronization of enterprise interfaces, and identify recurring integration issues requiring remediation. The Contractor shall maintain a CMDB accuracy rate of no less than 95% for production

configuration items following approval of the CMDB baseline or completion of any Government-approved cleanup period. Data quality assessments shall measure completeness, accuracy, and currency of configuration item records against defined data quality criteria approved by the Government. The Contractor shall provide a Data Integrity and Synchronization Assessment to support data integrity requirement.

Performance Standard	Acceptable Quality Level	Measurement Method
Integration Transaction Success Rate	Minimum 99% successful production integration transaction rate.	Integration monitoring and transaction logs.
CMDB Accuracy	Minimum 95% CMDB accuracy rate following approved baseline establishment.	CMDB audit and data quality assessment.
Integration Failure Detection	100% of integration failures identified and logged.	Integration monitoring system review.
Data Synchronization Integrity	No unresolved critical synchronization failures exceeding 5 business days.	Data integrity reporting and audit review.
Recurring Integration Issue Remediation	Corrective action identified for recurring integration failures within 10 business days.	COR review of remediation tracking.

Deliverables:

A. Data Integrity and Synchronization Assessment

5.2.11 SECURITY AND OPERATIONAL RESILIENCE

The Contractor shall maintain operational security and resilience capabilities sufficient to detect, respond to, contain, remediate, and recover from security incidents affecting enterprise platform operations. The Contractor shall comply with applicable VA security requirements, approved security processes, and Government-directed incident response procedures. The Contractor shall provide a Security Operations Dashboard for the following purposes.

For purposes of this section, a critical security incident means a confirmed or suspected security event that involves potential unauthorized access to Government data, active exploitation of a production system vulnerability, ransomware or destructive malware activity, confirmed or suspected data exfiltration, or any event that, if not immediately contained, could result in material degradation of enterprise platform operations or exposure of sensitive Government information.

For critical security incidents, the Contractor shall initiate response activities within 15 minutes of detection or notification and shall initiate containment actions within 2 hours after confirmation, unless otherwise directed by the Government.

The Contractor shall remediate vulnerabilities, configuration weaknesses, and security-related operational risks within timelines based on severity and operational impact. Unless otherwise directed by the Government or approved in writing by the Contracting Officer, Critical vulnerabilities shall be remediated within 15 calendar days, High vulnerabilities within 30 calendar days, Medium vulnerabilities within 60 calendar days, and Low vulnerabilities within 90 calendar days. More stringent VA cybersecurity policy, emergency directive, binding operational directive, or Government-directed timeline shall control.

The Contractor shall provide Security Incident Response and Remediation Package that identify recurring security-related operational risks, recommend preventive controls, and ensure security remediation activities do not unnecessarily degrade service availability or platform maintainability.

Performance Standard	Acceptable Quality Level	Measurement Method
Critical Security Incident Response	Response initiated within 15 minutes of detection or notification.	Security operations logs and incident review.
Critical Security Incident Containment	Containment actions initiated within 2 hours of confirmation.	Security incident response reporting.
Vulnerability Remediation Compliance	Vulnerabilities remediated within required severity timelines.	Vulnerability management reporting.
Security Risk Identification	Recurring security risks identified and documented monthly with mitigation recommendations.	Security operations reporting review.
Security Remediation Impact Management	Security remediation activities do not result in unauthorized operational disruption.	Change review and operational incident analysis.

Deliverables:

A. Security Incident Response and Remediation Package.

5.2.12 USER EXPERIENCE, ADOPTION, AND SERVICE EFFICIENCY

The Contractor shall maintain user support and service enablement capabilities sufficient to improve user experience, increase adoption of standardized enterprise services, reduce manual fulfillment activities, and improve service efficiency.

The Contractor shall achieve a Customer Satisfaction (CSAT) score of no less than 4.5 out of 5.0, calculated as the average satisfaction score across all survey responses received during the measurement period. The Contractor shall deploy a standardized survey instrument, submitted to the COR for approval prior to first use. Survey distribution methods shall reach a representative cross-section of platform users. The Contractor shall ensure response volumes are sufficient to produce statistically meaningful results, with a minimum of 100 valid responses or another Government-approved statistically valid sample size per measurement period required before CSAT results are used for AQL compliance determination.

The Contractor shall implement corrective actions when CSAT falls below the required level and shall include trend analysis and corrective action summaries in the User Experience Dashboard.

The Contractor shall increase self-service utilization, improve first-contact resolution, increase automation utilization, reduce manual fulfillment work, and improve service request completion efficiency. The Contractor shall measure adoption and utilization of delivered capabilities to ensure modernization activities result in actual operational value rather than unused functionality and provide an Adoption and Service Efficiency Assessment.

Performance Standard	Acceptable Quality Level	Measurement Method
Customer Satisfaction (CSAT)	Maintain minimum monthly CSAT score of 4.5 out of 5.0.	Approved customer survey analysis.
Survey Response Sufficiency	Minimum 100 valid responses or Government-approved statistically valid sample size per measurement period.	Survey participation reporting.
First-Contact Resolution Improvement	Minimum 5 percentage point increase year-over-year.	Service desk reporting and trend analysis.
Self-Service Utilization Improvement	Minimum 5 percentage point increase year-over-year.	Self-service portal usage reporting.

Performance Standard	Acceptable Quality Level	Measurement Method
Manual Fulfillment Reduction	Minimum 10% reduction in manual fulfillment transactions year-over-year.	Workflow automation and fulfillment reporting.

Deliverables:

A. Adoption and Service Efficiency Assessment

5.2.13 SYSTEM INTEGRATOR TRANSITION-IN SERVICES

The Contractor shall provide system integrator transition support sufficient to ensure continuity of enterprise operations during transition-in.

During transition-in, the Contractor shall validate current-state operations, identify operational risks, establish service baselines, confirm licensing and support dependencies, document platform configuration, and assume operational accountability without degradation of enterprise services.

The Contractor shall assume full operational accountability for enterprise platform services no later than 90 calendar days following award, unless the Government approves phased operational accountability milestones based on transition complexity, incumbent data limitations, or operational risk. At minimum, the Contractor shall provide transition status at 30, 60, and 90 calendar days when phased accountability is approved. Assumption of operational accountability shall be documented in the Transition-In Readiness Assessment and confirmed in writing by the COR.
During transition-out, the Contractor shall support orderly transfer of operational knowledge, documentation, configurations, workflows, integrations, data, open issues, support procedures, and sustainment responsibilities to the Government or successor contractor. The Contractor shall deliver a complete Transition-Out and Knowledge Transfer Plan no later than 120 calendar days before the scheduled contract expiration date. In the event of a Government-directed transition occurring before the 120-day threshold, the Contractor shall deliver the Transition-Out and Knowledge Transfer Plan within 30 calendar days of receipt of written Government transition notice.

Performance Standard	Acceptable Quality Level	Measurement Method
Transition-In Readiness Assessment	Submitted within required timeframe and accepted by Government.	COR review of deliverable.
Operational Accountability Assumption	Contractor assumes full operational accountability within 90 calendar days unless otherwise approved.	Government operational readiness review.

Performance Standard	Acceptable Quality Level	Measurement Method
Transition Acceptance	Transition activities accepted in writing by Government with no unresolved critical deficiencies.	COR transition acceptance documentation.

Deliverables:

A. Transition-In Readiness Assessment

5.3 ENTERPRISE RESOURCE PLANNING PLATFORM REQUIREMENTS

The Contractor shall configure, deploy and maintain a single, unified, cloud based ERP solution utilizing a multi instance PaaS architecture and delivered through an enterprise SaaS subscription model. The ERP solution shall provide VA with capabilities needed to support enterprise resource planning and to manage digital workflows for enterprise operations. The ERP solution must meet base functionality requirements, allow for enhancements and configuration, while providing robust and comprehensive features with limited customization and avoiding extensive custom development accounting for all technical debt, ensuring ease of future upgrades and maintenance.

The Contractor shall provide a single, unified product/platform to support an enterprise-wide ERP SaaS/PaaS solution with a subscription model that includes licensing and support of the following capabilities.

1. ITSM
2. ITAM
3. ITOM
4. ITBM
5. Digital Workplaces
6. Customer Service Management (CSM)
7. Security Operations (SecOps)
8. Integrated Risk Management (IRM)
9. Integration Center
10. Reporting and Analytics
11. Platform Tools
12. Production Instance
13. Non-Production Instance
14. Customer Performance Testing Instance
15. Enterprise Asset Management (EAM) – (Optional task)
16. Custom applications (Scope App) – (Optional task)
17. HRSD (Optional Task)

The ERP solution shall provide the capability to automate and streamline processes based on the Information Technology Infrastructure Library (ITIL) framework for ITSM, which include ITAM, ITOM, and ITBM. The cloud-based platform shall include incident, problem, change, asset, and configuration management capabilities, along with

scalability, integration features, application programming interfaces (API), support for plug-ins and external connectors, and the ability to develop custom applications to meet VA's operational and security requirements.

The Contractor shall provide support and maintenance for the ERP solution, including regular updates, troubleshooting, and user training to ensure sustained performance and user adoption.

5.3.1 ITSM

The Contractor shall provide, configure, deploy and maintain SaaS-based ITSM capabilities (incident, problem, change, release, service request, service catalog, Configuration Management Database (CMDB), knowledge, etc., thereby improving overall IT service delivery and support, meeting VA business and technical requirements.

The Contractor shall provide ITSM with the following capabilities:

1. Enable notifications and alerts, accessible dashboards and reports, and track the status of IT services.
2. Incident Management capabilities to efficiently handle and resolve IT incidents.
    a. Provide incident logging, categorization, prioritization, and assignment.
    b. Provide automated notifications and escalations that can be configured based on Service Level Targets and SLA response times.
3. Problem Management capabilities to identify and manage the root causes of Major Incidents and recurring incidents.
    a. Provide capability to avert occurrences and recurrences of impactful incidents.
    b. Provide logging, categorization, and prioritization of problems.
    c. Provide root cause analysis tools and permanent solution documentation.
    d. Provide sustainable Known Error Database capabilities as an output of Problem Management practice
4. Change Management capabilities to enable and control the lifecycle of all changes to reduce risk and disruption.
    a. Provide logging, categorization, and assessment of change requests.
    b. Provide automated workflows for change approvals and tracking.
    c. Include functionalities for impact analysis, risk assessment, and change calendar management.
    d. Support Change Freezes and blackout periods.
        i. A change freeze is defined as a period of time where production environment changes, via Change Control, are stopped and only supported changes are allowed to proceed.
        ii. Typically, a change freeze or change blackout period is initiated during specific hardware/software upgrades on the affected system. This is a planned event that is communicated to all customers.

iii. A freeze can be enterprise wide, but usually only covers a specific system or service. The scope of a freeze/blackout can include all systems interfacing with the affected system/service and is planned, communicated, and executed by the product team performing the production upgrade functions.

e. Support Communications and Collaboration on the Change workflows.

f. This concerns the required change control activities associated with the service or system being changed in the production environment. The project team (Government Fulltime Equivalents (FTE) and contractors) are required to work together to complete all change control requests and communications for their system.

g. Each change request has a workflow and the common workflow steps require all project team members to be involved and meet all normal requirements involved in the workflow steps. Common required workflow steps include approvals, communications, planning steps, execution, testing, documentation, and close out of change requests.

5. Service Request Management capabilities to streamline the handling of user requests.
    a. Provide service request logging, categorization, and prioritization.
    b. Provide automated workflows for request fulfillment and approval processes.
    c. Include self-service capabilities for users to submit and track their service requests.
6. Knowledge Management module to create, manage, and share knowledge articles.
    a. Provide capability to create and maintain a knowledge base with categorized and searchable articles.
    b. Provide functionalities for article approval, feedback, and lifecycle management.
    c. Integrate with other ITSM modules to offer contextual knowledge during incident and service request resolution.
7. Service Catalog module to present a centralized list of available IT services.
    a. Provide users with capability to browse, request, and track the status of IT services.
    b. Include capabilities for service definition, approval workflows, and request fulfillment tracking.
    c. Ensure integration with the Service Request Management module for seamless service delivery.
8. CMDB to provide the capability to establish a comprehensive repository of configuration items (CI) and their relationships.
    a. Provide accurate and up-to-date data through automated discovery, integration and manual updates.
    b. Provide data certification and reconciliation functions to validate and clean CMDB data.
    c. Provide impact analysis functionality to support change management, and incident/problem resolution.

9. Service Level Management module to define, track, and manage SLAs.
    a. Provide the capability to allow for creation of SLAs with measurable metrics and targets.
    b. Provide functionalities for SLA monitoring, reporting, and breach notifications.
    c. Include capabilities for tracking the performance of IT services against defined SLAs.
10. Self-Service Portal to empower users to resolve their own issues; verify and update their own information; and make requests using forms, Chat Services, Virtual Agent Services, Generative and Agentic Ai, and other modern technological advances. The portal shall:
    a. Provide access to the service catalog, knowledge base, and request/incident tracking.
    b. Provide personalized user interfaces and intuitive navigation.
    c. Ensure mobile responsiveness for access from various devices.
11. Automated Release Management module to manage and automate the release of software and updates and shall:
    a. Provide the scheduling and tracking of releases, ensuring minimal disruption to services.
    b. Integrate with existing Continuous Integration and Continuous Delivery/Deployment (CI/CD) pipelines and deployment tools for seamless release automation.
    c. Provide functionalities for rollback management, release notes, and compliance reporting.

The Contractor shall ensure that Incident Management, Problem Management, Monitoring and Event Management, and Change Enablement/Management, are interoperable with each other and enable us to trend and analyze these relationships, such as incidents caused by change, root cause analysis and incident trend reporting.

5.3.2 ITAM

The Contractor shall configure, deploy, and maintain a SaaS-based ITAM platform module(s) to support the Department's enterprise-wide IT asset lifecycle needs. The ITAM solution shall be capable of scaling for a large, complex enterprise with a geographically distributed and remote workforce. The Contractor shall ensure seamless integration of ITAM with ITSM modules for incident, problem, and change management to include third party integrations. The Contractor shall Correlate asset data with incidents to expedite troubleshooting and resolution. The Contractor shall utilize asset data for impact analysis during change management processes.

The Contractor shall provide ITAM with the following capabilities:

1. Asset Repository to maintain a centralized database of all IT assets.
    a. Ensure accurate recording of asset details such as asset type, serial number, location, status, and ownership.
    b. Enable automated and manual updates to keep the repository current.

2. Asset Discovery tools to automatically identify and record IT assets across the organization's network.
    a. Ensure the discovery tool captures data from physical, virtual, and cloud environments.
    b. Perform scheduled discovery runs to maintain up-to-date asset information.
3. Lifecycle Management processes to track IT assets from procurement to disposal.
    a. Define stages for each asset's lifecycle, including acquisition, deployment, maintenance, and retirement.
    b. Enable workflows for lifecycle stages to automate transitions and approvals.
4. Software Asset management (SAM) to track and manage software licenses, usage, and compliance.
    a. Enable license tracking for various software types, including on-premises and cloud-based solutions.
    b. Provide functionalities for license reconciliation, renewal alerts, and compliance reporting.
5. Hardware Asset Management to track physical IT assets such as servers, laptops, and networking equipment.
    a. Ensure accurate details for each asset, including specifications, purchase date, warranty status, and maintenance history.
    b. Integrate hardware management with service management for incident and change correlation.
6. Contract Management to track vendor contracts, warranties, and agreements.
    a. Enable alerts for contract renewals, expirations, and compliance requirements.
    b. Provide functionalities for evaluating vendor performance and managing vendor relationships**.**
    c. Track vendor details, such as contact information, SLAs, and performance metrics.
    d. Enable the assessment of vendor reliability and effectiveness in providing goods and services.
    e. Integrate Vendor Management with asset and financial management for comprehensive oversight.
7. Financial Management to track the cost, depreciation, and financial impact of IT assets.
    a. Enable budget allocation and expense tracking for asset-related activities.
    b. Provide reports on asset depreciation, total cost of ownership, and return on investment.
    c. Support multi-fund and multi-year budgeting and financial management program.
8. Compliance Management to ensure IT assets meet regulatory and industry standards.
    a. Provide audit trails and reporting capabilities to track asset history, changes, and compliance status.

   b. Enable functionalities for internal and external audits, providing necessary documentation and reports.
9. Self-Service Portal to empower users to manage their assigned assets.
   a. Provide functionalities for submitting asset-related requests, tracking asset status, and performing self-audits.
   b. Ensure mobile responsiveness for access from various devices.

