36C10B18R2609 A0004

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO. | 1. CONTRACT ID CODE | PAGE 1 | OF PAGES 38

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NUMBER	5. PROJECT NUMBER (if applicable)
A0004			TAC-18-45446

6. ISSUED BY — CODE

Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

7. ADMINISTERED BY (If other than Item 6) — CODE

Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code)

To all Offerors/Bidders

CODE | FACILITY CODE

(X) | 9A. AMENDMENT OF SOLICITATION NUMBER: 36C10B18R2609

X | 9B. DATED (SEE ITEM 11): 08-14-2018

10A. MODIFICATION OF CONTRACT/ORDER NUMBER

10B. DATED (SEE ITEM 13)

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [X] is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor [ ] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

SEE CONTINUATION PAGE

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

CONTINUATION PAGE

The purpose of this Amendment A0004, to Request for Proposal (RFP) 36C10B18R2609 titled "VA Mobile Applications Cloud Migration (MACM)," is as detailed below. All changes to RFP 36C10B18R2609 have been captured in track changes.

1. Section B.5 Performance Work Statement, Paragraph 5.3.5 Software License Management (T&M) is hereby revised. See Section B.5 Performance Work Statement for revision.

Except as provided herein, all other terms and conditions of RFP 36C10B18R2609 remain unchanged and in full force and effect.

B.5 PERFORMANCE WORK STATEMENT

DEPARTMENT OF VETERANS AFFAIRS (VA)
Office of Information & Technology
Enterprise Program Management Office (EPMO)

VA Mobile Applications Cloud Migration (MACM)

Date: 8/14/2018
TAC-18-45446
Version Number: 2.0

1.0 BACKGROUND

The Department of Veterans Affairs (VA) continuously seeks ways to improve the services provided to Veterans and their families. VA is using mobile technologies to transform the Veteran experience by improving access to VA resources need wherever they are needed.

VA's Office of Information and Technology (OIT) has partnered with VHA's Office of Connected Care (OCC) to establish a VA Mobile Infrastructure (VA MIS) platform currently hosted by Booz Allen Hamilton and International Business Machines (IBM) Terremark. The VA MIS is a General Support System (GSS) in Assessment and Authorization/Authority to Operate (A&A / ATO) terminology, and acts as an umbrella for sharing common controls and management across multiple enclaves and major applications (apps). Currently, VA MIS uses dedicated hosting resources identified in Attachment 001 – Current Servers and Attachment 002 – Current Software Inventory to this document for hosting all mobile apps and supporting web services in the production pipeline. Currently there are between 20 and 30 mobile apps supporting services hosted in the VA Mobile Framework (VAMF) production environment.

The VA MIS Platform currently consists of three enclaves (two internal and one external):

- External Cloud Environment (ECE), which allows mobile app users demonstrations and agile development with no connectivity back to VA's network.
- Mobile Application Environment (MAE) for web and mobile app development.
- VAMF for production web and mobile apps.

In addition to the current operational environments in the VA MIS platform, additional environments are being commissioned in the VA Enterprise Cloud (VAEC), located in Amazon AWS GovCloud (VAEC-AWS) and Microsoft Azure Government Cloud (VAEC-AZC). These environments will host all new app deployments and will eventually be utilized to host all services currently located in ECE, MAE, and VAMF. VA has begun a migration effort for the VA Online Scheduling (VAOS) based on Kubernetes (K8S), GitHub Enterprise, Unbound DNS, and AWS CLI and the following open source technologies: Consul, Vault, Packer, Terraform (all from HashiCorp) Nexus, Jenkins, Ansible.

The replacement solution for the VA MIS platform shall be the VA Mobile Applications Cloud Migration (MACM) as described in this PWS. VA requires the implementation, phasing in, and migration of mobile apps and supporting services into an operational VA MACM. OIT's ultimate goal is to achieve a Continuous Integration/Continuous Deployment (CI/CD) platform through hosting technologies within VAEC-AWS and VAEC-AZC as part of the VAEC. A full break down between VAEC and VA MACM contractor responsibilities is detailed in the "VAEC Technical Reference Guide for Acquisition Support" dated October 2017 (Attachment 003).

