



PERFORMANCE WORK STATEMENT DEPARTMENT OF VETERANS AFFAIRS

**Office of Information & Technology
Veterans Health Administration
Office of Finance, Managerial Cost Accounting Office**

Managerial Cost Accounting Software as a Solution

**Date: 09/24/2026
PWS Version Number: 1.0**

Managerial Cost Accounting SaaS Solution

VA-27-00007279

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information & Technology (OIT), VHA Office of Finance, Managerial Cost Accounting Office (MCAO) strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

Managerial Cost Accounting (MCA) is the VA program office responsible for systematically accumulating, monitoring, and reporting the full cost of VA-provided services and products in accordance with federal cost accounting standards. MCA operates under the authority of VA Financial Policy Volume XIII, Chapter 3, and aligns with the Chief Financial Officers (CFO) Act of 1990, Federal Financial Accounting Standards (SFFAS) No. 4, the Federal Financial Management Improvement Act (FFMIA) of 1996, the 2010 Government Performance and Results Modernization Act, Federal Financial Management System Requirements (FFMSR) 8, and OMB Circular A-130.

MCA serves front-end users at VA Medical Centers (VAMCs) nationwide, administrative users within MCAO, and super users within OIT. The system processes upward of 130 million data points per month and supports monthly year-to-date managerial cost accounting modeling for VHA, VBA, and NCA. The future solution must ingest clinical and financial data and connect securely to VA's Summit Data Platform (SDP), Corporate Data Warehouse (CDW), and source systems including the Financial Management System (FMS), Integrated Financial and Acquisition Management System (iFAMS), VistA, and Oracle Health.

VA is committed to modernizing its cost accounting infrastructure in alignment with VA Directive 6517 (Cloud Systems), VA's Zero Trust First Cybersecurity Strategy, Federal Cloud-First Policy, and FedRAMP authorization requirements. The MCA Software as a Solution (SaaS) solution's security and authorization requirements will be met through implementation of and adherence to NIST SP 800-53 Revision 5, VA Directive 6500, and VA Handbook 6500.6 Appendix C. The solution must obtain a VA Authority to Operate (ATO) prior to processing any VA data.

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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 \(idmanagement.gov\)](https://www.ficam.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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

**Managerial Cost Accounting SaaS Solution
VA-27-00007279**

3.0 SCOPE OF WORK

The VA requires a Commercial Off-the-Shelf (COTS), Software as a Service (SaaS) managerial cost accounting solution, together with the integration, configuration, testing, training, and production deployment services in accordance with the requirements of this PWS and Attachment 1 - Managerial Cost Acctg Solution Req 9.29.26. The Contractor shall provide the solution as a firm-fixed-price subscription for the life of the contract, inclusive of all major and minor releases, security patches, and vendor-supported enhancements, and shall assist VA in achieving and maintaining a VA ATO for the solution throughout the period of performance.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be 12 months from date of award, with four 12-month option periods. The overall Period of Performance shall not exceed 60 months.

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. All training sessions specified in Section 5.3 shall be delivered virtually.

**Managerial Cost Accounting SaaS Solution
VA-27-00007279**

4.3 TRAVEL

No travel is anticipated under this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

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 MONTHLY REPORTING REQUIREMENTS

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

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

Deliverable:

- A. Monthly Progress Report

Managerial Cost Accounting SaaS Solution VA-27-00007279

5.1.3 KICKOFF MEETING

Within three (3) calendar days of award, the Contractor shall host a Kickoff Meeting with VA via telephone or virtual conference. Key Contractor personnel involved in delivering the solution shall be introduced to the VA Program Manager (PM), Contracting Officer's Representative (COR), and other key VA stakeholders. A review of the contract deliverables and timelines shall occur to ensure all key VA stakeholders and Contractor personnel work collaboratively to ensure success of the DO.

5.2 SAAS SOLUTION REQUIREMENTS

The Contractor shall provide a COTS, SaaS managerial cost accounting solution meeting the requirements below and as further detailed in Attachment 1 – Managerial Cost Acctg Solution Req 9.29.26.