5.3.3 ITOM

The Contractor shall configure, deploy, and maintain a SaaS-based ITOM solution that enables enterprise-wide visibility, proactive monitoring, and optimization of IT infrastructure and services.

The Contractor shall provide ITOM with the following capabilities:

1. Discovery module to identify and map devices, applications, and services across the enterprise.
   a. Ensure Discovery accurately captures data from physical, virtual, and cloud environments.
   b. Set up scheduled discovery runs and configure patterns to match the existing environment.
   c. Validate and normalize discovered data to maintain data integrity and consistency**.**
2. Service Mapping to provide a comprehensive, real-time view of business services and their dependencies.
   a. Ensure accurate mapping of applications, services, and underlying infrastructure components.
   b. Regularly update and validate service maps to reflect current configurations and changes.
   c. Enable impact analysis to understand the potential effects of changes or incidents on business services.
3. Event Management to aggregate and correlate events from various monitoring tools and systems.
   a. Define event rules and thresholds to filter noise and highlight significant events.
   b. Integrate Event Management with existing monitoring tools such as Nagios, SolarWinds, or Splunk.
   c. Create actionable alerts and notifications for IT operations teams based on event severity and impact.
4. Operational Intelligence to analyze ITOM and real-time data, identifying trends and anomalies.
   a. Use AI/machine learning (ML) algorithms to detect patterns and predict potential issues before they occur.
   b. Set up dashboards and reports to provide insights into the health and performance of IT services.
   c. Facilitate proactive issue resolution through automated anomaly detection and alerting.

5. Orchestration to automate IT tasks and processes, reducing manual intervention and improving efficiency.
    a. Develop workflows to handle routine tasks such as user provisioning, software distribution, and patch management.
    b. Integrate Orchestration with external systems and applications to extend automation capabilities.
    c. Ensure compliance with organizational policies and standards while automating critical processes.
6. Cloud Management module to manage and optimize cloud resources across multiple providers.
    a. Enable provisioning, configuration, and governance of cloud assets through a single interface.
    b. Implement cost management and optimization features to control cloud spending and resource usage.
    c. Integrate Cloud Management with public and private cloud platforms such as AWS, Azure, and VMware.
7. Utilize the CMDB to maintain a comprehensive repository of CIs and their relationships.
    a. Ensure accurate and up-to-date data in the CMDB through automated discovery and service mapping.
    b. Implement data certification and reconciliation processes to validate and clean CMDB data.
    c. Use CMDB data for impact analysis, change management, and compliance reporting.
8. Integrate ITOM modules with the Change Management process to streamline change planning and execution.
    a. Use insights from Discovery, Service Mapping, and Event Management to assess change impacts.
    b. Automate change approval workflows and notifications to improve efficiency and reduce delays.
    c. Ensure changes are implemented with minimal disruption and maximum visibility into their effects.
9. Develop custom dashboards and reports to monitor ITOM activities and performance metrics.
    a. Provide real-time visibility into the health, performance, and status of IT services and infrastructure.
    b. Generate actionable insights for decision-makers to enhance operational efficiency and service delivery.
    c. Regularly review and update dashboards to align with evolving business needs and priorities.

5.3.4 ITBM

The Contractor shall configure, deploy, maintain a comprehensive IT Business Management capability that enables the VA to align technology investments with business strategy, optimize resources, and improve decision-making across the enterprise.

The Contractor shall provide ITBM with the following capabilities:

1. Project and Portfolio Management (PPM) capabilities to oversee and manage projects within the organization.
    a. Provide functionalities for project planning, execution, tracking, and reporting.
    b. Provide tools for portfolio management to prioritize and align projects with business objectives.
    c. Provide capabilities for resource allocation, risk management, and milestone tracking.
2. Demand Management capabilities to capture, assess, and prioritize incoming demands and requests.
    a. Provision of a centralized demand intake process to collect and evaluate business needs.
    b. Provision of tools for demand categorization, assessment, and approval workflows.
    c. Integration with PPM for seamless transition from demand capture to project initiation.
3. Financial Management capabilities to track and manage IT financials, including budgeting, forecasting, and cost tracking.
    a. Enablement of functionalities for cost transparency, chargeback/show back mechanisms, and financial planning.
    b. Provision of detailed financial reports and dashboarding capabilities to monitor IT spending and optimize IT investments.
    c. Integration of financial data with project and portfolio management for comprehensive financial oversight.
4. Resource Management capabilities to effectively allocate and optimize resources across projects and operations.
    a. Enablement of functionalities for resource planning, allocation, and capacity management.
    b. Provision of tools for skills management, resource forecasting, and utilization tracking.
    c. Integration with PPM to ensure optimal resource deployment and workload balancing.
5. Application Portfolio Management (APM) and Enterprise Architecture capabilities to manage and optimize the organization's application portfolio.
    a. Enable functionalities for application inventory, assessment, and rationalization.
    b. Provide tools to assess application value, cost, risks, and alignment with business objectives.
    c. Provide capabilities for setting application roadmaps and lifecycle management.
    d. Provide enhanced capabilities for enterprise modeling, visualization, and connection of business capabilities, technology, and data which enable VA

organizations to plan and manage the entire IT architecture, and therefore align with business strategy.

6. Agile Management capabilities to support agile methodologies and frameworks within the organization.
    a. Enablement of functionalities for backlog management, sprint planning, task tracking, and agile reporting.
    b. Provision of collaboration tools, agile boards, and dashboards to monitor agile team performance.
    c. Integration with PPM to align agile initiatives with broader project and portfolio goals.
7. Application Cost and Business Value Analysis to valuate total cost of ownership for applications and the ability to prioritize applications based on cost, risk, and alignment with enterprise goals.
8. Innovation Management capabilities to capture, evaluate, and develop innovative ideas within the organization.
    a. Enable functionalities for idea submission, evaluation, and prioritization.
    b. Provide tools for managing innovation pipelines, tracking progress, and assessing impact.
    c. Integrate with Demand Management to transition high-potential innovations into actionable projects.
9. Integration and Interface Management Capabilities to provide centralized management of integrations, interfaces, and system interactions including: documenting and assessing the purpose, dependencies, and risks of integrations across the enterprise.
10. Technology Portfolio Management capabilities to manage the lifecycle of enterprise technologies, identifying risks, compliance gaps, and exceptions including providing tools to evaluate business services and applications using technology inventories, audit data, and discovered information.
11. Reporting and Dashboarding capabilities to allow development of custom dashboards and reports to monitor ITBM activities and performance metrics including.
    a. Provide real-time visibility into project, portfolio, financial, resource, and agile management processes.
    b. Generate actionable insights for decision-makers to enhance strategic planning and execution.
    c. Regularly review and update dashboards to align with evolving business needs and priorities.

5.3.5 DIGITAL WORKPLACE

The Contractor shall configure, deploy, and maintain a Digital Workplaces designed to enhance productivity and streamline workflows by providing a unified, intuitive interface for users to perform their tasks more efficiently. The Digital Workplaces shall consolidate various functions, data, and applications into a single workspace to help users focus on their core responsibilities without the need to navigate multiple modules or screens.

The Digital Workplaces shall include the following key capabilities:

1. Provide a unified interface that combines multiple functionalities into a single, easy-to-navigate screen to include a cohesive user experience by integrating related tasks and data.
2. Provide the ability to create personalized dashboards that are configurable to display relevant metrics, reports, and tasks that users can tailor their workspace to show the information most pertinent to their role.
3. Provides real-time insights and analytics to help users make informed decisions.
4. Displays key performance indicators (KPI) and trends relevant to the user's responsibilities.
5. Centralized task lists and calendars to manage and prioritize work.
6. Allows users to track the status of their tasks and collaborate with team members.
7. Seamless integration with other applications and third-party tools.
8. Enable users to carry out a wide range of activities without switching contexts.
9. Displays relevant contextual information and data points related to the task at hand.
10. Facilitates better understanding and faster resolution of issues.
11. Optimized for use across different devices, including desktops, tablets, and smartphones.
12. Ensures consistent and efficient user experience on any device.

5.3.6 CSM

The Contractor shall configure, deploy, maintain a comprehensive Customer Service Management (CSM) solution that supports end-to-end case management, omnichannel customer engagement, and cross-team collaboration. The platform must include integrated knowledge management, AI/ML-driven automation and virtual agents, proactive monitoring and alerting, configurable workflows, and unified agent workspaces to improve efficiency and service delivery. Additionally, the solution should support integrations with related SaaS modules, customer and partner self-service portals, SLA and contract management, workforce productivity tools, and robust dashboards and reporting capabilities to enhance customer satisfaction, operational performance, and continuous improvement. The CSM module shall provide capabilities to both internal and external stakeholders, including customers outside of the VA network (e.g., Veterans).

The Contractor shall provide the following CSM capabilities:

1. Provide Case Management tools for tracking, managing, and resolving customer cases.
2. Enable linking of cases to related resources, records, or services.
3. Support collaboration across multiple teams for issue resolution.
4. Deliver OmniChannel Support to seamlessly provide customer interactions across channels including email, chat, web portal, phone, and social media
5. Ensure case continuity when customers switch between channels.
6. Provide a centralized knowledge base to store and share articles, Frequently Asked Questions (FAQ), and solutions.

7. Enable customers and service agents to quickly locate relevant information for faster resolution.
8. Provide a unified interface where customer service representatives can access cases, history, knowledge articles, and communication tools.
9. Ensure the workspace improves efficiency through streamlined navigation and automation.
10. Support integration with other SaaS platform modules such as ITSM, ITOM, and Field Service Management (FSM).
11. Enable cross-departmental workflows to provide a complete view of customer interactions and service delivery.
12. Monitor products, services, and customer activity to proactively detect and address potential issues before they impact end users.
13. Provide automated alerts and workflows to initiate resolution activities.
14. Use AI/ML to route cases, recommend solutions, and identify patterns or trends in customer activity.
15. Provide self-service recommendations to reduce manual intervention.
16. Provide dashboards and reporting tools to measure customer satisfaction, service efficiency, and compliance with SLAs.
17. Enable leadership to identify areas for improvement in customer service delivery.
18. Provide AI-driven virtual agents capable of handling routine inquiries, requests, and transactions.
19. Ensure the virtual agent escalates to a live representative for more complex cases.
20. Provide tools to manage team productivity, assign cases based on skill sets, and monitor workload distribution.
21. Support scheduling, training identification, and performance evaluation of customer service staff.
22. Provide customer and partner portals for self-service, request tracking, and engagement.
23. Support communities, forums, and peer-to-peer collaboration for shared knowledge.
24. Provide capabilities to manage service contracts, entitlements, and SLAs.
25. Ensure cases and requests are linked to the appropriate customer accounts, products, or services.
26. Provide configurable workflows to handle complex case management processes.
27. Support multi-step approvals, escalations, and automation to ensure timely resolution

5.3.7 SecOps

The Contractor shall configure, deploy, maintain a comprehensive Security Operations solution that enables security incident response, threat intelligence integration, vulnerability and risk management, patch orchestration, and enterprise-wide incident coordination. The platform must support centralized visibility into incidents, threats, vulnerabilities, and asset intelligence through integrations with enterprise security tools and Armis within the existing CMDB architecture. Additionally, the solution should include automated workflows, predefined response plans, executive dashboards,

compliance reporting, and cross-team collaboration capabilities to improve threat detection, mitigation, security posture management, and operational resilience.

The Contractor shall provide Security Operations with the following capabilities:

1. Provide Security Incident Response tools and workflows to detect, investigate, and respond to security incidents.
2. Enable execution of predefined response plans to ensure consistent and timely mitigation of threats.
3. Support integration of multiple threat intelligence feeds into the platform.
4. Correlate threat data with enterprise activity to enhance situational awareness and accelerate response.
5. Provide a vulnerability response and risk management capability to track, prioritize, and remediate security weaknesses.
6. Provide an application vulnerability management to identify and mitigate risks within deployed software.
7. Provide patch orchestration workflows to streamline updates, reduce risk exposure, and maintain compliance.
8. Provide integrated risk management features to evaluate and manage enterprise risks aligned to security frameworks and policies.
9. Enable processes for managing large-scale or critical security incidents.
10. Provide escalation workflows, communication tracking, and cross-team coordination to contain and resolve incidents effectively.
11. Provide executive-level dashboards to track incident trends, vulnerabilities, patching status, and overall security posture.
12. Enable exportable reports to support compliance, audits, and leadership briefings.
13. Provide integration bundles to connect with enterprise security tools (e.g., SIEMs, monitoring solutions, endpoint protection systems).
14. Provide centralized security capabilities to consolidate incident, threat, and vulnerability information into a unified view.
15. Integrate Armis as a primary asset intelligence and exposure-management source into the existing CMDB architecture, ensuring alignment with VA's multi-source CMDB strategy and authoritative-source direction. Integration shall support ingestion of asset inventory, device profiling, behavioral risk indicators, and security-relevant metadata from Armis into native CMDB classes and relationships, consistent with enterprise governance requirements.

5.3.8 INTEGRATED RISK MANAGEMENT

The Contractor shall configure, deploy, maintain a comprehensive Integrated Risk Management (IRM) solution that supports business user engagement, advanced risk and compliance management, and enterprise-wide integration capabilities. The platform must enable policy exception approvals, compliance case management, risk monitoring, business continuity and crisis management workflows, and centralized access to policies and compliance activities. Additionally, the solution should provide advanced risk analysis, automated audit and third-party risk management, privacy and ESG oversight, AI-driven compliance automation, executive dashboards, and configurable

reporting. The IRM platform must also integrate with enterprise systems such as ITSM, SecOps, and CSM while offering pre-built templates and accelerators aligned to frameworks such as NIST, FedRAMP, ISO, and HIPAA to streamline implementation and regulatory compliance.

The Contractor shall provide Integration Risk Management with the following capabilities:

1. Core Business User Tasks:
    a. Provide functionality for business users to approve policy exceptions, evidence requests, and advanced risk assessments.
    b. Enable users to report new compliance cases (e.g., policy violations) and view or respond to existing issues.
    c. Allow users to respond to automated tasks generated by Key Risk Indicators (KRI) and related risk monitoring activities.
    d. Provide access to IRM processes through a centralized portal where employees can view policies, submit requests, and track compliance activities.
    e. Provide the ability for users to view, download, and update the status of business continuity and disaster recovery plans during exercises and real crisis events.
    f. Enable participation in workflows for Business Impact Analysis (BIA), Business Continuity Planning (BCP), and crisis management, including reviewing and approving analysis outputs.
2. Advanced Risk and Compliance Management:
    a. Provide advanced quantitative and qualitative risk analysis tools to identify, measure, and mitigate risks.
    b. Provide centralized policy and compliance management processes for creating, approving, and managing policies, standards, procedures, and regulatory requirements.
    c. Automate the audit management lifecycle, including planning, scheduling, fieldwork, findings, and reporting.
    d. Provide capabilities to assess, monitor, and mitigate risks posed by third-party vendors and partners.
    e. Include modules for managing privacy obligations, Environmental, Social, and Governance (ESG) requirements.
    f. Utilize advanced automation and AI to provide issue summarization, accelerate system certifications, enable continuous compliance monitoring, and automate regulatory update tracking.
    g. Provide executive cybersecurity and compliance dashboards and customizable reporting for risk metrics, compliance posture, audit outcomes, and security trends.
    h. Provide advanced workflows and accelerators for business continuity, crisis management, and resilience planning.
3. Integration, Reporting, and Accelerators

a. Enable cross-platform integration with ITSM, SecOps, CSM, and other enterprise systems to ensure risk data informs operational processes.
b. Provide configurable reports, dashboards, and visualizations to analyze compliance and risk data at multiple organizational levels.
c. Provide pre-built content, templates, and use case accelerators for frameworks (e.g., NIST, FedRAMP, ISO, HIPAA) to speed implementation and compliance alignment.

5.3.9 INTEGRATION CENTER

The Contractor shall configure, deploy, maintain a comprehensive Integration Center solution that supports secure, scalable, and highly available integrations across VA enterprise systems, cloud services, SaaS platforms, and external partners. The platform must support standard APIs and protocols, pre-built and custom connectors, workflow-driven orchestration, event-driven automation, data transformation and mapping, and API management capabilities. Additionally, the solution should provide robust monitoring, logging, governance, and compliance controls aligned with FedRAMP High, FISMA, and HIPAA requirements, while enabling hybrid and multi-cloud integration. The platform must also include visual low-code/no-code workflow and integration design tools to allow users to automate processes, manage APIs, and facilitate seamless data exchange across IT and business systems. The Contractor shall support seamless integration and real-time data sharing across multi-instances.