2.0 APPLICABLE DOCUMENTS

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

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

5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
6. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
9. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
12. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, http://www.va.gov/vapubs/
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, http://www.va.gov/vapubs
14. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
15. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
16. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
17. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
22. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
23. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
24. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", July 28, 2016
25. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
26. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
27. VA Handbook 6500.6, "Contract Security," March 12, 2010
28. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
29. OI&T Process Asset Library (PAL), https://www.va.gov/process/ . Reference Process MACMs at https://www.va.gov/process/MACMs.asp and Artifact templates at https://www.va.gov/process/artifacts.asp
30. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
31. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014

32. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
33. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
34. VA Directive 6300, Records and Information Management, February 26, 2009
35. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
36. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 10, 2014
37. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
38. OMB Memorandum, "Transition to IPv6", September 28, 2010
39. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
40. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
41. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
42. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
43. 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
44. OMB memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
45. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
46. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
47. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
48. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
49. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
50. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
51. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
52. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
53. 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)
54. 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)
55. VA Memorandum "Mandate to meet PIV Requirements for New and Existing Systems" (VAIQ# 7712300), June 30, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846

56. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
57. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
58. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
59. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
60. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
61. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
62. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
63. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
64. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
65. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
66. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
67. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
68. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
69. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
70. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
71. "Veteran Focused Integration Process (VIP) Guide 2.0", May 2017, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
72. "VIP Release Process Guide", Version 1.4, May 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
73. "POLARIS User Guide", Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412
74. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
75. VA Memorandum "Updated VA Information Security Rules of Behavior (VAIQ #7823189)", September, 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
76. API Best Practices
    a. 18 F API Standards (https://github.com/18F/api-standards)
    b. WH API Standards https://github.com/WhiteHouse/api-standards
77. Building Twelve-Factor App (https://12factor.net/).

78. Experience with incorporating and using open source technologies (https://sourcecode.cio.gov/OSS/).
79. The Agile Manifesto (http://www.agilemanifesto.org/)
80. Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) (https://www.pmi.org/)
81. The U.S. Digital Services Playbook (https://playbook.cio.gov/)
82. The Techfar Hub (https://techfarhub.cio.gov/)
83. VA Enterprise Cloud (VAEC) Technical Reference Guide for Acquisition Support, October 2017 (Attachment 003)
84. Best Practices for Agile Practices (Attachment 004)
85. VA MACM Maintenance Definitions (Attachment 005).

3.0 SCOPE OF WORK

The Government requires a VA MACM solution that will be comprised of three environments, Development, Staging and Production, hosted in the VAEC. There will be approximately 20 - 30 mobile responsive web apps hosted in the MACM in addition to the services needed to support these apps.

The Contractor shall implement, operate, and maintain the VA MACM including all cloud services required to support VA MACM operations. The Contractor shall migrate mobile apps and supporting services into an operational VA MACM. The Contractor shall provide operations and maintenance (O&M) support of all VA MACM cloud environments as well as the infrastructure software contained within each environment. The Contractor shall provide all software and support required to create and maintain an operational VA MACM as described in this PWS. This effort also includes an optional task for transition out services.

The Government will provide the Contractor with access to the VAEC to include the credits required for all VAEC cloud development, testing, and production environment requirements. The VAEC includes a secure dedicated Wide Area Network connection between VA and the VAEC Cloud Service Provider (CSP). The Contractor shall not be responsible for buying cloud credits for this contract. The VAEC is currently supported by two Federal Risk and Authorization Management Program (FedRAMP) High Certified and VA ATO approved CSPs. Both VAEC environments provide access to all CSP's FedRAMP Authorized Services in each respective CSP cloud to implement the proposed solution. In addition, each VAEC CSP provides a set of common shared services such as security scanning; Active Directory and single-sign (SSO); PIV integration; and performance monitoring to facilitate solution implementation. Specifications for each VAEC CSP, including access requirements, will be provided at the project kick off meeting and in Attachment 003 to this document. For this effort the Contractor is required to utilize the VAEC-AWS environment for its platform and the Contractor shall be provided credits to the VAEC-AWS as Government Furnished Equipment (GFE) during contract performance.