The Contractor's SaaS solution shall meet the following minimum required capabilities:

1. **Deployment.** The Contractor's solution shall:
 - Operate as a cloud-hosted solution with no on-premises VA infrastructure required;
 - Support a centralized enterprise cost model; and
 - Provide separate Development, Test, Production, and Training environments.
2. **Security Authorization.** The Contractor's solution shall comply with NIST SP 800-53 Rev 5 controls and be capable of achieving a VA ATO. Existing FedRAMP authorization (any impact level), if held, shall be disclosed but is not required for award.
3. **Authority to Operate.** The Contractor's solution shall be capable of achieving a VA ATO within 60 calendar days of completed VA Office of Information Security (OIS) authorization intake. The Contractor shall provide all technical documentation, artifacts, and support necessary to enable timely VA OIS review and shall respond to VA OIS requests without delay that would extend this timeframe.
4. **Accessibility.** The Contractor's solution shall be compliant with the Rehabilitation Act of 1973, as amended. (*Cross-reference PWS Addendum A, "Notice of the Federal Accessibility Law" section — do not duplicate full 508 language here.*)
5. **Hosting Location.** The Contractor's solution shall be physically located within the Continental United States.
6. **Scale — Cost Centers.** The Contractor's solution shall support a minimum of 2,000 cost centers.
7. **Scale — Cost Activities.** The Contractor's solution shall support a minimum of 100,000 unique cost activities.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

8. **Scale — Data Ingestion.** The Contractor's solution shall support ingestion of at least 130 million records per month from multiple financial, operational, and clinical source systems using configurable interfaces and standard integration methods.
9. **Processing Performance.** The Contractor's solution shall:
 - Complete monthly cost model processing within 3 business days following receipt of all required source data;
 - Support configurable business-rule validation and exception reporting; and
 - Support a minimum of 120 concurrent users without degradation of performance.
10. **Costing Methodology.** The Contractor's solution shall support full-cost computation and activity-based, job, and standard costing consistent with SFFAS No. 4 and VA Financial Policy Volume XIII, including administrator-configurable allocation rules, cost drivers, cost activities, mappings, and business rules without custom software development.
11. **Costing Precision.** The Contractor's solution shall support activity driver/weighting factor calculation to 8 decimal places (4 decimal places for DSSRVU generation).
12. **Authentication.** The Contractor's solution shall support:
 - PIV-based Multi-Factor Authentication (MFA);
 - SSOi/SSOe federation; and
 - Role-based access controls. *(This complements, not replaces, PWS Section 6.1.3 FICAM — no conflict, both apply.)*
13. **Encryption.** The Contractor's solution shall provide:
 - AES-256 encryption at rest; and
 - HTTPS/TLS encryption in transit.
14. **Network Security.** The Contractor's solution shall be compliant with all applicable VA TIC 3.0 requirements. *(Cross-reference PWS Section 6.1.5 TIC.)*
15. **Reporting.** The Contractor's solution shall support:
 - Export to CSV, TXT, and Microsoft Excel;
 - Configurable ad hoc reporting;
 - Scenario ("what-if") analysis without affecting production cost models; and
 - Standard vendor-provided reporting capabilities (custom report development is not required).
16. **Outbound Extract Throughput.** The Contractor's solution shall support a minimum of 500+ GB annually in outbound extracts without error.
17. **Integration.** The Contractor's solution shall support API-based connectivity and configurable interfaces with VA enterprise systems, including but not limited to SDP, CDW, FMS, iFAMS, Vista, Oracle Health, IEAMS Vista, and other Government-approved source systems.
18. **Programming Languages.** The Contractor's solution shall use only commonly supported programming languages with readily available documentation.
19. **Licensing.** The Contractor's SaaS subscription shall include, at no additional cost to the Government throughout the period of performance including all exercised option periods:
 - All major and minor releases;

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- Security patches and updates;
 - Vendor-supported product enhancements; and
 - Support for a minimum of 120 named users.
20. **Care in the Community (CITC) Support.** The Contractor's solution shall support scenario modeling to compare CITC and VHA-provided care costs for make/buy analysis.
21. **Auditability.** The Contractor's solution shall maintain audit history for configuration changes, data loads, cost model execution, and user activities to support auditability and traceability.
22. **SaaS Support Services.** The Contractor shall provide ongoing maintenance and support services for the SaaS solution throughout the period of performance, including all exercised option periods. Support services shall adhere to the following:
- Unlimited software support services shall be available by phone and through a Contractor-provided support channel Monday through Friday from 8:00am – 8:00pm EST, at minimum.
 - Support services must be provided from U.S.-based personnel and facilities located within the Continental United States.
 - Support services shall assist with remediation of all vulnerabilities identified through Government security scans, consistent with the timeframes in Section 5.4.
 - The Contractor shall provide current versions of all software included in this PWS throughout the period of performance, including all major and minor releases, security patches, and vendor-supported enhancements, consistent with Item 19 (Licensing) above.
 - The Contractor shall respond to production system outages or degraded performance affecting cost model processing within 1 hours during support hours, given the operational impact of an outage on MCAO's monthly cost accounting cycle.