The Contractor shall provide the following integration center capabilities and support all modules and their associated requirements.

1. Support Standard Protocols and APIs:
    a. Provide Representational State Transfer (REST), Simple Object Access Protocol (SOAP), Open Data Protocol (OData), and open-source query language (GraphQL) APIs to have the capability to connect to internal VA systems and external partner systems.
    b. Ensure backward compatibility and API version management.
2. Enable Pre-Built and Custom Connectors:
1. Deliver pre-built connectors for common federal systems, cloud services, and Commercial Off-The-Shelf (COTS) applications.
    a. Allow VA technical staff to build and manage custom connectors through a low-code/no-code environment.
    b. Provide ability to create custom integrations by building actions and connectors for VA internal and external systems.
3. Provide Secure Data Exchange:
    a. Ensure all integrations comply with VA security and data governance requirements (FedRAMP High, FISMA, HIPAA).
    b. Provide encryption in transit and at rest.
    c. Enforce role-based access controls for integration activities.
4. Support Orchestration and Automation:
    a. Enable workflow-driven integrations that allow business and IT users to automate cross-platform processes.

b. Provide event-driven triggers for real-time data exchange.

5. Offer Monitoring and Logging:
    a. Deliver dashboards for real-time monitoring of integration health, throughput and status.
    b. Maintain detailed logs for compliance, troubleshooting, and auditing.
    c. Users should be able to view logs, track errors, and analyze the flow of data through their integration workflows, facilitating troubleshooting and maintenance
6. Ensure Scalability and High Availability:
    a. Support enterprise-level scale across 600,000+ VA users and multiple VA systems.
    b. Provide load balancing and failover capabilities to ensure uninterrupted integration services.
    c. Support asynchronous processing and parallel execution of tasks to ensure optimal performance.
7. Facilitate Data Transformation and Mapping:
    a. Provide native tools for data normalization, schema mapping, and transformation between systems with different data models.
    b. Provide user capability to map fields, apply transformations, and validate data as part of their integration workflows.
8. Support Hybrid and Multi-Cloud Environments:
    2. Allow seamless integration between on-premises VA systems, SaaS tools, and cloud-based services (IaaS/PaaS/SaaS).
    3. Allow seamless integration and real-time data sharing across multi-instances. Data and transaction synchronization between instances with minimal latency.
9. Enable Governance and Compliance:
    a. Provide governance tools for managing integration lifecycles.
    b. Track ownership, approvals, and compliance with VA IT governance policies.
10. Provide API Management tool:
    a. Provide tools for managing and securing APIs.
    b. The tool shall include the capabilities for creation, publication, and monitoring of APIs, ensuring secure and reliable communication between systems.
    c. Ability to integrate the VA SaaS platform ERP products with VA enterprise systems (identity management, Human Resources (HR), monitoring, asset management, etc.) using secure APIs.
11. The tool shall have capabilities to handle authentication, authorization, and token management. Provide Visual Workflow Designer and Flow Designer Integration tool:
    a. Integration Center should be able to integrate with Flow designer and Visual Workflow designer for automating processes and tasks through flows, to incorporate integration actions into flows, enabling seamless data exchange and process automation between different systems.

b. Provide capability to users to design and execute integration workflows using a visual, drag-and-drop interface.
c. Support custom integrations with other IT and business tools.

5.3.10 REPORTING AND ANALYTICS

The Contractor shall configure, deploy, and maintain a comprehensive Reporting and Analytics solution that delivers ITIL-aligned out-of-box reporting, customizable dashboards, near real-time operational metrics, and advanced data visualization capabilities accessible across desktop and mobile platforms. The platform must support self-service and ad hoc reporting, role-based access controls, automated scheduling and alerting, cross-module data correlation, and integration with enterprise BI tools and data warehouses. Additionally, the solution should provide data standardization and transformation capabilities, predictive and prescriptive analytics powered by AI/ML, compliance and audit reporting, historical data retention, and accessible, user-friendly interfaces compliant with Section 508 and WCAG 2.1 standards.

The Contractor shall provide the following Reporting and Analytics capabilities:

1. Provide pre-built, out-of-box (OOB) reports aligned with ITIL practices, including:
    a. Incident Management
    b. Problem Management Change Management
    c. Request Fulfillment
    d. Configuration Management
    e. Service Level Management
2. Knowledge Management comprised of a user-friendly interface that allows authorized users to create, modify, and save custom reports without requiring advanced programming skills.
3. Enable templates to be stored, shared, and reused by authorized personnel
4. Provide role-based access controls to ensure users only view or edit reports relevant to their assigned roles and permissions.
5. Provide dashboarding and data visualization Configurable, role-based dashboards composed of customizable widgets Multiple visualization types include charts, graphs, heat maps, service maps, trend lines, and tabular formats.
6. Support for access to dashboards from desktops, tablets, and mobile devices.
7. Provide near real-time automated metrics.
8. Provide near real-time data updates for operational monitoring.
9. Provide scheduling automated report generation and delivery via email or other approved methods.
10. Provide configurable alerting capabilities when SLA thresholds are breached.
11. Produce operational and strategic performance metrics, including SLA/Operational Level Agreement (OLA) compliance, backlog trends, resolution and fulfillment times, volumes, transactional changes (e.g., re-assignments, re-openings), and customer satisfaction scores.

12. Provide ad hoc querying and analysis allowing authorized users to perform ad hoc queries with advanced filtering, grouping, and sorting in a controlled fashion that will not impede operational performance.
13. Support pivot-style data analysis and cross-module data correlation (e.g., incidents, problems, changes, CMDB).
14. Provide non-technical language query capability to simply data analysis for non-technical users.
15. Provide information delivery and sharing:
    a. Ability to export reports and dashboards in multiple formats including PDF, Excel, CSV, HTML, and image formats.
16. Allow embedding or linking reports within other enterprise platforms (e.g., intranet, SharePoint, collaboration tools).
17. Provide secure, role-based self-service access for authorized users to retrieve reports without administrative intervention.
18. Provide API-based access to reporting data for integration with other authorized enterprise systems.
19. Provide Business Intelligence (BI) and data integration:
    a. Provide native or connector-based integration with enterprise BI platforms (e.g., Power BI, Tableau, Qlik) as approved by the VA.
20. Support export or synchronization of ITSM data to federal data warehouses or data lakes.
21. Collect data from multiple sources, standardize, cleanse, and transform it.—applying filtering, corrections, and conflict resolution—to ensure consistency and readiness for analysis.
    a. Load the processed data into a designated target system such as a data warehouse, database, or data lake, making it accessible for reporting, dashboards, and data visualization.
22. Provide Predictive and Prescriptive Analytics:
    a. Support trend analysis to identify patterns that could lead to service degradation and/or inefficient service delivery.
    b. Provide forecasting capabilities for ticket and transactional volumes, resource demand, and incident likelihood.
    c. Provide AI/ML-assisted insights for problem resolution, process improvement, and risk mitigation.
    d. Provide automated root cause identification capabilities that correlate events, incidents, changes, and outages.
23. Provide compliance and audit support:
    a. Maintain audit logs for reporting and analytics activities.
    b. Produce compliance-ready reports in alignment with applicable standards (e.g., ITIL, ISO 20000, IS27001, FedRAMP).
    c. Retain and provide historical performance data for required retention periods.
24. Provide user experience and accessibility:
    a. Provide an intuitive reporting interface requiring minimal training for basic report creation.

b. Comply with Section 508 and Web Content Accessibility Guidelines (WCAG) 2.1 accessibility standards.

5.3.11 PLATFORM TOOLS

The Contractor shall provide, configure, deploy, and maintain a comprehensive enterprise platform ecosystem that includes foundational data management aligned to CSDM, secure authentication, DevSecOps and CI/CD pipelines, low-code/no-code rapid application development tools, workflow automation, integration capabilities, and scalable processing server infrastructure. The platform must support robust monitoring, performance optimization, plugin and subscription management, encryption, import/export functionality, automated testing services, code health and application health scanning, and centralized administration with RBAC and MFA controls. Additionally, the solution must ensure seamless integration with existing VA systems, support scalable and resilient operations, maintain compliance with federal security and accessibility standards, and provide comprehensive documentation, training, backup and recovery, and ongoing support and maintenance services.

The Contractor shall provide, configure, deploy and maintain the following set of core comprehensive platform tools:

1. Core Foundational Tables:
    a. Implement and configure core foundational tables aligning to Common Service Data Model (CSDM) to support enterprise organizational data needs.
    b. Ensure tables are designed to maintain data integrity, consistency, and scalability.
    c. Develop data models and schemas aligning with existing business processes and workflows.
    d. Develop a data certification model governance to maintain the data integrity.
    e. Implement data validation and normalization processes to maintain accurate records.
    f. Integrate Single Sign-On (SSO) and Entra ID login for secure and seamless user authentication.
2. DevSecOps Pipeline:
    a. Develop and implement a DevSecOps pipeline integrating security at every stage of the development lifecycle.
    b. Utilize an Automated Testing framework to create and manage automated test scripts for continuous testing.
    c. Ensure the pipeline supports automated code scans, security testing, and vulnerability assessments.
    d. Integrate the platform with existing development tools and repositories (e.g., GitHub, GitLab).
3. CI/CD Pipeline:
    a. Implement a robust CI/CD pipeline.

b. Automate the build, test, and deployment processes to ensure efficient and reliable code releases.
c. Integrate CI/CD tools with automated testing, static code analysis, and security scanning tools.
d. Enable rollbacks and version control to manage code changes and deployments effectively.

4. Application Engine Suite Capability (Rapid Application Development Tools):
    a. Support both custom and low code application development:
    b. Provide a platform for building custom applications without the need for extensive coding.
    c. Provide low-code/no-code development tools to enable rapid application development by users with varying technical skills.
    d. Allow for the creation, modification, and deployment of applications through an intuitive interface such as Creator Studio.
    e. Provide drag-and-drop capabilities to design user interfaces, workflows, and data models-Enables end-users to create and customize applications without extensive coding knowledge.
    f. Ensure tools are user-friendly, secure, and comply with organizational standards and policies.
    g. Provide a platform for developing and hosting web applications at scale. This should include both Low code and pro code web applications.
    h. Provide seamless integration capability with existing VA systems and databases
    i. Pre-Built Components and Templates:
        i. Provide a library of pre-built components and templates to accelerate application development.
        ii. Allow customization of these components and templates to align with VA specifications.
    j. Workflow Automation:
        i. Support the automation of business processes through built-in workflow tools.
        ii. Enable the creation of complex workflows involving multiple steps and conditions.
        iii. Provide tools for monitoring and managing these automated workflows.
    k. Application Engine Management:
        i. Provide real-time monitoring and performance analytics for custom applications.
        ii. Enable efficient application maintenance, updates, and version control.
        iii. Provide automated backups and disaster recovery mechanisms.
5. Integration Spokes:
    a. Implement integration spokes to connect systems and applications.
    b. Develop custom spokes where necessary to meet specific integration requirements.

c. Ensure seamless data flow and process automation across integrated systems.
d. Maintain up-to-date documentation and support for all integration points.

6. Platform Performance Monitoring Tools:
    a. Implement real-time monitoring dashboards to provide visibility into system performance, usage, and issues.
    b. Set up alerts and notifications for performance anomalies and potential issues.
    c. Conduct regular performance reviews and optimize configurations to maintain optimal performance levels.
7. Workflow Scheduler: The Contractor shall provide capability to automate various processes and workflows.
8. Notifications: The Contractor shall provide and configure capability to send and receive emails and SMS type notification in Production and non-production instances.
9. Import / Export functionalities: Provide data import/export functionalities and provide robust tools for data manipulation.
10. Encryption: The Contractor shall provide encryption capability to safeguard PII and PHI data.
11. Code Health Scan Ability:
    a. Implement tools for automated code health scanning within the environment.
    b. Conduct regular static code analysis to identify code quality issues, security vulnerabilities, and compliance violations.
    c. Integrate code health scans into the CI/CD pipeline to ensure ongoing code quality.
    d. Provide detailed reports and remediation recommendations for identified issues.
12. Health Scan Tools:
    a. Deploy health scan tools to continuously monitor the health of the software applications and infrastructure.
    b. Configure the tools to perform regular health checks, diagnostics, and generate actionable insights.
    c. Ensure health scan tools integrate seamlessly with performance monitoring and DevSecOps pipelines.
13. Plugin Management:
    a. Plugin Management System within the ERP tools to manage Out of the box plugins and third-party plugins and extensions.
    b. Enable seamless installation and configuration of third-party plugins.
    c. Compatibility and integration with the ERP tool’s core functionalities.
    d. Managing the lifecycle of plugins, including updates and decommissioning.
    e. Monitor and report on plugin performance and usage.
14. Subscription Management:
    a. Provide users with capability to subscribe and manage their access to services.

b. Track and report on subscription utilization and costs.

15. Admin Center Capability:
    a. Provide an Admin Center – a single pane within the ERP tool to centralize administrative functions and streamline management tasks.
        i. Manage user accounts, roles, and permissions centrally.
        ii. Ensure Roles Based Access Controls (RBAC) are available and in compliance with governance policies, and multi-factor authentication is in alignment with VA cybersecurity policies for Production and Non-Production Instances.
        iii. Facilitate system configuration, updates, and maintenance from a unified interface.
        iv. Provide tools for monitoring system performance and health.
        v. Provide comprehensive administrative capabilities for monitoring, managing, and maintaining platform health, including platform upgrades, cloning, patches, and performance tuning
16. Automation Testing Services
    a. Provide capabilities to ensure effective management of automation testing, tools and processes.
    b. Tools and Processes:
        i. Provide, configure, deploy and maintain automation testing tools and frameworks (e.g., ATF, Selenium, JUnit, Jenkins, etc.).
        ii. Establish, maintain, and update a repository of automated test scripts.
        iii. Ensure that the automation testing framework remains compatible with evolving technologies and software updates.
    c. Test Automation Execution:
        i. Develop, maintain and execute automated test cases covering functional, regression, integration, and performance testing including load testing.
        ii. Ensure automation scripts are designed to run in CI/CD environment.
        iii. Provide support for maintaining and updating test scripts as the software under test evolves.
    d. Defect Management and Reporting:
        i. Provide and maintain Defect management tools and processes.
        ii. Provide detailed defect reports and root cause analyses for identified issues.
        iii. Track the resolution of defects and conduct subsequent retesting as required.
    e. Quality Assurance and Compliance:
        i. Maintain compliance with federal standards, 508 standards and guidelines related to software testing and quality assurance.
        ii. Conduct periodic reviews of the automation testing strategy and make improvements as necessary to enhance efficiency and coverage.

iii. Ensure all test activities are documented and accessible according to VA policies and protocols.

17. Processing Servers Infrastructure & Discovery Agents:
    a. Provide multiple agents/probes for on-premises access. The Contractor shall provide, establish and maintain a set of servers that ensures processing of scalable and seamless integration, data flow, and automation within the organization's infrastructure.
    b. The Contractor shall install a lightweight application to locally and securely relay commands and retrieve data between the platform and internal systems, such as databases, devices, applications, or other cloud/on-prem IT resources.
    c. Processing Server Capability:
        i. Provide scalable agent probes for on-premises access
        ii. Provide redundancy and cluster capability
        iii. Support VA discovery custom applications
        iv. Centrally managed from the Platform
        v. Integrate seamlessly with the ERP Platform.
        vi. Provide a messaging bus
    d. Servers Provisioning:
        i. Provision a Server that matches the specifications of the current environment.
        ii. Ensure compatibility with existing systems, applications, and network infrastructure.
        iii. Perform initial configuration and setup to align with current operational standards.
    e. Tools Integration:
        i. Integrate the Server with existing IT tools such as monitoring systems, ITSM platforms, data analytics tools, and other enterprise applications.
        ii. Ensure all existing integrations are replicated and remain functional.
        iii. Perform testing to validate integration points and ensure data integrity and reliability.
    f. Process Mapping and Replication:
        i. Document existing processes that interact with the current Mid Server.
        ii. Replicate these processes on the new Server, ensuring no disruption to current operations.
        iii. Adjust configurations as necessary to match current operational workflows.
    g. Security and Compliance:
        i. Implement security measures to protect data in transit and at rest.
        ii. Ensure the Server complies with organizational security policies and regulatory requirements.
        iii. Regularly update and patch the Server to address security vulnerabilities.

h. Monitoring and Management:
    i. Implement monitoring tools to track the performance, availability, and health of the Server.
    ii. Set up alerts and notifications for any performance issues or service disruptions.
    iii. Ensure the Server is managed continuously to maintain optimal performance levels.
i. Data Transfer and Synchronization:
    i. Ensure data transfer processes between the Server and existing systems are reliable and efficient.
    ii. Set up data synchronization mechanisms to maintain data consistency across all integrated systems.
    iii. Perform regular data integrity checks and resolve any discrepancies promptly.
j. Documentation and Training:
    i. Provide comprehensive documentation covering Server setup, configurations, integrations, and processes.
    ii. Offer training sessions for IT staff to ensure they are proficient in managing and operating the Server.
    iii. Keep documentation updated with any changes or upgrades.
k. Backup and Recovery:
    i. Implement backup solutions to safeguard Server configurations and data.
    ii. Establish a disaster recovery plan to ensure quick restoration of services in case of server failure.
    iii. Conduct regular backup and recovery tests to ensure the effectiveness of the recovery plan.
l. Support and Maintenance:
    i. Provide ongoing support for the Server, including troubleshooting and issue resolution.
    ii. Offer maintenance services to keep the Server updated and functioning optimally.
    iii. Maintain an SLA that outlines response times and resolution times for support requests.
m. Performance Optimization:
    i. Regularly review Server performance metrics and implement optimizations as needed.
    ii. Ensure the Server can scale according to organizational growth and changing requirements.
    iii. Continuously evaluate and improve processes to enhance efficiency and performance.
n. Technology Modernization and Innovation:
    i. The Contractor shall maintain the ERP solution in a current, secure, and fully supported state throughout the period of performance.
    ii. The Contractor shall provide access to and implement all standard OEM platform enhancements, security updates, performance

improvements, workflow automation capabilities, analytics capabilities, and AI capabilities included within the Government's licensed subscription at no additional cost to the Government.

iii. The Contractor shall maintain upgrade readiness and support implementation of OEM-supported releases within Government-approved timelines.