4.0 PERFORMANCE DETAILS

This is a hybrid Firm-Fixed Price (FFP)/Time-and-Materials (T&M)/Labor-Hour type contract. Only tasks identified as T&M shall be on a T&M basis.

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be a base of 12 months followed by four (4) 12-month option periods. There are 10 Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

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

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

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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their submission**.**

4.3 TRAVEL

The Government anticipates travel to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. The meeting locations shall be located in St. Petersburg, Florida or Washington DC. The Contractor shall include all estimated travel costs in its FFP line items. These costs will not be directly reimbursed by the Government. The following is the estimated travel for the FFP portion of the effort.

Purpose	Number of Trips	Number of Days	Number of Staff	Base/Option
Kick-off Meeting	1	1-3	4	Base
Quarterly Program Reviews	4	1-3	4	Base and Option

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule,

milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon by the VA Program Manager (PM). The VA PM will provide detailed comments on the initial baseline CPMP, which shall be incorporated in the operational CPMP. The CPMP shall be updated based on input provided by the VA PM and shall be updated and maintained monthly thereafter throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall deliver Monthly Status Reports. These reports shall provide accurate, timely, and complete project information supporting reporting Requirements. The Monthly Status Report shall include the following data elements and reporting capability shall address the below requirements:

a. Project Name
b. Overview and description of the contract
c. Overall high-level assessment of contract progress
d. All work in-progress and completed during the reporting period
e. Identification of any contract related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
f. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
g. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
h. Work planned for the subsequent four reporting periods, when applicable
i. Current contract schedule overlaid on original contract schedule showing any delays or advancement in schedule
j. Provide expenditures based upon your proposed spend plan.
k. Workforce staffing data showing all Contractor personnel performing on the effort by task during the current reporting period along with status of their background investigation/VA clearance and biographies. After the initial labor baseline is provided, each Monthly Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract.
l. Original schedule of deliverables and the corresponding deliverables made during the current reporting period.
m. Cost analysis that includes consumption of cloud resources by app.
n. Software licenses at or nearing end of life and software security certificates nearing expiration.

The report shall also include an itemized list of all Electronic and Information Technology (EIT) 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.
For each T&M task, indicate:

a. Summary of work performed
b. Expenditures for the reporting period
c. Contract Line Item Number expenditure
d. Burn rate
e. Percentage of work completed

Deliverable:
A. Monthly Status Report

5.1.3 TECHNICAL KICK-OFF MEETING

The Contractor shall conduct a kick-off meeting with the VA PM, Contracting Officer's Representative (COR) and the Contracting Officer (CO). The meeting shall be held within 10 business days after contract award. The kick-off meeting shall be a face-to-face meeting in a VA or VA-approved Contractor facility. The Contractor shall propose an agenda for VA COR approval three days prior to the meeting. The Contractor shall provide meeting minutes capturing discussion, agreements, and action items resulting from the kick-off meeting. The kick-off meeting shall address post award topics and shall present the Contractor's draft plans and approach for meeting PWS requirements.

5.1.4 KEY PERSONNEL

Specific expertise and experience in Program/Project Management, Cloud Architecture, Configuration Management, and Information Security is essential for accomplishing the tasks outlined in this PWS. The key personnel positions are identified below along with the minimum requisite qualifications for each position.

Key Personnel Positions:

- Project Manager:
  - Expertise Managing Entire Agile Software Development Life Cycle for a project of at least one million dollars up to and including production delivery and some phase of post-delivery support.
  - Expertise Managing Project with at least 15 software professionals with a duration of greater than one year.
- Chief Cloud Architect:
  - Background as a Software Engineer for at least three years prior to a position as a Cloud Architect.
  - Expertise as a Software Engineer for at least one project using Container Orchestration and AWS GovCloud.
  - Cloud Architect or Senior Engineer on a Production System in one of the VAEC CSP Vendors' Clouds.
  - Cloud Architect or Senior Engineer on a Production System that uses a Container Orchestration System.
- Chief Configuration Manager:
  - Background as a Lead Developer, Lead Release Manager, or Lead/Chief Configuration Manager for at least one year.
- Chief Network and Security Architect:
  - Background as a Software Engineer, Site Reliability Engineer, or DevOps Engineer for at least three years prior to a position as an Architect.
  - Security Architect or Senior Engineer on a Production System using a Software Defined Infrastructure.