5.3 INTEGRATION AND CONFIGURATION SERVICES (FIXED SCOPE)

In addition to the SaaS solution requirements in Section 5.2, the Contractor shall provide the following discrete, fixed-scope implementation services necessary for system integration, configuration, testing, training, and VA production deployment.

The Contractor shall:

- Perform initial data source integration and API configuration for FMS, iFAMS, Vista, Oracle Health, and SDP/CDW.
- Perform cost model configuration, legacy DSS migration, data validation, and business rule configuration.
- Provide a FedRAMP/VA ATO technical support package.
- Provide end-user training and documentation, to include up to two instructor-led virtual training sessions and virtual Administrator training for up to eight personnel.

Managerial Cost Accounting SaaS Solution VA-27-00007279

- Provide production deployment, testing, and go-live support.

Deliverable:

- Cost Model Configuration and Migration Completion Certification

5.4 SAAS FEDRAMP ASSESSMENT, AUTHORIZATION, AND CONTINUOUS MONITORING REQUIREMENTS

The following three scenarios describe the Assessment & Authorization (A&A) and Authority to Operate (ATO) pathway applicable after contract award, based on the awardee's authorization status at that time. FedRAMP authorization status is not a condition of contract eligibility or award; VA will determine the required impact level through its risk categorization process (FIPS 199/NIST SP 800-53 Rev 5) in coordination with the awardee, consistent with VA Directive 6500 and Handbook 6500.6 Appendix C. For this solution the required impact level is Moderate.

VA will identify a Mission Owner for this system who will formally acknowledge risk at the time of authorization and hold ongoing accountability for meeting authorization conditions and continuous evaluation requirements. VA's target is to reach an authorization decision within 60 calendar days of completed intake. Upon a favorable determination, this system may be authorized through Continuous Evaluation rather than a traditional time-bound ATO. The Contractor's deliverable timelines below reflect the Contractor's submission obligations needed to support that intake and review; they do not themselves constitute the VA decision timeline, which runs from the Government's own intake completion.

5.4.1 IF THE SOLUTION IS NOT FEDRAMP AUTHORIZED

1. The information system solution selected by the Contractor shall comply with the Federal Information Security Management Act (FISMA).
2. The Contractor shall comply with [FedRAMP](#) requirements at the Moderate Impact Level, as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement.
3. The Contractor shall provide a SaaS product as defined by the following criteria: SaaS is an application delivery model in which the application is hosted on a cloud infrastructure outside the security boundary of VA and is provided to the Cloud Service Customer (CSC) over the internet. The CSC uses the SaaS offering via a thin-client interface, such as a web-browser or a program interface. The CSC subscribes to the SaaS offering and is only responsible for minor in-app customizations. The Cloud Service Provider (CSP) offering the application is responsible for management of the application, safeguarding of data stored or processed by the application, and all elements of the underlying infrastructure. Additionally, the CSP is responsible for all on-going compliance. In order to qualify as SaaS for use at VA, and to align with Federal Risk and Authorization Management Program

Managerial Cost Accounting SaaS Solution VA-27-00007279

(FedRAMP) requirements, the hosting for the offering must conform to the NIST 800-145 definition of Cloud Computing and thus contain following key characteristics:

- *On-Demand Self-Service*: The CSP fully automates the provisioning of both the customer interface and the underlying cloud components of the SaaS offering. In some cases, the CSP may provision internal resources manually, while providing the CSC an automated interface to request and track the service.
 - *Broad Network Access*: The SaaS capabilities are available over the internet or over a network that is available from all access points the CSC requires. The SaaS offering is accessible through common platforms (e.g., mobile phones, tablets, laptops, and workstations).
 - *Resource Pooling*: The computing infrastructure supporting the SaaS offering is shared among more than one CSC using a multi-tenant model, and resources are dynamically assigned depending on customer demand.
 - *Rapid Elasticity*: Computing capabilities are automatically provisioned and released in a manner that scales with customer demand. In some cases, the scaling of resources may not be fully automated, but it should be fast enough to support the needs of the CSC, which the CSC would have to define.
 - *Measured Service*: Resource usage, such as storage, processing, bandwidth, and user activity are measured and reported on in a manner that is relevant to the SaaS offering.
4. Following guidance from the Federal CIO, VA will utilize existing JAB ATO or agency ATO issued by another agency as a starting point for FedRAMP requirements. If neither of those exist, VA will sponsor The Cloud Service Provider for a FedRAMP Authorization. VA will be using the FedRAMP baselines as a starting point, since they are specifically tailored for cloud services.
 5. The Contractor shall, where applicable, assist with the VA ATO Process to help achieve agency authorization of the cloud service or migrated application at the impact level required by VA to utilize the product. For this solution the required impact level is moderate from the Data Security Categorization.
 6. The Contractor shall comply with FedRAMP requirements surrounding data location within the Continental United States. FedRAMP specifies data location requirements in the High Baseline as part of control SA-9 (5); however, FedRAMP does not provide or specify data location requirements for other baselines.
 7. The Contractor shall complete a FedRAMP System Security Plan (SSP) and supporting documentation including required attachments.
 8. The Contractor shall work with a VA DTC Subject Matter Expert to develop and provide a VA system boundary diagram including any integration and connectivity components for VA use. This will be known as the VA Implementation Diagram (VAID) and will demonstrate the proposed implementation of this system at VA.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

9. The Contractor shall complete a Third-Party Assessment Organization (3PAO) Security Assessment Plan (SAP).
10. The Contractor shall complete a 3PAO Security Assessment Report (SAR).
11. If new or unanticipated vulnerabilities are discovered by either VA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall bring the situation to the attention of the other party within one hour in accordance with Addendum B, VA Information and Information System Security/Privacy Language.
12. The Contractor shall comply with FedRAMP data management requirements.
13. Successful issuance of a VA ATO will be required before live VA data can be used in the system.
14. The Contractor shall participate in FedRAMP Continuous Monitoring activities as outlined by FedRAMP's Continuous Monitoring Strategy Guide found on the FedRAMP website.
15. The Contractor shall participate in monthly Agency and FedRAMP Sustainment meetings following the granting of a VA ATO.
16. The Contractor shall provide continuous monitoring activities including, but not limited to, scans, security artifacts, and provide Continuous Monitoring Monthly Scans and monthly Plan of Action and Milestones (POAM) reports as outlined by VA and FedRAMP requirements.
17. The Contractor shall provide a Monthly VA License Report of VA sites currently utilizing the cloud product post ATO award. The license report shall include the number of subscription licenses being utilized and the specific VA site where they're in use.

Deliverables:

- A. FedRAMP System Security Plan (SSP) and required Attachments
- B. VA Implementation Diagram
- C. 3PAO Security Assessment Plan (SAP)
- D. 3PAO Security Assessment Report (SAR)
- E. Plan of Action and Milestones Reports.
- F. Monthly VA License Report

5.4.2 IF THE SOLUTION IS FEDRAMP AUTHORIZED BUT NOT VA AUTHORIZED

1. The information system solution selected by the Contractor shall comply with the Federal Information Security Management Act (FISMA)
2. The Contractor shall remain in compliance 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 system must be FedRAMP Authorized at no less than the moderate level from the Data Security Categorization.
4. The Contractor shall provide confirmation of the completion of its FedRAMP System Security Plan (SSP) and supporting documentation by providing, to the VA PM, COR, and DTC, its repository ID number and associated link for VA to

Managerial Cost Accounting SaaS Solution
VA-27-00007279

download the SSP and all required artifacts within five calendar days of contract award.

5. The Contractor shall work with a VA DTC Subject Matter Expert to develop and provide a VA specific system boundary diagram including any integration and connectivity components for VA use. This will be known as the VA Implementation Diagram (VAID) and will demonstrate the proposed implementation of this system at VA.
6. The Contractor shall provide the results of their most recent Third-Party Assessment Organization (3PAO) Security Assessment Plan (SAP).
7. The Contractor shall complete a 3PAO Security Assessment Report (SAR).
8. The Contractor shall provide VA with the most recent monthly scans for the production environment within the authorization boundary and their scan upload schedule for FedRAMP within 30 calendar days of contract award.
9. The Contractor shall provide their availability to participate in monthly continuous monitoring meetings to be scheduled following successful VA ATO within 30 calendar days of contract award.
10. If new or unanticipated vulnerabilities are discovered by either VA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall bring the situation to the attention of the other party within one hour in accordance with Addendum B, VA Information and Information System Security/Privacy Language.
11. The Contractor shall comply with FedRAMP data management requirements.
12. Successful issuance of a VA ATO will be required before live VA data can be used in the system.
13. The Contractor shall participate in FedRAMP Continuous Monitoring activities as outlined by FedRAMP's Continuous Monitoring Strategy.
14. The Contractor shall participate in monthly Agency and FedRAMP Sustainment meetings following the granting of a VA ATO.
15. The Contractor shall provide continuous monitoring activities including, but not limited to scans, security artifacts, and provide Continuous Monitoring Monthly Scans and monthly Plan of Action and Milestones (POAM) reports as outlined by VA and FedRAMP requirements.
16. The Contractor shall provide a Monthly VA License Report of VA sites currently utilizing the cloud product post ATO award. The license report shall include the number of subscription licenses being utilized and the specific VA site where they're in use.