5.3.12 MOBILE

The Contractor shall configure, deploy, maintain a fully functional mobile application(s) for the ERP platform that supports secure, role-based access for both end users and support personnel. The mobile solution shall operate seamlessly across iOS and Android devices and deliver functionality comparable to the web-based platform experience. The Contractor shall provide services to implement and manage a comprehensive mobile solution, ensuring robust functionality, integration, security, performance, and user experience. The Contractor shall provide 99.99% uptime for mobile availability.

The Contractor shall provide the following Mobile capabilities and support all ERP modules and their associated requirements:

a. Submit, view, assign and update all ERP tool record types, track all records statuses in real time, and receive push notifications for status changes, approvals, or required user actions.
b. Search and view knowledge articles, FAQs, and self-help resources, and to bookmark or save frequently used articles.
c. Access to a virtual agent for automated assistance and the ability to launch commonly used self-service functions, such as password resets or account unlocks.
d. View Reports and Dashboards
e. View your work and your team’s work
f. Provide real time synchronization of data to mobile and web views.
g. Support Push notifications delivered within one minute of a status change based on notification preferences.
h. Create, view, assign, and update all ERP tool records, changes, and tasks; add work notes, comments, or attachments via mobile device.
i. Receive and process approvals for all applicable record types, and other workflow tasks; and notifications of pending approvals delivered in real time.
j. Monitoring alerts, receive and respond to critical priority notifications.
k. View dashboards or summaries for assigned queues or teams;
l. Support configurable branding (logos, color schemes) to align with Department of VA enterprise standards, and a customizable home screen to highlight VA-specific services, FAQs, or announcements.
m. Support role-based views, mainly tailored mobile views for end users vs. support personnel, with role-based menus, and dashboards aligned to VA governance.
n. Add, modify, or hide mobile functions without requiring vendor code changes and support for workflow automation and low-code/no-code configuration.

o. Configurable to support key business processes, customize pre-built components and templates to meet specific organizational needs, and ensure seamless interface with existing enterprise platform instances.
p. Support encryption, authentication, and authorization; support SSO and Multi-Factor Authentication (MFA).
q. Support security scans to detect vulnerabilities on the Mobile platform.
r. Provide an intuitive and user-friendly interface and ensure consistent experience across different devices and platforms.

5.3.13 PRODUCTION INSTANCES

The Contractor shall configure, deploy, maintain a FedRAMP high robust and scalable secure cloud infrastructure capable of supporting approximately 600,000 end users, processing millions of transactions monthly, and managing tens of thousands of concurrent workflow activities. The Contractor shall provide multiple production instances to support Multi Instance Architecture. The Contractor shall design the Cloud Computing Platform to operate within the VA production environment (e.g., ITSM, CSM, GRC) with 99.99% uptime availability and built-in resilience to ensure uninterrupted service delivery. The Contractor shall provide unique configurations that align with the scale and complexity of the VA's enterprise-level operations. The Contractor shall provide multiple production instances and support aligning them to multi-instance architecture. The Contractor shall provide and maintain SaaS production instances within the VA enterprise platform. These environments shall be provisioned, secured, and managed in accordance with VA enterprise and federal standards.

The Platform Cloud Environment shall meet the following requirements:

1. Data Security and Compliance:
   The Contractor Shall:
   a. Ensure data is encrypted with strong security measures.
   b. Implement role-based access controls and security rules to ensure data access is limited to authorized personnel.
   c. Ensure the platform complies with requirements such as HIPAA (for healthcare) and undergoes third-party audits like ISO 27001 and SOC 2.
   d. Ensure the platform meets FedRAMP high security policies and controls.
   e. Comply with Section 508 and WCAG 2.1 accessibility standards.

2. High Availability and Disaster Recovery:

   The Contractor Shall:
   a. The Contractor shall utilize a multi-instance/redundant architecture with Data Centers for advanced high availability and disaster recovery. The Data centers should support geographic redundancy
   b. The Contractor shall ensure real-time database replication between Data Centers to keep data in sync.
   4. The Contractor shall implement automated failover procedures that can recover data and restore service in case of disruptions.

5. The Contractor shall maintain 99.99% uptime availability across all Production Instances.

3. Storage and Database Management:

   The Contractor Shall:
   a. Provision scalable storage to handle large volumes of data, ensuring high availability and performance.
   b. Optimize database performance, ensuring efficient data retrieval and management.
   c. Adjust storage and database configurations to accommodate growing data volumes and user activity.

4. Platform Performance Management:

   The Contractor Shall:
   a. Design platform instances for high performance with redundant components
   b. Manage platform nodes, scaling up or down as necessary to meet performance and capacity requirements.
   c. Implement load balancing to ensure even distribution of workload across nodes.

5. Data Retention:

   The Contractor Shall:
   a. Implement data retention policies that comply with VA regulations and ensure data is retained for the required periods as stated in the general records schedule.
   b. Provide mechanisms for secure data archival and ensure archived data remains accessible for the duration of the retention period.
   c. Ensure that data is securely deleted or anonymized after the retention period has elapsed, in accordance with VA data handling policies.
   d. Provide access to the retained data and prevent unauthorized access and protection of sensitive data.
6. Cloning and Data Management:

   The Contractor Shall:
   a. Provide the ability to clone production data into non-production instances to support development and validation activities.
   b. Apply masking, anonymization, or redaction of sensitive data (PII, PHI, or VA-sensitive data) to meet VA privacy and security requirements.
   c. Support clone exclusions

7. Security and Compliance:

The Contractor Shall:

a. Implement all applicable security and compliance controls in production, including FedRAMP High, FISMA, HIPAA, and VA-specific requirements.
b. Enable audit logging, vulnerability monitoring, and compliance reporting consistent with production standards.
c. Provide system performance benchmarks demonstrating at least 99.99% uptime availability and scalability to support 600,000+ users and millions of monthly transactions.

5.3.14 NON-PRODUCTION INSTANCES

The Contractor shall configure, deploy, maintain and maintain SaaS non-production instances within the VA enterprise platform to support activities such as development, testing, training, and prototyping for multiple Software Development Life Cycle (SDLC) pipelines to support segregated production environments. These environments shall be provisioned, secured, and managed in accordance with VA enterprise and federal standards.

The non-production instances shall contain all the items listed under Platform tools section and include the following additional capabilities:

1. Email Sending Capabilities (Configurable):

   The Contractor Shall:

   a. Ensure that non-production instances have the ability to send emails to a specific test email address.
   b. Provide a capability to turn off the emails being sent and view the email logs to validate the actual email being sent.
   c. Ensure no test emails are sent to production or external recipients.

2. Cloning from non-production:

   The Contractor Shall:

   a. Provide the ability to clone non-production data to other non-production Instances for testing and development purposes.
   b. Support clone exclusions.

3. Security and Compliance:

   The Contractor Shall:

   a. Implement all applicable security and compliance controls in non-production instances, including FedRAMP High, FISMA, HIPAA, and VA-specific requirements.
   b. Enable audit logging, vulnerability monitoring, and compliance reporting consistent with production standards.

4. Standard Non-Production Environment Features:

The Contractor Shall:

a. Provide environments for the development and testing of custom applications, workflows, and configurations.
b. Provide environments for testing new releases, patches, and enhancements before deployment to production.
c. Provide safe environments for training administrators, developers, and end-users.
d. Provide environments for prototyping and user research.
e. Provide separate instances for the Software Development Life Cycle (SDLC), including development, testing, pre-production, deployment, distributed development, and training SDLC pipelines to support multiple production instances.
f. Provide dedicated instances for running pilots and proofs of concepts.
g. Provide SDLC instances for low code/no code application development.
h. Support multiple concurrent development environments.
i. Provide instances dedicated to testing platform upgrades.
j. Provide instances specifically for cloning data from production.
k. Provide instances used for backup and recovery testing.

5. Platform Performance Management:

The Contractor Shall:

a. Ensure high-performance non-production instances with load balancing and redundant components.
b. Provide scalable storage solutions to accommodate growing data volumes in non-production instances.
c. Continuously optimize database performance in non-production environments to handle growing data and transaction volumes.
d. Dynamically adjust nodes within non-production environments to handle increasing or fluctuating workloads.

5.3.15 PLATFORM PERFORMANCE TESTING INSTANCE

The Contractor shall provide and maintain a Platform Performance Testing Instance within the VA enterprise SaaS platform. This environment shall be used to simulate application performance under various operational conditions, validate system responsiveness, and ensure that VA applications meet enterprise-level performance standards.

The Contractor shall:

1. Provision a dedicated Platform Performance Testing Instance separate from production and non-production environments.
2. Configure this instance to replicate production-scale workloads, user traffic, and data volumes to support accurate performance testing.

3. Simulate and test application performance under various operating conditions, including peak usage scenarios.
4. Execute load, stress, and scalability tests to assess response time, throughput, error rates, and transaction handling capacity.
5. Enable performance monitoring and profiling capabilities using automated testing frameworks.
6. Detect performance degradation during upgrades, patches, or configuration changes.
7. Identify slow or inefficient transaction steps and provide recommendations for optimization.
8. Provide access to system logs, monitoring dashboards, and diagnostic tools to support troubleshooting and debugging of performance-related issues.
9. Ensure logs capture sufficient detail to trace issues across services, integrations, and workflows.
10. Support the use of industry-standard performance and load testing tools (e.g., Apache JMeter, LoadRunner, Gatling, BlazeMeter) for VA Cloud Computing applications.
11. Integrate these tools with monitoring and alerting systems to provide real-time visibility of performance metrics.
12. Provide capability to view transaction trending reports highlighting the top transactions, their performance behavior, and any anomalies.
13. Document identified performance bottlenecks, risks, and recommended remediation and optimization actions to ensure sustained system performance.

5.4 TRAINING

The Contractor shall provide comprehensive, enterprise-wide training programs to ensure all VA end users, administrators, and managers are fully equipped to operate and sustain the SaaS ERP platform. The Contractor shall ensure that training is accessible to all 600,000 users, potentially through a combination of live sessions, recorded modules, webinars, and supporting manuals. The Contractor shall provide trainings to include: 1. Core Platform Navigation; 2. Security Awareness; and 3. Compliance Responsibilities (aligned with FedRAMP, FISMA, NIST, and VA-specific mandates).

The Contractor shall deliver Enterprise-Wide Training to include role-based training programs for end users, administrators, and technical users (which include developers, testers, automated testers, product owners, program managers, and executives).

The Contractor shall:

1. Provide all end users with remote Basic Training on how to operate the ERP Platform before the platform goes live. The Basic Training shall include the following:
    a. Navigate the platform
    b. Submit and track requests
    c. Understand security and compliance expectations

2. Provide administrators and technical users with remote Advanced Training on operation and sustainment of the ERP Platform before they begin configuration or development tasks.
3. Deliver module-specific Credentialed and Certification-based Remote Training to administrator and technical users for activated SaaS modules.
4. Provide updated certification paths when the platform releases new versions or new modules. The Credentialed and Certification-based Training shall include:
    a. Access to credential-bearing courses for each platform module used by VA.
    b. Preparation materials (study guides, practice tests, instructional videos).
    c. Access to official certification exams.
    d. Awarding certificates to trainees who pass the exam.
5. Provide Bi-annually Refresher Training for the end user, administrators, and technical users with any updates, new features, new modules, upgrades, and governance updates to the ERP Platform.
6. Provide all users with access to self-paced, On Demand, online learning available at any time. The Contractor shall provide Quarterly On Demand Online Training Report to include the following:
    a. Number of staff trained
    b. Test scores and completion status
    c. Certification progress
    d. Readiness for production go-live
    e. Any gaps or risks in workforce capability
7. Develop and deliver training materials and user documentation tailored to the new ERP tool.

Deliverable:

A. Quarterly On Demand Online Training Report

5.5 OPTION PERIOD ONE - FOUR

The Contractor shall continue to perform tasks and provide deliverables as indicated in sections 5.1, 5.2, 5.3 and 5.4

5.6 PLATFORM TRANSITION IN – TOOL REQUIREMENTS (OPTIONAL TASK 1)

The Contractor shall provide transition-in support to ensure a smooth and effective transfer of responsibilities, knowledge, and processes from the outgoing solution (ServiceNow). The Contractor shall begin transitioning in support immediately after contract award and complete all transition-in tasks to ensure VA retains full operational capability and continuity of service. The Contractor shall submit a comprehensive Transition-In Plan detailing the steps, timeline, resources, and milestones for the successful completion of the transition to the new ERP tool ensuring the new ERP tool has the same functionality as VA has with the incumbent's ERP tool. The Contractor shall ensure the transition to the new platform is performed in no more than 12 Months from time of award. The Contractor shall conduct Phase-In Transition meetings with the

outgoing contractor, the VA COR, and/or VA organizations identified by the COR to discuss and coordinate all necessary activities.

The Contractor shall provide dedicated support during the transition-in period, including:

1. Onsite and remote support for critical transition-in activities.
2. A dedicated transition team to resolve issues and address concerns promptly.
3. Weekly status updates to VA project management detailing progress, risks, and mitigation strategies.

The Contractor shall develop and maintain a Contingency Plan to address any failures or delays in the transition-in process. This plan shall outline alternative measures and resource reallocations to ensure the transition remains on track and shall be provided as part of Transition-In Plan

Deliverable:

A. Transition-In Plan

5.6.1 IMPLEMENT CURRENT FUNCTIONALITY

The Contractor shall perform the following activities to ensure the seamless transition within the agreed upon timeline:

A. Conduct a thorough review of the VA's current environment and functionality.
B. Coordinate and execute the cut-over to the new ERP tool within the agreed upon transition period.
C. Ensure all current capabilities on the VA ServiceNow platform are configured, built and delivered on the new ERP tool within agreed upon timeline from the contract award. The Contractor shall configure and implement the following current capabilities:
    a. All implemented modules functionality including the Employee Center/Service portal, Mobile and Chat.
    b. All reports and dashboards.
    c. All integrations.
    d. All plugin functionalities.
    e. Automated Test Framework (ATF) test scripts.
    f. All Service Catalog workflows.
    g. All custom applications.
    h. All scoped applications

D. Develop an Application Development and Configuration Plan as part of the Transition Plan**.** This shall be a detailed plan outlining the approach for OOB configuration, custom application development, and deployment.
E. Ensure the complete and accurate transition of all knowledge articles. The Knowledge Articles shall be created or updated or migrated to align with the new ERP tool and existing VA processes.