    - Security Architect or Senior Engineer on a Production System using one of the VAEC CSP Vendors Clouds.
- Chief Operations Manager:
    - Expertise running a 24x7 Software based System for at least 6 months.
    - Experience with oversight of an operations team of at least 5 people for at least one year.
    - Expertise in Incident Management for a Software based System.
    - Expertise with oversight of a team running a trouble ticket system.

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

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

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

The Contractor agrees that it has a contractual obligation to mitigate the consequences of the loss of Key Personnel and shall promptly secure any necessary replacements in accordance with (IAW) this PWS section. Failure to replace a Key Personnel pursuant to this clause and without a break in performance of the labor category at issue shall be considered a condition endangering contract performance and may provide grounds for default termination.

5.1.5 DAILY STATUS UPDATES

The Contractor shall support daily status meetings to discuss issues, propose resolutions, plan moves/add/changes, plan upgrades, and resolve tickets. These meetings will be conducted via teleconference.

5.1.6 PRIVACY AND HIPAA TRAINING

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

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

Deliverables:

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

5.2 VA MACM PLATFORM DEVELOPMENT AND APP MIGRATION

The Contractor shall provide cross-functional Contractor Sprint Teams to support the development of the VA MACM Platform and the migration of mobile apps from the VA MIS platform to the VA MACM Platform. Both development of the VA MACM Platform and migration of mobile apps to the VA MACM Platform shall take place in iterative two-week sprints. The Government estimates that each Contractor Sprint Team shall be comprised of 5 - 7 staff. The Contractor may invoice at the end of each sprint upon Government acceptance of the Sprint Certification Package and Artifacts.

For MACM platform development and migration tasks, the Contractor shall follow an agile continuous integration (CI) / continuous deployment (CD) methodology, as outlined in "Best Practices for Agile Processes" (Attachment 004), that may result in several releases in each sprint. If app development releases are required, the Contractor shall follow OIT's Veterans Integrated Process (VIP) requirements, IAW PWS Section 6.1.6, in coordination with the VA PM/COR, the VA Product Owner, and OIT personnel.

The specific scope of functionality of the tasks will be determined by VA App Product Owners and the VA PM/COR, prior to sprint commencing. The Contractor shall adjust deliverables and updates to match the nature of each task.

At the beginning of each two-week sprint, each Contractor Sprint Team shall initiate, coordinate, and participate in a Sprint Planning Meeting and develop a Sprint Plan with the VA Project Team, including the VA PM, COR, designated VA Product Owner and additional stakeholders, to plan the work to be accomplished for the sprint. Additionally, the team shall determine the acceptance criteria for the sprint and populate the Sprint Backlog. The Contractor, in collaboration with the VA Project Team, shall use an Agile Poker Estimation technique to define the relative complexity of each task and determine the amount of work that can be accomplished. All activity scheduled in each sprint and backlog shall be captured and have status showing all work items, changes, impediments, and retrospectives. The Contractor shall update the Sprint Plan at the conclusion of sprint planning. Once the Sprint Plan is accepted by the VA PM/COR

and the VA Product Team, the sprint backlog may change throughout the duration of the sprint, however, the effort of work will remain constant.

The Contractor shall provide Sprint Demonstration that confirms all functionality developed in the sprint is operational. At the Sprint Demonstration, the Contractor Sprint Team shall submit a Sprint Certification Package to the VA PM/COR for review and approval.

The Sprint Certification Package shall include a summary of the planned, accomplished, and unaccomplished work for the two-week sprint to include issues encountered and corrective actions taken as well as all artifacts produced, including any and all code (submitted to VA source code repository), during the sprint. This package, certification that all work is completed, and a demonstration that all work planned for the sprint has been fully implemented, are necessary for sprint acceptance by the Government. The Contractor must complete all work planned for each sprint and receive VA PM/COR approval of the Sprint Certification Package for the prior two-week sprint before beginning a new sprint.

The Contractor shall provide 13 sprints in the base contract period for the development of the VA MACM Platform and the migration of mobile apps from the VA MIS platform to the VA MACM Platform. The Contractor may be required to staff 1 – 4 Sprint Teams in parallel.