Deliverables:

- A. VA Implementation Diagram
- B. 3PAO Security Assessment Plan (SAP)
- C. 3PAO Security Assessment Report (SAR)
- D. Plan of Action and Milestones Reports
- E. Monthly VA License Report

Managerial Cost Accounting SaaS Solution
VA-27-00007279

5.4.3 IF THE SOLUTION IS FEDRAMP AUTHORIZED AND VA AUTHORIZED

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 remain in compliance 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 Level from the Data Security Categorization.
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 subscription licenses to FedRAMP authorized and VA authorized environments.
6. If new or unanticipated vulnerabilities are discovered by either VA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall bring the situation to the attention of the other party within one hour in accordance with Addendum B, VA Information and Information System Security/Privacy Language. VA Privacy and Security deliverables as directed by the VA System owner.
7. The Contractor shall comply with FedRAMP data management requirements.
8. Successful issuance of a VA ATO will be required before live VA data can be used in the system.
9. The Contractor shall participate in FedRAMP Continuous Monitoring activities as outlined by FedRAMP's Continuous Monitoring Strategy Guide found on the FedRAMP Website.
10. The Contractor shall provide continuous monitoring activities including, but not limited to, scans, security artifacts, and provide Continuous Monitoring Monthly Scans and monthly Plan of Action and Milestones (POAM) reports as outlined by FedRAMP requirements.
11. The Contractor shall participate in monthly Agency and FedRAMP Sustainment meetings following the granting of a VA ATO.
12. The Contractor shall provide a Monthly VA License report of VA sites currently utilizing the cloud product post ATO award. The license report shall include the number of subscription licenses being utilized and the specific VA site where they're in use.

Deliverables:

- A. Continuous Monitoring Monthly Scans
- B. Plan of Action and Milestones Reports.
- C. Monthly VA License Report

**Managerial Cost Accounting SaaS Solution
VA-27-00007279**

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 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

Managerial Cost Accounting SaaS Solution VA-27-00007279

Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, VA Handbook 6500, 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 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VIEWS 00155984, PIV Logical Access Policy Clarification <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>.

Managerial Cost Accounting SaaS Solution VA-27-00007279

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

Managerial Cost Accounting SaaS Solution VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution

VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution VA-27-00007279

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 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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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.

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

**6.1.11.1 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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- 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

6.1.11.2 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 monthly Progress Reports.

Deliverable:

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

6.1.11.3 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

6.2 SECURITY AND PRIVACY REQUIREMENTS

**Managerial Cost Accounting SaaS Solution
VA-27-00007279**

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	☐	☒	☐

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution

VA-27-00007279

- 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.

**Managerial Cost Accounting SaaS Solution
VA-27-00007279**

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 5.	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. 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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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:

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- ☒ 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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

N/A

**Managerial Cost Accounting SaaS Solution
VA-27-00007279**

**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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- 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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- 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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- (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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- (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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- (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 employees 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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- 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 through 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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

successor), M-21-31 and supporting NIST guidance. This applies to 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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- l. The Contractor shall comply with the Privacy Act of 1974 (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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- 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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

(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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

- 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

Managerial Cost Accounting SaaS Solution
VA-27-00007279

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)

N/A

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.

Managerial Cost Accounting SaaS Solution
VA-27-00007279

POINTS OF CONTACT

VA Program Manager:

Name: Provided at award.
Address: N/A
Voice: N/A
Email: N/A

Contracting Officer's Representative:

Name: Provided at award
Address: N/A
Voice: N/A
Email: N/A

Contracting Officer:

Name: Lori L. Walker
Voice: 512-981-4134
Email: lori.walker1@va.gov

Contract Specialist:

Name: Brianna Feaster
Voice: 848-377-5271
Email: Brianna.Feaster@va.gov

1.