2423 a. Facilitate knowledge transfer sessions to ensure continuity of expertise
2424 and seamless operations post-transition
2425 F. Ensure proper creation of test suite which includes test cases and Test steps
2426 aligning to the new ERP tool implemented functionality.
2427 G. Ensure user provisioning using Entra-ID is implemented.
2428 H. Ensure SSO setup is implemented on the new tool using Entra-ID.
2429 I. Transition or setup of Processing Servers Infrastructure & Discovery Agents (Mid-
2430 server or alternate solutions).
2431 J. Set up synthetic monitoring.
2432 K. Create a detailed Overarching Transition-In Implementation Plan encompassing:
2433 a. Detail implementation schedule
2434 b. Integration documentation by each product, detailing the integration data.
2435 c. Infrastructure diagrams, including architectural diagrams.
2436 d. Configuration management document identifying baseline configurations.
2437 e. Data dictionary
2438 f. Detailed documentation of backup and disaster recovery procedures.
2439 g. Plan on how data elements will be archived, complying with federal and
2440 VA retention policies and supporting the needs of OIT for historical
2441 reporting needs.
2442 h. Reporting and Analytics Implementation Plan outlining configuration,
2443 customization, integration, and deployment timelines for reporting and
2444 analytics functions; that include stakeholder roles, milestones, and
2445 acceptance criteria
2446 i. Report and Dashboard Inventory Directory that detail a complete catalog
2447 of pre-built OOB reports, standard dashboards, KPIs, and metrics
2448 available at go-live. The inventory directory shall include data sources,
2449 owners, refresh schedules, and other pertinent support information
2450 L. Transition/set up existing CI/CD pipeline functionality.
2451 a. Provide a comprehensive guide on CI/CD pipeline setup, including testing
2452 and scanning tool integration.
2453 M. Create real-time monitoring dashboards and alerts to track platform performance
2454 for the new ERP tool.
2455 N. Set up code health reports on code quality, security vulnerabilities, and compliance
2456 status.
2457 O. Provide detailed health scan reports, including diagnostics and recommended
2458 remediation actions.
2459 P. Implement best practice tool (such as Best Practice Engine/Linter) capability within
2460 the ERP tool and set up rules to perform code reviews against development best
2461 practices.
2462 Q. Transition and map user roles and access controls to match existing user roles
2463 and application access.
2464 R. Implement data retention rules based on VA Data Retention/Archive rules.
2465
2466 **Deliverables:**
2467 A. Overarching Transition-In Implementation Plan
2468

5.6.2 MIGRATION FROM SERVICENOW

The Contractor shall migrate the current capabilities of the ServiceNow platform, user profiles and data to the proposed solution. The Contractor shall provide the perform the following in support of the migration effort:

1. Perform all necessary data migration, system configuration, and integration tasks to ensure a seamless cut-over to the new ERP tool without disrupting service operations.
2. All data from the old tool to be migrated to new tool in usable format for end users.
3. Implement measures to ensure no data loss during migration. Users should be able to build reports off this data.
4. Migrate the archived data.
5. Migrate all historical agile records like projects, stories, epics, demands, and themes accurately.
6. Migrate encrypted data including PII and PHI data and encrypt it in the new ERP tool.
7. Prior to initiating data migration activities, the Contractor shall coordinate with VA to implement a change restriction period on the incumbent platform not to exceed 14 calendar days. During this period, development activity and non-critical configuration changes on the incumbent platform shall be suspended to ensure data consistency and reduce migration risk. The Contractor shall define approved change categories, escalation procedures, and emergency exception criteria in the Migration Plan.
8. Prior to beginning migration, the Contractor shall prepare and present a proposed solution Migration Plan that describes the Contractor's plan to migrate current ServiceNow users to the proposed solution. The Migration Plan shall include:
    a. Step by step description of the migration process, documentation, training of VA staff, communication of the VA enterprise,
    b. Schedule for migrating current users and data from ServiceNow to the proposed solution including their existing profiles,
    c. VA responsibilities in the migration process,
    d. Any impacts to VA.

Deliverable:

A. Migration Plan

5.6.3 FedRAMP AUTHORIZED AND VA AUTHORIZED

The Contractor shall disclose the status of the FedRAMP SaaS package associated with the ERP solution and shall adhere to the following:

1. The information system solution selected by the Contractor shall comply with the Federal Information Security Management Act (FISMA) and have a current VA authorization.

2. The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement.
3. The FedRAMP Authorization level and existing VA ATO should be no less than the level required for this use case which has been defined as Moderate
4. The Contractor shall, where applicable, assist with the VA ATO Sustainment Process to help maintain health and quality of agency authorization of the cloud service or migrated application.
5. The Contractor shall exclusively provide licenses and/or accounts to FedRAMP authorized and VA authorized environments.
6. The Contractor shall afford VA access to the Contractor's and Cloud Service Provider's (CSP) facilities, installations, technical capabilities, operations, documentation, records, and databases.
7. If new or unanticipated vulnerabilities are discovered by either VA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party in accordance with Addendum B, VA Information and Information System Security/Privacy LAN usage. VA Privacy and Security deliverables as directed by the VA System owner.
8. The Contractor shall comply with data management requirements.
9. The Contractor shall complete and provide an updated 3PAO Security Assessment Report (SAR).
10. Successful issuance of a VA ATO will be required before live VA data can be used in the system.
11. The Contractor shall participate in FedRAMP Continuous Monitoring activities as outlined by FedRAMP's Continuous Monitoring Strategy Guide found on the FedRAMP Website.
12. The Contractor shall provide continuous monitoring activities including, but not limited to, scans, security artifacts, and monthly Plan of Action and Milestones (POAM) reports as outlined by FedRAMP requirements.
13. The Contractor shall participate in monthly Agency and FedRAMP Sustainment meetings following the granting of a VA ATO.
14. The Contractor shall provide a monthly inventory report of VA sites currently utilizing the cloud product post ATO award. The inventory report will include the number of licenses being utilized and the specific VA site.

Deliverables:

A. 3PAO Security Assessment Report (SAR)
B. Continuous Monitoring Monthly Scans
C. Plan of Action and Milestones Monthly Reports.
D. Monthly Inventory Report

5.7 ENTERPRISE ASSET MANAGEMENT (OPTIONAL TASK 2)

The Contractor shall provide EAM capabilities within the SaaS platform, integrated with ITAM, to ensure a unified approach for managing enterprise and IT assets. The period

of performance should match the award period of the base, based on execution date. Pricing shall be structured in a modular manner (e.g., per instance, per user, or per asset tier).

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The Contractor shall perform the following tasks when this option is exercised:

1. Provide tools to track, manage, and optimize the full lifecycle of enterprise assets (e.g., facilities, fleet vehicles, medical equipment, and specialized devices) from acquisition through disposal.
2. Deliver centralized visibility of all enterprise assets, ensuring accurate inventory records with the ability to tag, categorize, and associate assets with business units, locations, or services.
3. Deploy Maintenance Management to handle routine and preventive maintenance of assets.
4. Schedule and track maintenance activities to ensure assets remain in optimal condition.
5. Integrate with Asset Lifecycle Management for seamless tracking and updates.
6. Include features for managing work orders, maintenance logs, and technician assignment
7. Enable preventive and corrective maintenance scheduling, work order tracking, and asset health monitoring to extend useful life and reduce downtime of enterprise assets.
8. Provide capabilities to track enterprise asset contracts, leases, service agreements, and warranties alongside IT contracts to ensure compliance and cost efficiency.
9. Deploy Financial Management to track the cost, depreciation, and financial impact of assets.
10. Enable budget allocation and expense tracking for asset-related activities.
11. Provide reports on asset depreciation, total cost of ownership, and return on investment.
12. Provide tools to manage depreciation, total cost of ownership, and financial planning for enterprise assets to support budgeting and capital planning.
13. Ensure that enterprise assets comply with regulatory, safety, and environmental standards and provide mechanisms to track inspections, audits, and certifications.
14. Ensure seamless integration between ITAM and EAM modules to enable holistic reporting, analytics, and governance across IT and non-IT assets.
15. Deliver performance dashboards and analytic tools to track asset utilization, costs, risks, and lifecycle status, supporting informed decision-making at the enterprise level

5.8 ENTERPRISE HRSD (OPTIONAL TASK 3)

The Contractor shall provide an Enterprise HRSD module within the SaaS platform. Pricing for this optional task should be provided separately on a per-module or per-user basis, scalable by workforce size, and aligned with subscription or enterprise license models.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The Contractor shall perform the following tasks to support HRSD capabilities:

1. Provide a centralized, user-friendly portal where employees can access HR services, policies, and resources.
2. Ensure the portal supports mobile access and self-service functionality.
3. Deliver tools to create, track, and manage HR cases from initiation to resolution.
4. Provide knowledge management functionality to promote employee self-help and reduce repetitive case submissions.
5. Provide workflows to support employee onboarding, transfers, and offboarding.
6. Enable lifecycle event tracking (e.g., promotions, relocations, separations) to improve continuity and employee experience.
7. Provide tools to design and manage employee journey touchpoints.
8. Include configurable templates for lifecycle events such as new hire onboarding, training, and career development.
9. Enable employees to submit and track requests across HR and related departments.
10. Automate fulfillment of requests and integrate with other ERP workflows.
11. Deliver AI-driven tools such as virtual agents and chatbots to respond to employee inquiries.
12. Provide predictive and automated resolution for common HR requests.
13. Automate repetitive HR tasks such as approvals, documentation updates, and compliance reporting.
14. Enable cross-departmental workflows for HR events impacting IT, facilities, or finance.
15. Provide dashboards and reports to monitor HR service delivery, employee satisfaction, and process performance.
16. Deliver insights to support continual service improvement.
17. Provide secure storage, retrieval, and lifecycle management of employee-related documents.
18. Support compliance requirements such as health and safety reporting, employee relations, and vaccination tracking.

5.9 ARTIFICIAL INTELLIGENCE (OPTIONAL TASK 4)

The Contractor shall provide an ERP solution equipped with AI capabilities as outlined in the following requirements. These capabilities are designed to automate and optimize

service desk operations, increase the accuracy of issue handling, and improve overall service delivery. The Contractor shall provide metrics to measure the solution's performance, including Accuracy and relevance of AI-generated content.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The NTE quantity must meet the needs of up to 600,000 users across the VA Enterprise.

5.9.1 GENERATIVE AI CAPABILITIES

The Generative AI:

1. Summarize long or complex support tickets into concise, readable descriptions to facilitate faster triage and reporting.
2. Provide Dynamic Knowledge Article Creation and convert resolved tickets or chat sessions into formatted knowledge base (KB) articles.
3. Provide Natural Language Ticket Generation and shall enable users to describe issues in plain language and generate properly categorized and formatted tickets.
4. Generate guided conversational troubleshooting paths based on previous cases and documentation.
5. Enhance virtual agents with human-like natural-sounding, contextually relevant responses.
6. Provide Context-Aware Agent Assist and suggest responses, fixes, or documentation to live support agents during ticket handling.
7. Draft emails and internal or external communications related to incidents, changes, or outages.
8. Generate post-incident reports or root cause analyses and reports using structured data and ticket history.
9. Generate first drafts of standard operating procedures (SOP), on-demand access request policies, or support documentation.
10. Produce human-readable narratives and insight from dashboards and metrics.
11. Provide integrated self-service portal search capabilities.

5.9.2 AGENTIC AI CAPABILITIES

The Agentic AI shall:

1. Provide Autonomous Incident Triage & Resolution, automatically receive, categorize, and prioritize incidents and autonomously resolve routine issues.

2. Provide Proactive Problem Management, detect patterns in incidents to identify underlying problems before users report them.
3. Act as the first point of contact for users via chat or voice, providing AI-Powered Virtual Agents for Tier-1 Support**.**
4. Provide Knowledge Base Auto-Creation & Maintenance, build and update documentation based on resolved tickets.
5. Perform Intelligent Routing & Assignment and assign tickets to the most appropriate agent or team based on context.
6. Provide Self-Healing IT Infrastructure and shall monitor infrastructure and take corrective actions without human intervention.
7. Perform Change Management Automation and shall support and drive change requests through the approval and implementation process.
8. Perform Service Desk Analytics & Optimization, continuously analyze service desk performance and suggest improvements.
9. Provide Integrated Workflow Orchestration Across Tools and coordinate actions across multiple systems.
10. Provide User Sentiment Analysis & Experience Management, the Contractor shall understand and act on user satisfaction feedback.

5.9.3 COMBINED GENERATIVE AI AND AGENTIC AI USE CASES

The ERP solution shall harness the synergy between generative AI and agentic AI to deliver enhanced functionalities including but not limited to the following:

1. Provide Virtual Agent Self-Service, generate fluent responses and execute actions (e.g., password reset).
2. Provide Knowledge Base Maintenance, draft or update articles while flagging the ones needing updates.
3. Provide Ticket Triage & Routing, rewrite/clarify ticket intent and classify and assign tickets.
4. Provide Change Request Automation, draft change justifications and submit requests, track approvals.

5.10 DATA LAKE SOLUTION (OPTIONAL TASK 5)

The Contractor shall provide the services required to implement and manage a comprehensive Data Lake solution, ensuring robust data ingestion, storage, cataloging, security, governance, processing, analytics, scalability, integration, backup, monitoring, user interface, and support.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The Contractor shall provide the following services:

1. Data Ingestion and Processing:
    a. Support multiple data ingestion methods including batch, real-time streaming, and micro-batch processing.
    b. Ensure the system is capable of ingesting data from various sources such as databases, APIs, file systems, and IoT devices.
    c. Provide real-time data ingestion and processing capabilities.
    d. Support intake and ingestion of new data tables and fields demands to scale to new data requirements.
2. Data Bus System Management:
    a. Manage and maintain a data bus system that provides real-time bulk data streaming for multiple data producers and consumers.
    b. Administer, monitor, ensure the availability, reliability, performance, and secure operations of the system, and provide metrics related to its operations.
    c. Provide support and assist customers that request to use or integrate with the data bus. This includes instantiation of user accounts/credentials, management of access controls, and ensuring secure encrypted communications between the user or user system and the bus.
3. Storage Capabilities:
    a. Support scalable storage capabilities to handle large volumes of structured, semi-structured, and unstructured data.
    b. Support multiple storage formats such as CSV, JSON, Avro, Parquet, ORC, and raw binary.
4. Data Catalog:
    a. Implement, manage, and maintain a robust data catalog to manage metadata and provide data discovery capabilities.
    b. Ensure the system supports automated metadata extraction and tagging.
5. Security Measures:
    a. Implement IAW VA 6500 as Summit Data Platform which must also be FedRAMP High, including encryption at rest and in transit.
    b. Provide RBAC and fine-grained access control, integrated with identity management systems.
    c. Respond to and mitigate any Data Lake Solution-related security findings or incidents, including those associated with ingestion mechanisms, storage, cataloging, or management systems.
6. Regulatory Compliance and Monitoring:
    a. Include features for data lineage, data quality monitoring, and compliance with regulatory requirements.
    b. Support audit logging and data policy enforcement.
    c. Support data management and data retention of the data based on data retention policy and rules.
7. Data Processing Frameworks:
    a. Support various data processing frameworks and engines such as Apache Spark, Flink, and Hadoop.

b. Facilitate data querying and analysis using SQL-like languages and ML libraries.

8. Scalability and Performance:
    a. Ensure the system is scalable to accommodate growing data volumes and user queries.
    b. Provide high-performance data retrieval and processing capabilities.
9. System Integration:
    a. Integrate the Data Lake with existing data systems, ETL tools, BI tools, and data warehouses.
    b. Ensure interoperability with cloud services and on-premises infrastructure.
10. Backup and Recovery:
    a. Include mechanisms for data backup and disaster recovery to prevent data loss.
    b. Support versioning and rollback features to manage data changes over time.
11. Monitoring and Management:
    a. Provide monitoring tools for tracking system health, usage, and performance metrics, and configure alerts.
    b. Implement management features for efficient resource allocation and cost management.
12. User Interface and Support:
    a. Provide a user-friendly interface for data ingestion, exploration, and management, onboarding of users
    b. Support self-service capabilities for end-users to explore and analyze data.
    c. Include comprehensive documentation for users and administrators and provide support channels for troubleshooting and resolving issues.
13. Onboarding:
    a. Provide automated onboarding process to submit, track and fulfill onboarding requests.
    b. Support set-up of onboarding groups, views and provisioning of data access.