The price for the delivery of the Minimum Viable Product (MVP) as defined in PWS 5.2.1 is 100 percent of the fixed-price of each sprint provided the Contractor successfully delivers and the Government accepts the MVP within three months from contract award. Upon Contractor delivery and Government acceptance of each sprint, the Government shall pay 75 percent of the fixed-price of the sprint. Upon the successful delivery and acceptance of the MVP within three months from contract award, the Government shall pay the Contractor the remaining 25 percent of the fixed-price of each sprint withheld at the time of each Sprint delivery. In the event the Contractor delivers the MVP later than three months from contract award, the price for the delivery of the MVP shall be 75 percent of the fixed-price for each sprint. The Government will continue to pay 75 percent of the fixed-price of each sprint until successful delivery and acceptance by the Government of the MVP. Notwithstanding when the MVP is delivered and accepted by the Government, the Contractor remains obligated to deliver the MVP and failure to deliver the MVP within a commercially reasonable time from contract award will be deemed a condition endangering contract performance and may provide grounds for default termination. Upon successful delivery and acceptance of the MVP, additional sprints for the Mobile Application Migration IAW PWS Section 5.2.2 will be paid at 100 percent of the fixed-price of each sprint.

The below subtasks contain the basic requirements for the development of the VA MACM MVP as well as app migration. Once the VA MACM MVP has been delivered by the Contractor, additional sprints will enhance, maintain, and sustain VA MACM as well as perform app migration through the period of performance of this contract.

Deliverables:

A. Sprint Plan
B. Sprint Certification Package and Artifacts with Source Code

5.2.1 VA MACM MVP REQUIREMENTS

The Contractor shall deliver a stable and functional VA MACM MVP which meets each and every baseline requirement as set forth below in order to support all VA Mobile Application engineering activities such as application operations, development, testing, and troubleshooting. The Contractor shall provide the configuration, administration, integration, application programming Interface (API) configuration, and future upgrades of the VA MACM. The baseline requirements for the VA MACM MVP shall include the following:

a. Container Orchestration System
b. Continuous Integration and Continuous Delivery System
c. Monitoring of availability and accessibility
d. Access Auditing
e. External Connectivity
f. Test Case Management and Automation Framework
g. Infrastructure, platform, and apps successfully build from code
h. Intermediate artifacts are stored in repositories
i. Deployable runtimes that have successful health checks
j. Established Incidence Response procedure
k. Integration of Project Management Systems, including:
l. A Ticketing system (e.g. JIRA and its Plugins)
m. A Knowledge management system (e.g. Confluence and its Plugins)
n. A Source Code Management system (e.g. GitHub Enterprise)
o. A Service Desk support tool (e.g. JIRA Help Desk Atlassian)
p. A real-time collaboration system (e.g. HipChat)
q. As necessary a single sign on service (e.g. Crowd)
r. VA MACM Standard Operating Procedures (SOP) and Tooling Support Plan to support the use of development and engineering tools to be used in MACM environments
s. Developer's Manual that instructs development teams on how to build, deploy, test, and monitor their apps using the platform
t. Automated ad-hoc build analytics as well as the ability to provide system performance analytic reports requested by the VA.
u. Display a working health check application, running in the VA MACM production environment that shows the running status of the orchestration software.

The Contractor shall include all project artifacts in the Sprint Certification Package.

Rights in Computer Software:
The Contractor is required to deliver the VA MACM MVP, technical data, configurations, documentation or other information, including source code, during contract performance. The Government shall receive Unlimited Rights in intellectual property first produced and delivered in the performance of this contract in accordance with FAR 52.227-14, Rights In Data-General (DEC 2007). This includes all rights to source code and any and all documentation created in support thereof. License rights in any Commercial Computer Software shall be governed by FAR 52.227-19, Commercial Computer Software

5.2.2 MOBILE APPLICATION MIGRATION

The Contractor shall migrate all VA mobile applications located in IBM Terremark (currently 20 to 30 mobile apps; however, the number of apps may change) as well as all associated databases

and supporting services to the VA MACM IAW sprint planning activities. Each app shall be migrated from IBM Terremark to the MACM and the Contractor shall demonstrate that the app is working in all MACM environments using the CI/CD system.