5.11 GREENFIELD SOLUTION - OUT OF THE BOX (OPTIONAL TASK 6)

The Contractor shall build out a new, Greenfield, Out-Of-The-Box (OOTB) instance of ERP, ensuring only absolute business needs are added. The Contractor shall provide customization, and configuration changes to the Greenfield Solution to meet business needs. Any necessary customization requiring code changes must be approved by the OIT Technical Domain leadership team before implementation.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated

based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The Contractor shall:

1. Install and configure the OOTB ERP instance.
2. Install ensure the platform meets baseline security and compliance requirements.
3. Deliver a detail Greenfield Solution Project Plan outlining project phases, timelines, and milestones.
4. Deliver comprehensive Greenfield Solution Requirement Documentation detailing Greenfield Solution business requirements and stakeholder needs.
5. Collaborate with VA stakeholders to identify and document absolute business needs, conduct workshops to gather and validate requirements and provide Greenfield Solution Business Use Cases that reflect VA stakeholders' business requirement.
6. Prioritize configurations over custom code development.
7. Implement necessary workflows, forms, and dashboards within the OOTB framework.
8. Ensure usability and accessibility compliance with Section 508 standards.
9. Implement necessary integrations with existing VA systems using OOTB connectors and configuration where possible. The Contractor shall provide a Greenfield Solution System Integration Plan outlining all systems that are being integrated with ERP and integration schedule.
10. Ensure data integrity and synchronization across platforms.
11. Develop and execute comprehensive Greenfield Solution Test Plan to ensure the platform meets all business requirements. The Greenfield Solution Test Plan shall include testing scope, test schedule, testing criteria, testing environment requirements, and role & responsibilities of testing team members and their duties.
12. Conduct User Acceptance Testing (UAT) with VA stakeholders.
13. Address any issues or bugs identified during testing.
14. Develop Greenfield Solution Training Materials and conduct training sessions for end-users and administrators. The Greenfield Solution Training Materials shall include schedule with course curriculum, Guide with step by step lesson plan, Power Point presentation slide decks, scripts for system walk through, user manual,
15. Propose any customizations requiring code changes to the OIT Technical Domain leadership team.
16. Document detailed justifications for code-based customizations.
17. Obtain OIT Technical Domain leadership team approval before proceeding with any code changes.
18. Provide detailed documentation on configurations made, including any code
19. Provide post-deployment support to ensure smooth transition and operation.

Deliverables:

A. Greenfield Solution Project Plan

B. Greenfield Solution Business Use Cases
C. Greenfield Solution System Integration Plan
D. Greenfield Solution Test Plan
E. Greenfield Solution Training Materials

5.12 VENDOR RISK MANAGEMENT (VRM) (OPTIONAL TASK 7)

The Contractor shall provide a VRM module to assist VA to manage and mitigate risks associated with their third-party vendor relationships. The Contractor shall ensure a robust and efficient approach to vendor risk management, thereby enhancing overall risk mitigation and operational effectiveness.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The NTE quantity must meet the needs of up to 600,000 users across the VA Enterprise.

The VRM Module shall provide the following key capabilities and features:

1. The VRM module must provide centralized vendor management, offering a single platform to manage vendor information, contracts, and risk assessments, thereby eliminating the need for disparate tools such as spreadsheets. The module shall include automated risk assessment functionality, streamlining the process of generating, sending, and managing risk assessments to vendors to ensure consistency and efficiency.
2. The VRM module shall support customizable risk assessment templates tailored to specific vendor types and risks, guaranteeing comprehensive evaluations. The module shall also allow for real-time monitoring of vendor activities and provide real-time reporting dashboards, facilitating the quick identification and response to emerging risks.
3. Issue management and remediation processes shall be streamlined through the VRM module, enabling the identification, tracking, and resolution of issues related to vendor performance or compliance. The VRM shall include the capability for automated issue generation and remediation plans. The module shall feature a dedicated third-party portal to facilitate seamless communication and collaboration with vendors throughout the risk management process.
4. Vendor tiering management is another critical requirement, allowing vendors to be categorized based on their associated risk levels so that the organization can prioritize assessments and allocate resources effectively. The VRM module must integrate with content providers to enhance risk assessments using external intelligence and ratings.

5. The VRM module shall integrate with other Governance, Risk, and Compliance (GRC) applications to provide a holistic view of risks across the enterprise. The Contractor shall integrate third-party risk scores and the IRM portfolio, ensuring comprehensive risk management across all aspects of the enterprise.

5.13 FIELD SERVICE MANAGEMENT (OPTIONAL TASK 8)

The Contractor shall provide Field Service Management Module with the ability to access and perform tasks related to fulfilling field service requests. The module shall provide VA users with the capability to actively work on records and complete assigned field service tasks.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The NTE quantity must meet the needs of up to 600,000 users across the VA Enterprise.

The Field Service Management Modules shall have the following key capabilities and features:

1. Work Order Management:
    a. Access and manage work orders and tasks assigned to them.
    b. View details of the assigned work order, including required parts, customer history, and step-by-step guidance.
2. Mobile Agent Functionality:
    a. Utilize a mobile application to view and update information related to their job tasks, even when offline.
    b. Manage tasks, location, and inventory on the go.
3. Real-time Data Access and Update:
    a. Access real-time information about job status, resource allocation, and inventory availability.
    b. Update work order progress, track their location, and record information related to their job tasks.
4. Inventory Management:
    a. Access information about inventory, including parts needed for the job, to find them quickly.
    b. Track part availability and easily transfer parts from one location to another.
5. AI-Driven Assistance and Guidance:
    a. Benefit from AI-driven insights and guidance to resolve issues more quickly.
    b. Access a knowledge base for resolutions, safety protocols, and FAQs.
6. Utilize route optimization tools to minimize travel time between job sites.

7. Streamline administrative work such as organizing documentation, tracking inventory, managing timesheets, and collecting customer approvals on mobile.

5.14 CLOUD COST MANAGEMENT & FINANCIAL OPERATIONS (FINOPS) (OPTIONAL TASK 9)

The Contractor shall provide a full-cycle accounting system including customizable chart of accounts, department/group tracking, inventory management, financial reporting, Accounts Payable/AR, GL, budgeting, reconciliation, and asset management.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The NTE quantity must meet the needs of up to 600,000 users across the VA Enterprise.

The Contractor shall provide an integrated Customer Relationship Management (CRM) module supporting full customer lifecycle management, including customer data management, customer interactions, ticket tracking, quoting, and comprehensive customer contract management capabilities to include:

1. Authoring, clause libraries, version control, internal review and approval workflows prior to external submission or signature, baselining and modifications, renewals, integration with legal workflows, forecasting, and document upload/repository functionality.
2. Tracking and reporting of services provided under each customer contract, including estimated monthly consumption and cost based on approved fiscal year rates, actual monthly charges, projections, and variance analysis.
3. Customizable dashboards for customer lifecycle metrics, pipeline status, ticket volumes, service performance, and contract statuses.
4. Drill-down capabilities from summary dashboards to underlying transaction or contract details.
5. Support for historical data trending, forecasting, and variance analysis

The Contractor shall provide the following capability:

1. Employee time tracking supporting project allocations, billable time, approvals, and auditability.
2. Cloud credit usage tracking with usage reporting, integration with CSP billing/consumption data, and forecasting dashboards.
3. Cloud Cost Visibility & Reporting
    a. Ability to ingest and normalize cost/usage data from AWS, Azure, and other CSPs.

3014 b. Support for multi-cloud dashboards, cost allocation, tagging compliance,
3015 forecasting, and variance analysis.
3016 4. Optimization Identification & Recommendations
3017 a. Automated identification of waste, underutilization, rightsizing
3018 opportunities, reserved instance and savings plan recommendations, and
3019 architecture-level optimization.
3020 b. Ability to surface optimization insights similar to tools currently used by VA
3021 (Apptio, Cloudability, KubeCost)
3022 5. Describe alignment with FinOps principles and governance practices (e.g., VA's
3023 Cloud Cost Optimization guidance and VAEC Sentry program)
3024 6. Ability to serve as a system of record for consumption-based billing and
3025 chargeback/showback.
3026
3027 The Contractor shall provide a solution that provides native or integrated Cloud Cost
3028 Management (CCM) capabilities that meet or exceed the following requirements:
3029
3030 1. <u>MultiCloud Cost Ingestion & Normalization</u>
3031 The Contractor's solution Shall:
3032 • Ingest, normalize, and reconcile detailed billing and usage data from
3033 AWS, Azure, GCP, OCI, and on Prem virtualization platforms.
3034 • Support daily (or more frequent) ingestion of provider's native cost and
3035 usage files.
3036 • Maintain auditability and versioning of ingested billing records.
3037 • Support integration with the VA's financial systems, general ledger
3038 structures, and cost centers for accurate allocation and reporting.
3039 2. <u>Cost Allocation, Tagging, and Metadata Compliance</u>
3040 Capabilities must include:
3041 • Automated tagging compliance checks, including detection and
3042 categorization of missing, malformed, or stale tags.
3043 • Automated allocation of untagged or shared costs using rules - based
3044 methods (percentage, usage based, fixed allocation).
3045 • Mapping of cloud costs to VA business lines (Executive, Portfolio, Product
3046 Line, System/Application), services, customer contracts, portfolios, and
3047 workloads.
3048 • Ability to integrate with Configuration Management Database (CMDB) to
3049 tie resources to applications, owners, and business services.
3050
3051 3. <u>Cost Visibility & Reporting</u>
3052 The solution must:
3053 • Provide executive, financial, operational, and engineering dashboards with
3054 drilldown capabilities to resource level details.
3055 • Provide customizable, exportable reports for budgets, forecasts, variance
3056 analyses, and consumption-based billing.
3057 • Support showback and chargeback models consistent with VA Franchise
3058 Fund and OIT financial practices.

- Enable trend analysis on historical data, including multiyear benchmarking.

4. Forecasting, Budgeting & Anomaly Detection

   Capabilities must include:
   - Forecasting using historical consumption, adjustable models, and seasonal patterns.
   - Budget creation, monitoring, alerts, and variance reporting.
   - Automated anomaly detection with configurable alert thresholds and routing workflows.
5. Optimization & Recommendations

   The solution must:
   - Identify unused, underutilized, or misconfigured cloud resources (compute, storage, databases, container workloads, etc.).
   - Provide actionable insights for:
     - Rightsizing
     - Idle resource elimination
     - Savings Plan / Reserved Instance / committed use recommendations
     - License optimization (including (Bring your own License (BYOL))
     - Architecture level improvements
   - Use CSP native analytics where possible (e.g., AWS Compute Optimizer).
   - Provide visibility into realized vs. unrealized optimization (rate + workload), aligned to VA FinOps practices (as reinforced through ongoing Apptio/Cloudability optimization work in VAEC programs
   - Provide rate optimization plus workload optimization capabilities to achieve a full picture of cloud and on prem cost management.
6. inOps Maturity, Governance & Integration

   The Contractor's Solution Shall:
   - Demonstrate alignment with FinOps principles (Inform, Optimize, Operate).
   - Support role-based views for FinOps practitioners, finance, engineering, and executives.
   - Integrate with platforms such as:
     - ServiceNow (workflows, financial automation, CMDB)
     - Apptio (cost models, chargeback)
     - Microsoft 365 applications
7. System of Record for Consumption-Based Billing

   The solution must:
   - Serve as the authoritative system of record for consumption-based service billing within OIT.
   - Support customer contract alignment, tracking, and billing for cloud service costs.
   - Provide auditable lineage from resource usage → cost → allocation → billed/charged amount.
8. Security, Access Control & Compliance

   The solution must:

- Comply with FedRAMP High
- Support role-based access controls, MFA, and integration with federal Identity Credential, and Access Management (ICAM) standards.
- Provide Role-Based Access Control (RBAC), to include but not limited to:
  - Global, Organizational, Resource-Specific, and Custom roles
- Provide full audit trails for billing data, optimization actions, allocations, and changes

9. Additional Functional Requirements

   The Contractor shall provide additional functional requirements including;
   - Workflow automation and configurable approvals
   - Financial and operational reporting
   - Audit/controls aligned with federal requirements (FAR 4, FAR 31)
   - Identity and access management (SSO, SAML, OAuth)
   - Data import/export and ETL capabilities
   - Role-based access controls
   - Ability to generate scheduled and ad hoc reports with configurable filters, data fields, and export format (e.g., CSV, Excel, PDF).
10. Integration Requirements

    The Contractor shall provide the following integration requirements for their solution:
    - ServiceNow: ticketing, CMDB, request workflows, financial automation
    - Apptio: cost models, chargeback/showback, financial interface, seamless data exchange, real-time synchronization
    - Cloud Service Providers (AWS, Azure, GCP, OCI) billing files, consumption data, cost reporting
    - Microsoft 360 applications
    - Identity and access compliance with federal ICAM standards
    - Cost Optimization recommendation and implementation cloud native tools

5.15 DISTRIBUTED DEVELOPMENT AND SUSTAINMENT (OPTIONAL TASK 10)

This Optional task establishes an enterprise-controlled capability delivery and sustainment model that enables VA organizations, referred to as Participating Organizations, to fund, scope, prioritize, price, and implement approved enhancements, automations, integrations, workflows, configurations, reports, and mission capabilities on the enterprise ERP.

This optional item may be exercised at the Government's discretion at any time and from time to time during performance up to the NTE quantity. The Contractor shall propose a prorated daily unit price below; the term shall be cotermed with the expiration of the period in which the optional task was exercised The Total Price of this CLIN shall be calculated based on the prorated daily unit price multiplied by 365 days multiplied by the NTE quantity.

The Contractor shall provide Participating Organizations a standardized mechanism to leverage the enterprise platform without creating separate standalone contracts,

duplicative environments, fragmented solutions, unsupported customizations, isolated operational silos, or non-standard implementations. The Contractor shall support enterprise modernization while preserving centralized governance, architecture alignment, security compliance, operational consistency, upgrade compatibility, and long-term sustainment readiness.

Work authorized under this task shall be limited to discrete, funded capability enhancements, integrations, automations, or configurations that are not required as part of the Contractor's baseline sustainment, operations, or maintenance obligations under the base contract. Work that the Contractor is otherwise required to perform under the base contract shall not be reauthorized or repriced under this CLIN.
This task shall not be used as a staff augmentation vehicle, labor-hour ordering mechanism, or body-shop arrangement. The Contractor shall not price or execute work primarily on the basis of directed labor categories, Government-directed staffing levels, or Government-directed team composition. Work shall be scoped, priced, authorized, accepted, and measured based on defined outcomes, approved scope, delivery complexity, operational value, sustainment impact, and achievement of acceptance criteria.
The following table provides examples to clarify the boundary between base contract work and Optional CLIN work. The examples are illustrative and do not limit the Government's authority to determine the appropriate funding and authorization approach for a specific requirement.

Base Contract Work Examples	Optional CLIN Work Examples
Routine sustainment, operations, monitoring, break/fix support, patching, release support, security remediation, service desk coordination, and maintenance necessary to meet the contracted enterprise service levels.	Discrete funded capability enhancements, new integrations, new automations, new workflows, mission-specific dashboards, reports, analytics, or configurations that are not required to meet baseline contract obligations.
Correction of defects, failed changes, integration issues, performance degradation, or security weaknesses caused by Contractor work or required to maintain existing functionality.	Approved enhancements that expand platform capability beyond the existing baseline, add new business processes, automate new functions, or deliver new mission outcomes for a Participating Organization.
Documentation updates, runbook maintenance, operational readiness support, transition support, and lifecycle sustainment required by the base PWS.	Separately authorized capability packages with defined scope, price, schedule, deliverables, acceptance criteria, and sustainment expectations.

5.15.1 ORDERING AND AUTHORIZATION MODEL

Each effort under this CLIN shall be initiated by a Participating Organization through a Government-approved intake, work authorization, task authorization, capability

package, contract modification, or equivalent ordering mechanism. The authorization shall identify the sponsoring organization, funding source, desired business outcome, scope boundaries, expected operational benefit, required timeframe, known dependencies, acceptance criteria, and any constraints established by the Government.

The Government shall authorize discovery and scoping activities through a written intake authorization identifying the sponsoring organization, the estimated scope of the assessment, the funding source, and any constraints on assessment activities. Discovery and scoping activities shall be separately authorized, included in an approved work package, or incorporated into a Government-approved intake process before becoming compensable. Discovery and scoping activities performed without written authorization shall not be compensable under this contract.

The Contractor shall not begin implementation work until the Government provides written authorization. Initial discovery, assessment, estimation, and scoping activities may occur only to the extent authorized by the Government and shall be limited to the activities necessary to develop a complete scope, price, schedule, risk assessment, and recommendation for Government review.

The Government retains authority to approve, reject, defer, reprioritize, consolidate, suspend, or terminate any proposed or active effort based on mission priorities, funding availability, enterprise risk, platform constraints, governance determinations, or operational impact.

5.15.2 OUTCOME-BASED SCOPING AND SOLUTION ASSESSMENT

For each proposed effort, the Contractor shall perform an outcome-based scoping and solution assessment sufficient to allow the Government to determine whether the work should proceed, how it should be structured, what it should cost, what outcomes it will produce, and how the resulting capability will be sustained.

The assessment shall define the business problem or opportunity, the mission outcome to be supported, the users or organizations affected, the expected operational improvement, the functional capabilities required, and the measurable acceptance criteria. The Contractor shall evaluate whether the requested capability can be satisfied through reuse of existing platform functionality, existing workflows, existing integrations, existing reports, configuration changes, automation, or other standardized enterprise capabilities before recommending new development or customization.

The Contractor shall assess technical feasibility, integration complexity, data impacts, security implications, architecture alignment, sustainment requirements, upgrade compatibility, testing needs, deployment considerations, operational risks, and dependencies. The Contractor shall identify assumptions, constraints, exclusions, and Government responsibilities necessary to support successful delivery.

The Contractor shall document the assessment in a Solution Assessment Package. The package shall provide the Government with a clear basis for deciding whether to approve, modify, defer, or reject the proposed effort.

Performance Standard	Acceptable Quality Level	Measurement Method
Solution Assessment Package Completeness	All required scope, risk, integration, sustainment, and business outcome elements included.	COR review of deliverable.
Reuse Evaluation	100% of proposed efforts evaluated for reuse of existing enterprise capabilities before recommending customization.	Architecture and reuse assessment review.
Scope Clarity	No material scope ambiguities identified during Government review.	Government review of assessment package.
Technical Feasibility Assessment	All assessments include documented technical feasibility and dependency analysis.	COR technical review.
Assessment Submission Timeliness	Submitted within timeframe established in work authorization.	Deliverable tracking and CDRL review.

Deliverable:

A. Solution Assessment Package

5.15.3 SCOPE DEFINITION AND WORK PACKAGE REQUIREMENTS

Each approved effort shall be documented in a work package or equivalent Government-approved authorization document. The work package shall describe the approved outcome, scope, price, schedule, deliverables, acceptance criteria, dependencies, assumptions, exclusions, and sustainment expectations.

The scope shall be defined in terms of the capability to be delivered and the operational outcome to be achieved. The scope shall not be defined primarily by contractor labor categories or staffing levels. The Contractor shall determine the staffing approach, delivery method, technical approach, internal resource allocation, tools, and execution strategy necessary to achieve the approved outcome.

Each work package shall include a description of what is included in the effort and what is excluded from the effort. Exclusions shall be specific enough to prevent scope ambiguity and shall identify work that would require a separate authorization, modification, or future funded effort.

The Contractor shall provide Capability Work Package's and ensure each work package contains acceptance criteria that are objective, testable, and tied to the approved business outcome. Acceptance criteria may include functional performance, successful integration, security validation, user acceptance, reporting accuracy, automation execution, workflow completion, documentation completion, operational readiness, and sustainment readiness, as applicable.

Performance Standard	Acceptable Quality Level	Measurement Method
Work Package Completeness	All approved work packages include scope, exclusions, acceptance criteria, pricing, schedule, and sustainment expectations.	COR review of work package.
Objective Acceptance Criteria	100% of work packages contain measurable and testable acceptance criteria.	Government review and acceptance validation.
Scope Boundary Definition	Included and excluded scope clearly documented with no unresolved ambiguity.	Work package review and change request analysis.
Outcome-Based Scope Alignment	Scope defined by operational outcome rather than labor categories or staffing levels.	COR review of work package structure.
Sustainment Expectations Documentation	Sustainment responsibilities documented for all delivered capabilities.	Government review of work package documentation.

Deliverable:

A. Approved Capability Work Package

5.15.4 STANDARDIZED PRICING AND CONSUMPTION MODEL

The Contractor shall maintain a Standardized Pricing Methodology for efforts performed under this CLIN. The methodology shall provide repeatable, transparent, and auditable pricing based on the approved scope, complexity, risk, integration requirements, security requirements, sustainment impact, delivery timeline, operational dependencies, and expected business outcome.

Offerors shall submit aPricing and Scope Traceability Matrix with initial proposed pricing methodology with their proposal to allow the Government to evaluate pricing logic, cost drivers, transparency, and reasonableness before award. The Contractor shall submit the final Standardized Pricing Methodology to the Contracting Officer for review and approval within 60 calendar days of contract award. The Contractor shall submit

proposed revisions to the methodology to the Contracting Officer for approval no later than 30 calendar days before the proposed effective date of any revision. The Government reserves the right to reject or require modification of any pricing methodology that is not sufficiently transparent, auditable, or aligned with the outcome-based scope requirements of this section.

Pricing shall not be based solely on labor hours, labor categories, or staffing levels. The Contractor may use internal labor estimates to develop pricing; however, the price presented to the Government shall be tied to the capability, outcome, complexity, and scope of the approved work package.

The Contractor shall establish pricing categories or complexity tiers that allow Participating Organizations to understand the expected cost drivers associated with common types of work. These categories may include configuration changes, workflow automation, integration enhancement, reporting and analytics, self-service enablement, data management, platform optimization, and larger enterprise modernization activities. For each proposed effort, the Contractor shall provide a Capability Pricing Estimate Package that identifies the proposed price, pricing assumptions, complexity determination, scope boundaries, included services, excluded services, dependencies, sustainment assumptions, and conditions that could require price revision. The Contractor shall provide sufficient detail to allow the Government to validate that the proposed price is reasonable, consistent, and aligned with the approved scope.

The Government reserves the right to negotiate, reject, request clarification, request refinement, or require rescoping of any proposed price or work package before authorizing performance.

Performance Standard	**Acceptable Quality Level**	**Measurement Method**
Initial Pricing Methodology Submission	Submitted with proposal and finalized within 60 calendar days of award.	COR review of methodology submission.
Pricing Transparency	Pricing estimates include assumptions, exclusions, dependencies, and complexity rationale.	Pricing package review.
Pricing Consistency	Similar work efforts priced consistently across comparable complexity tiers.	Pricing audit and comparative analysis.
Outcome-Based Pricing Compliance	Pricing tied to approved scope and outcomes rather than labor-hour estimates alone.	Government review of pricing packages.

Performance Standard	Acceptable Quality Level	Measurement Method
Pricing Revision Notice	Proposed pricing methodology revisions submitted at least 30 calendar days before implementation.	CO review of revision submissions.

Deliverables:

A. Standardized Pricing Methodology
B. Capability Pricing Estimate Package
C. Pricing and Scope Traceability Matrix

5.15.5 ENTERPRISE DEMAND MANAGEMENT AND FORECASTING

The Contractor shall maintain demand management capabilities sufficient to support intake, assessment, prioritization, forecasting, sequencing, and coordination of multiple concurrent efforts under this CLIN. Demand management shall provide the Government visibility into the modernization pipeline, approved work, pending requests, capacity constraints, schedule dependencies, funding dependencies, and enterprise risks.

The Contractor shall maintain a modernization pipeline that identifies proposed, assessed, approved, active, deferred, completed, and cancelled efforts. The pipeline shall show expected delivery timing, sponsoring organization, high-level outcome, current status, major dependencies, known risks, and potential impacts to enterprise operations or other modernization efforts.

The Contractor shall provide Enterprise Demand Forecast that is sufficient to help the Government understand how new demand may affect timelines, platform capacity, release planning, sustainment workload, and enterprise priorities. Forecasting shall support Government decisions regarding sequencing, consolidation, funding, prioritization, and use of this CLIN by Participating Organizations.

Performance Standard	Acceptable Quality Level	Measurement Method
Modernization Pipeline Maintenance	Pipeline updated monthly with status, dependencies, risks, and schedule data.	COR review of pipeline dashboard.
Forecasting Accuracy	Forecasts reflect current approved workload, capacity constraints, and modernization demand.	Government review of forecasting artifacts.
Demand Visibility	100% of approved and pending efforts reflected in enterprise demand reporting.	Demand management dashboard review.

Performance Standard	Acceptable Quality Level	Measurement Method
Risk Identification	Major modernization sequencing or capacity risks identified prior to operational impact.	Operational governance review.
Reporting Timeliness	Forecast and prioritization reports submitted monthly on schedule.	Deliverable tracking review.

Deliverables:

A. Enterprise Demand Forecast

5.15.6 ENTERPRISE ARCHITECTURE, REUSE, AND STANDARDIZATION

The Contractor shall ensure all capabilities delivered under this CLIN comply with approved enterprise architecture, data models, integration standards, security requirements, governance processes, operational standards, and sustainment objectives.

The Contractor shall maximize reuse of existing enterprise workflows, configurations, integrations, automations, reports, data structures, and platform capabilities before proposing new development or customization and provide an Enterprise Reuse Assessment. The Contractor shall not create duplicative functionality when an existing enterprise capability can reasonably satisfy the approved business need.

Customizations shall be minimized and shall require documented justification through a Customization Justification Package. The Contractor shall demonstrate that proposed customizations are necessary to meet approved business outcomes, do not create avoidable technical debt, do not impair upgradeability, do not reduce maintainability, do not create unsupported dependencies, and do not conflict with enterprise architecture or platform standards.

The Contractor shall identify opportunities to consolidate duplicative processes, retire redundant workflows, increase reuse, standardize configurations, and reduce fragmentation across the enterprise platform.

Performance Standard	Acceptable Quality Level	Measurement Method
Architecture Compliance	100% of delivered capabilities comply with approved enterprise architecture standards.	Architecture review and validation.
Enterprise Reuse Optimization	Existing enterprise capabilities evaluated before creation of new custom functionality.	Reuse assessment review.

Performance Standard	Acceptable Quality Level	Measurement Method
Unsupported Customization Prevention	No unsupported customizations introduced without written Government approval.	Configuration and modernization assessment review.
Duplicate Functionality Reduction	Net reduction in duplicative workflows or capabilities year-over-year where applicable.	Enterprise architecture assessment.
Customization Justification	All approved customizations supported by documented business justification and sustainment analysis.	COR review of customization packages.

Deliverables:

A. Enterprise Reuse Assessment
B. Customization Justification Package

5.15.7 DELIVERY ACCOUNTABILITY AND OPERATIONAL READINESS

The Contractor shall deliver complete, production-ready capabilities that satisfy the approved work package, meet acceptance criteria, comply with applicable architecture and security requirements, and are ready for sustainment at the time of deployment.

The Contractor shall remain accountable for delivery quality, technical correctness, security compliance, integration performance, documentation completeness, operational readiness, sustainment readiness, upgrade compatibility, user adoption enablement, and achievement of approved outcomes.

No capability shall be deployed into production until it has completed required validation activities. Validation shall include, as applicable, functional testing, integration testing, security validation, user acceptance, operational readiness review, sustainment readiness review, documentation review, deployment planning, and rollback or recovery planning.

The Contractor shall ensure delivered capabilities do not degrade platform performance, existing enterprise services, integration stability, security posture, data integrity, upgrade compatibility, or operational maintainability.

Performance Standard	Acceptable Quality Level	Measurement Method
Production Readiness Validation	100% of deployments complete required validation activities before production release.	Operational readiness review.

Performance Standard	Acceptable Quality Level	Measurement Method
Acceptance Criteria Compliance	Delivered capabilities meet all approved acceptance criteria before Government acceptance.	User acceptance testing and validation review.
Documentation Completeness	All operational, sustainment, and deployment documentation delivered prior to production release.	Documentation review and acceptance.
Operational Impact Prevention	No deployment introduces unauthorized degradation to production services.	Post-deployment monitoring and incident review.
Sustainment Readiness	Sustainment support procedures established before production deployment.	Sustainment readiness assessment review.

5.15.8 SUSTAINMENT AND LIFECYCLE ACCOUNTABILITY

The Contractor shall provide sustainment support for capabilities delivered under this CLIN unless otherwise directed by the Government. The contractor shall provide a Sustainment Plan that shall include defect remediation, break/fix support, upgrade compatibility maintenance, release alignment, documentation maintenance, performance tuning, security remediation, and operational support coordination.

The Contractor shall provide an Upgrade Compatibility Assessment that ensures delivered capabilities remain compatible with enterprise platform upgrades, security requirements, integration changes, governance standards, and operational processes. The Contractor shall identify sustainment risks before deployment and shall ensure those risks are addressed or accepted by the Government prior to production release.

If a delivered capability causes operational disruption, performance degradation, integration failure, security concern, or upgrade incompatibility, the Contractor shall remediate the issue within applicable SLA timelines and shall provide root cause, corrective action, and preventive action information to the Government.

Performance Standard	Acceptable Quality Level	Measurement Method
Defect Remediation Timeliness	Defects remediated within applicable SLA timelines.	Incident and defect management reporting.
Upgrade Compatibility Maintenance	Delivered capabilities remain compatible with supported platform upgrades.	Upgrade testing and validation review.

Performance Standard	Acceptable Quality Level	Measurement Method
Sustainment Support Coverage	Sustainment support maintained for all active delivered capabilities unless otherwise directed.	Sustainment support reporting review.
Root Cause Analysis for Operational Disruption	RCA submitted for disruptions caused by delivered capabilities within 5 business days.	COR review of RCA submissions.
Security and Compliance Alignment	Delivered capabilities maintain compliance with enterprise security and governance requirements.	Security assessment and compliance review.

Deliverables:

A. Sustainment Support Plan
B. Upgrade Compatibility Assessment

5.15.9 PERFORMANCE OUTCOMES AND KEY PERFORMANCE INDICATORS

The Contractor shall achieve measurable modernization, delivery, sustainment, and business-value outcomes for work performed under this CLIN. Performance shall be evaluated at both the individual work package level and the aggregate CLIN level.

At a minimum, the Contractor shall achieve a 95% on-time milestone achievement rate, a 95% first-submission acceptance rate for deliverables requiring Government acceptance, sustained compliance with enterprise SLAs, measurable reduction in post-production defects, increased reuse of enterprise capabilities, reduction in duplicative functionality, improved modernization throughput, reduced rework, increased automation utilization, and Customer Satisfaction of no less than 4.5 out of 5.0.

The Contractor shall track first-submission acceptance rate monthly across all deliverables. A submission shall be counted as accepted on first submission if the Government issues written acceptance without requiring resubmission. Submissions returned for revision shall count as not accepted on first submission regardless of the reason for return.

The Contractor shall notify the COR in writing if the Government fails to provide written acceptance or rejection. Submissions pending Government response beyond the established review period shall be excluded from the first-submission acceptance rate calculation for the affected measurement period, provided the Contractor has submitted all required content and the submission is not under dispute.

A milestone is defined as a scheduled event identified in the Government-approved work package schedule that marks completion of a discrete, verifiable phase of work. On-time milestone achievement shall be calculated as milestones completed on or

before the approved scheduled date divided by total milestones scheduled during the measurement period, multiplied by 100.

The Contractor shall also measure adoption and value realization for delivered capabilities. Value realization may include increased utilization of delivered functionality, reduced manual processing, reduced process completion time, increased self-service usage, reduced duplicate workflows, improved operational throughput, improved reporting accuracy, or other measurable operational benefits approved by the Government.

All SLA measurements shall include the measurement period, data source, numerator, denominator, any exclusions applied, and the calculation method used. Definitions shall be submitted to the Government for approval within 60 calendar days of contract award and shall be applied consistently across all efforts throughout the Period of Performance.

Performance Standard	Acceptable Quality Level	Measurement Method
On-Time Milestone Achievement	Minimum 95% of milestones completed on or before approved scheduled dates.	Milestone tracking and schedule review.
First-Submission Acceptance Rate	Minimum 95% first-submission acceptance rate for CDRL deliverables.	Deliverable acceptance tracking.
Customer Satisfaction	Maintain minimum CSAT score of 4.5 out of 5.0.	Approved survey reporting.
Enterprise Reuse Improvement	Year-over-year increase in reuse of enterprise capabilities.	Reuse metrics analysis.
Reduction in Post-Production Defects	Measurable reduction in production defects year-over-year.	Defect trend analysis.
SLA Reporting Completeness	All SLA reports include numerator, denominator, exclusions, and methodology.	COR review of SLA reporting packages.

5.16 TRANSITION OUT (OPTIONAL TASK 11)

If the Optional Task is exercised by VA, the Contractor shall provide transition Out support for a period of 90 days. The Contractor shall provide Transition Out Support in the event that all or part of the tasks are terminated or completely transitioned to the Government or a new Contractor at the end of the PoP. The Contractor shall develop and deliver a Phase-Out Transition Plan and execute the Phase-Out Transition Plan upon Government approval by the COR. The Contractor shall provide subject matter expertise support to affect the requisite knowledge transfer in accordance with the

resulting Phase-Out Transition Plan. The Phase-Out Transition Plan shall detail both the assumption of responsibilities and the transfer of responsibilities to follow on parties at the conclusion of the PoP.

This Phase-Out Transition Plan shall include the following:

a. Executive Summary: Overview of the transition strategy, including key objectives and KPIs.
b. Scope of Work: Detailed description of the systems, services, and operations being transitioned out, including affected departments and stakeholders.
c. Transition Timeline: Detailed schedule outlining the key milestones and timelines for the phase-out process.
d. Resource Allocation and Staffing Plan: Overview of the resources required for the transition, including personnel assignments, roles, and responsibilities.
e. Identification and assessment of potential risks, along with mitigation strategies to address these risks.
f. Strategy for communicating the phase-out plan to all stakeholders, including frequency and methods of communication.
g. Detailed plan for the secure migration and archiving of data, including verification and validation processes.
h. Training and Knowledge Transfer: Plans for training and transferring knowledge to ensure continuity of operations and support for any new systems or processes.
i. Compliance and Security: Assurance that the phase-out process meets all relevant legal, regulatory, and security requirements.
j. Quality Assurance: Measures to ensure that the transition meets quality standards and does not disrupt business operations.

The Contractor shall work collaboratively with other support Contractors and/or Government personnel. As part of collaboration, the Contractor shall convey any and all information, as it pertains to this effort. This support shall also consist of providing advice, clarification or explanation to facilitate the understanding of the information presented. The Contractor shall provide the following Transition Support.

a. Coordination with Government representatives,
b. Review, evaluation and transition of current support services,
c. Assist in the transition of historic data to new Contractor system (e.g. Project Management System)
d. Government-approved training and certification process,
e. Transfer of all necessary business and/or technical documentation,
f. Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
g. Knowledge transfer demonstration

Deliverable:

A. Phase-Out Transition Plan

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 VA TECHNICAL REFERENCE MODEL

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

6.1.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

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

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

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 Architecture (EA), and VA Identity and Access Management (IAM) approved Enterprise Technology Guidelines (ETG). 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 Executive Order 14028, VA Handbook 6510 VA Identity and Access Management, VA Handbook 0735 Homeland Security Presidential Directive 12 (HSPD-12) Program, CISA Binding Operational Directive 23-01, 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) 800-63-4, VA Handbook 6500, and VA IAM

enterprise requirements for direct, assertion-based authentication, and/or trust based authentication, as determined by the ETGs. 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, M-22-09, and NIST Federal Information Processing Standard (FIPS) 201-3. Contractor delivered applications and systems shall be on the FIPS 201 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 Technology Guideline as outlined in VA ETG.
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 800-63-4 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.

6.1.4 INTERNET PROTOCOL VERSION 6 (IPv6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020

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

6.1.5 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).

6.1.6 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, Windows 11, Edge (Chromium based), and 365 Apps for enterprise. Applications delivered to VA and intended to be deployed to Windows 11 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 Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

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

The Contractor shall support VA efforts IAW the Veteran-Focused Integration Process (VIP) Guide and Product Line Management (PLM) Playbook. The major focus of VIP is on Enterprise Oversight, Governance, reporting, and establishing practices that focus on outcomes and continuously delivering sustainable IT capabilities to benefit the Veteran. 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 Transformation Playbook and can be found at: https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371 and the PLM Transformation Playbook can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946. VIP and PLM are the authoritative processes that IT projects must follow to ensure development and delivery of IT products.

The VIP Guide provides guidance for transitioning from project-centric to product-centric delivery. The VIP guide applies to all OIT Office of Management and Budget (OMB) reportable products that are required to collect and report costs, schedules, risks, and other valuable information in VA PARS (whether products are procured or developed by VA) and any VA Information Technology project effort in Software Product Management (SPM) and Infrastructure Operations (IO), or their successors, that touch the VA network regardless of IT organizational alignment (whether it spends government funding from VA's Congressional IT Appropriation or any other appropriation).

The PLM Transformation Playbook details how OIT leadership expects Product Lines (PLs) to implement PLM, DevOps, and Lean-Agile principles, methods, practices, and techniques through levels of maturity. The PLM Transformation Playbook applies to all Information Technology (IT) products aligned to PLs in the Software Product Management, Infrastructure Operations and Product Engineering organizations within the OIT organization.

Others outside the referenced groups or organizations may use the VIP Guide and PLM Transformation Playbook for situational awareness as needed.

6.1.8 PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL). The PAL includes a spectrum of OIT functions and activities, such as 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. OIT utilizes 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

process_CONB_ext.docx (live.com). The main PAL can be accessed at www.va.gov/process.

6.1.9 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 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 VA Profile to access personal contact information, if the solution relies on VA Veteran personal contact information data. VA Profile 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.
7. Interfacing with VA Systems Inventory (VASI) to access VA systems information, if the solution relies on VA system information. VASI is the authoritative source for VA Information Technology systems.
8. Interfacing with Enterprise Mission Assurance Support Service (eMASS) to access the historical Authority to Operate (ATO) status of all VA Information Systems prior to migrating to ServiceNow Continuous Authorization and Monitoring (SNowCAM) until it is determined the migration is completed and eMASS is sunset. eMASS contains the historical Authority to Operate (ATO) status of all VA Information Systems prior to September 30, 2025, with all status provided through SNowCAM once migration is completed.

6.1.10 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 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.

6.1.11 SOFTWARE AND LICENSING REQUIREMENTS

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

6.1.12 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

If Artificial Intelligence (AI) is part of the Contractor system/solution, the Contractor shall be in compliance with E.O. 13960 and 14319, OMB Memorandums M-25-21, M-25-22, and M-26-04, and VA Directive and Handbook 6500 to support VA in trustworthy, secure, responsible, accountable, Truth Seeking, and Ideologically Neutral AI innovation.

No web-based, publicly available generative AI service has been approved for use with VA-sensitive data including, but not limited to OpenAI's ChatGPT, Microsoft's Copilot, Google's Gemini, and Anthropic's Claude. No PII, protected health information (PHI), or VA-sensitive data should be entered into these unapproved services. The entire definition of VA Sensitive Data can be found at 38 U.S.C. § 5727 (23). The Contractor shall protect VA Sensitive data from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's commercial offerings without express permission from VA. Only VA-hosted instances of generative AI services may be approved for use with VA-sensitive data.

The Contractor shall deliver the services, technical data, configurations, models, weights, documentation or other information, including source code, developed during contract performance. The Contractor, in collaboration with VA, must evaluate the output of any AI tool for accuracy prior to using the output in VA efforts. All data,

including models, weights, algorithms, and outputs generated using either Government-furnished data or data first developed under this contract shall be the property of the Government with unlimited rights as defined by FAR 52.227-14. The Contractor shall also deliver any custom-developed code developed with AI methodologies in accordance with the SHARE IT Act, if applicable. VA shall also retain unlimited rights to any improvements to that data, including the continued design, development, testing, and operation of AI systems and/or systems utilizing AI.

The Contractor shall ensure that all AI Systems, including Large Language Models (LLM), whether standalone LLMs or integrated into broader software platforms, procured under this effort and/or used in performance of this contract complies with the Unbiased AI Principles as defined in Executive Order 14319 and OMB Memorandum M-26-04, e.g. Truth Seeking and Ideologically Neutral, as applicable to the intended use of the system.

The Contractor shall ensure that AI System/LLM generated outputs are truthful in responding to user prompts seeking factual information or analysis, prioritize historical accuracy, scientific inquiry, and objectivity, as well as acknowledge uncertainty where reliable information is incomplete or contradictory and do not fabricate, hallucinate, or present unverifiable information as fact.

The Contractor shall ensure that LLMs and AI outputs are neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas such as Diversity, Equity, and Inclusion (DEI). The Contractor shall ensure that the LLMs, including the AI System, are not intentionally encoded with partisan or ideological judgments within an AI System's/LLM's outputs unless those judgments are prompted by or otherwise readily accessible to the end user.

Compliance with the AI requirements of this contract, including adherence to the Unbiased AI Principles, Truth-Seeking and Ideological Neutrality requirements, disclosure obligations, monitoring and reporting requirements, and corrective action responsibilities, is a material condition of eligibility for payment and continued performance. In accordance with OMB Memorandum M-26-04, failure to comply with these requirements, or refusal to take timely and appropriate corrective action to remedy identified noncompliance, may constitute a material breach of contract and may result in remedies consistent with the terms of the contract and applicable law including but not limited to withholding of payment, termination for cause/default, or other appropriate contractual remedies, as determined by the Contracting Officer.

All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation as identified in the Artificial Intelligence in VA Contracts clause, to include its associated list of AI being used in contract performance.

Deliverable:

A. Statement of Attestation

6.1.12.1 AI SYSTEM/LLM DEVELOPMENT AND OPERATION DOCUMENTATION REQUIREMENTS

To enable Government continued assessment of compliance with Trustworthy AI requirements and both Unbiased AI Principles, Truth-seeking and Ideological Neutrality, in accordance with OMB M-26-04, the Contractor shall provide AI System/LLM Development and Operation Documentation Package to include, at a minimum:

1. **Acceptable Use Policy**
   The Contractor shall provide an Acceptable Use Policy document governing its AI operation that characterizes and differentiates appropriate and inappropriate use of their product offering
2. **Model Cards, System Cards and/or Data Cards**
   The Contractor shall provide documentation describing essential information about the model, system, and or data as it relates to the AI/LLM product offering. The documentation shall address summaries of training process, identified risks and mitigations, and model evaluation scores on LLM benchmarks at a minimum, where appropriate
3. **End User Resources**
   The Contractor shall provide documentation to include product tutorials, developer guides, and/or other tools to assist VA in ensuring proper use of the AI/LLM to maximize utility
4. **Mechanism for End User Feedback**
   The Contractor shall provide documentation describing the mechanism employed to provide feedback to the Offeror on outputs identified that violate the Unbiased AI Principles. This may be satisfied by a general inbox, specific Point of Contact, or similar feedback mechanism.
5. **Pre-Training and Post-Training Activities of the AI System/LLM**
   The Contractor shall provide documentation of Pre-Training and Post Training Activity that provides details on:
   a. Actions taken that impact the factuality and grounding of AI System/LLM outputs
   b. System-level prompts that provide natural language instructions to the model specifying guidelines on responding to user-generated queries, to include how a model responds when reliable information is incomplete, contradictory, or subject to individual interpretation
   c. The type of outputs restricted via content moderation and safety filters
   d. The use of red teaming as a means of continuously assessing the model to protect against incidents of bias in generated output.
   e. Training or development, if any, that occurred outside the United States, to include the type of activity and the country in which it occurred.
   f. Any modifications or configurations undertaken to comply with any regulation from a government other than the U.S. Federal Government.
6. **Model Evaluation Results and Methodologies**

The Contractor shall provide documentation describing the Evaluation Results of bias evaluations conducted by the Vendor to include the methodology for performing such tests (e.g., testing prompt pairs for politically oriented topics). The documentation shall also include Benchmark scoring results measuring the model's bias, helpfulness, honesty, or accuracy when provided with ambiguous versus straightforward questions. (Including any benchmarks comparing performance across multiple languages, where applicable).

7. **Description of Enterprise-Level Controls**
   The Contractor shall provide documentation describing the Enterprise Governance tools and controls, such as:
   a. Customizable system instructions that are additive to a base model's system prompts or content generation filters.
   b. Product features that require a model to cite sources of its outputs or otherwise provide visibility into the provenance of the model's outputs.
   c. AI System/LLM model evaluation tools that enable comparisons either between a model's outputs, or across various models.
8. **Third Party Modification Disclosure**
   The Contractor shall disclose of any additional controls to modify an AI Model's/LLM's output applied by the Contractor if the Contractor is not a direct developer of the LLM (e.g., classifiers, system prompts, fine-tuning, content moderation and filters, etc.)

Deliverable:

A. AI System/LLM Development and Operation Documentation Package

6.1.12.2 MONITORING, REPORTING, AND CORRECTIVE ACTION

The Contractor shall develop and implement a Compliance Monitoring and Reporting Plan supporting ongoing monitoring processes to evaluate AI outputs for compliance with Trustworthy AI and Unbiased AI principles. This plan shall include the mechanism for authorized users to provide end user feedback to report suspected violations of Truth-Seeking or Ideological Neutrality requirements.

The Contractor shall notify the COR within 10 business days of identifying any material deviation from these principles and shall submit a written Corrective Action Plan describing mitigation steps, responsible parties, and timelines. Any material deviation, corrective action taken, and results shall be detailed in the ***<Weekly or Monthly>*** Progress Reports.

Deliverable:

A. Compliance Monitoring and Reporting Plan
B. Corrective Action Plan

6.1.12.3 AI MODEL UPDATES AND CHANGE DISCLOSURES

The Contractor, in an AI Model/LLM Change Disclosure, shall notify the Government throughout the PoP in advance of any material changes to AI models, including new AI enhancements, features and/or components, controls, retraining, classifiers, system

prompts, fine-tuning, content moderation, filters, version replacement, or architectural changes, that could reasonably affect compliance with Trustworthy AI or Unbiased AI principles. Updated documentation shall be provided to VA for VA approval prior to implementation of such changes.

Deliverable:

A. AI Model/LLM Change Disclosure

6.1.13 SOURCE CODE HARMONIZATION AND REUSE IN INFORMATION TECHNOLOGY (SHARE IT Act)

The Contractor shall comply with the Source Code Harmonization and Reuse in Information Technology (SHARE IT) Act, P.L. 118-187, when developing and delivering custom code first produced for the VA in the performance of this Contract/Order. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14, to include without limitation, all custom-developed code and other key technical components of the code (including documentation, data models, schemas, metadata, architecture designs, configuration scripts, and artifacts required to develop, build, test, and deploy the code). Custom-developed code includes source code, or segregable portions of source code and all documentation created in support thereof to include source code written for a software project, product, module, plugin, script, middleware, or application programming interface.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☐	☒	☐
5.2	☐	☒	☐
5.3	☐	☒	☐
5.4	☐	☒	☐
5.5	☐	☒	☐
5.6	☐	☒	☐

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.7	☐	☒	☐
5.8	☐	☒	☐
5.9	☐	☒	☐
5.10	☐	☒	☐
5.11	☐	☒	☐
5.12	☐	☒	☐
5.13	☐	☒	☐
5.14	☐	☒	☐

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 6.2.1 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 (or its successor) are to encrypt the file, use a secure fax, or use a traceable mail service. (Note that by September 22, 2026, all FIPS 140-2 certificate validations will be placed on the Historical List. See FIPS Transition Effort

Timeline for more details: https://csrc.nist.gov/projects/fips-140-3-transition-effort#schedule)

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 Personnel Security Adjudication Center (PSAC) 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 PSAC 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 Defense Counterintelligence and Security Agency (DCSA) National Background Investigation Services (NBIS) Electronic Application (eAPP) (formerly e-QIP) after receiving an email notification from the PSAC.

f. The Contractor employee shall certify and release the eAPP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the PSAC. These documents shall be submitted to the COR within 3 business days of receipt of the eAPP notification email. (Note: DCSA 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 eAPP).

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 4), signed “Contractor Rules of Behavior”, and with a valid, operational Personal Identity Verification (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 DCSA. 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 DCSA.

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. PIV 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 suite, MS Word, MS Excel, MS PowerPoint, MS Project, MS Access, MS Visio, AutoCAD, 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 in addition to the task specific SLAs throughout the PWS and Attachment 001 – Service Leve Agreement.

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	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. 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

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) and now the Azure Virtual Desktop (AVD) (as VA is currently transitioning from CAG to the AVD), are the current and only VA approved methods 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 System Security Officer (ISSO) 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. 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 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. Government Furnished Property (GFP) may also include Government Furnished Material (GFM), Government Furnished Information (GFI), and GFE and shall be identified in the individual TO.
Number of Laptops: XXXX

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

Not applicable

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to assessment and authorization and continuous monitoring.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before 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)

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

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)

- ☒ E204 Functional Performance Criteria
- ☒ E206 Hardware Requirements
- ☒ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

A3.2. Compatibility with Assistive Technology

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

A3.3. Acceptance and Acceptance Testing

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

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

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall 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

Not applicable

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

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

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

B1. GENERAL

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

B2. VA INFORMATION CUSTODIAL LANGUAGE

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter “contract”) unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

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

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 Vetting 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

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

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

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-26-05 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. 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

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

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

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

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

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

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

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

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

B11. CRYPTOGRAPHIC REQUIREMENT

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

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

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

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

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

B12. PATCHING GOVERNANCE

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)

Not applicable

B14. DATA CENTER PROVISIONS

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

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

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

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

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

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