The Contractor shall include all project artifacts in the Sprint Certification Package.

5.2.3 ADDITIONAL VA MACM PLATFORM DEVELOPMENT APP MIGRATION SUPPORT (OPTIONAL TASK)

In the event the Government exercises the Optional Task in the base period or any option period, the Contractor shall provide up to 32 iterative two-week sprints, as defined in PWS Section 5.2 above, to enhance, maintain, and sustain VA MACM as well as perform app migration through the period of performance of this contract.

5.3 MOBILE ENVIRONMENT SUPPORT

5.3.1 VA MACM OPERATIONS AND SYSTEM MAINTENANCE SUPPORT

The Contractor shall maintain and operate the ongoing availability of VA MACM. The Contractor shall develop a VA MACM Operations and Maintenance (O&M) Support Plan that details the Contractor's plan to maintain all VA MACM including incidence resolution procedures. The Contractor shall deliver the VA MACM O&M Support Plan to the VA PM/COR for review and approval.

The Contractor shall maintain and operate multiple VA environments within MACM including, but not limited to the following environments:

- Development
- Staging/Testing
- Production

Each VA environment may be divided into sub-environments as determined by VA. The Contractor shall ensure that all software associated with maintaining and operating the VA MACM is delivered and tracked on VA owned and operated version control systems. The Contractor shall ensure COTS software is licensed appropriately. VA shall provide the Contractor with access to such systems.

The Contractor shall provide VA MACM system maintenance to include corrective maintenance; adaptive maintenance; perfective maintenance; and preventative maintenance to ensure all apps and services hosted in MACM are continuously available, function correctly, provide current information features, and provide the best possible user experience. Maintenance types are defined in the "VA MACM Systems Maintenance Definitions" (Attachment 005). The Contractor shall:

a. Provide 24x7 Production support for VA MACM application infrastructure; database infrastructure to support database systems; security, and their utilities IAW the approved VA MACM O&M Support Plan.
b. Provide Database Administration (DBA) support to cloud-based and hosted database systems in the VA MACM.
c. Provide non-production environment support during normal VA business hours (7 am – 9 pm EST).

d. Identify requirements for additional functionality within the application infrastructure. The Contractor shall include the results of this activity in an Application Infrastructure Recommendations Report appended to the Monthly Status Report.
e. Monitor system, network, application, database logs, and Service Level Agreement (SLA) metrics via VA approved monitoring tools and provide a real-time dashboard available to all program stakeholders.
f. Write and monitor synthetic monitoring scripts for VA infrastructure and apps.
g. Provide configuration management and change control with VA and other teams as directed.
h. Provide external systems integration support through configuring, testing, and documenting the integration.
i. Provide database performance monitoring and provide results and recommendations for optimizing performance in a Database Optimization Recommendations Report appended to the Monthly Status Report.
j. Provide operations support for the container orchestration platform.
k. Perform system upgrades and patches within pre-defined maintenance windows.
l. Define and administer users and user groups, and user access.

The Contractor shall be responsible for the break-fix of any apps hosted in the MACM environment affected by changes made to the environment by the MACM Contractor.

The Contractor shall provide an SLA Monitoring Plan that defines how SLA metrics will be monitored throughout the performance of the requirements, including the automated testing tools and automated SLA testing scripts that shall be used. The Contractor shall provide the SLA Monitoring Plan to the VA PM/COR for review and approval. Upon approval, the Contractor shall implement SLA monitoring IAW the approved plan and establish an SLA Dashboard that provides real time SLA metrics data available to all program stakeholders. The Contractor shall provide a VA MACM SLA Report on a biweekly basis which shall capture data as specified in the Deliverable Metrics/SLAs.

Deliverables:

A. VA MACM O&M Support Plan
B. SLA Monitoring Plan
C. VA MACM SLA Report

DELIVERABLE METRICS/SLAs:

System Availability: The Contractor shall provide an aggregate uptime for all MACM components (i.e. databases, services, servers, storage) of no less than 99.9%. When this outcome is achieved an external entity shall be able to log into the environment, execute build and deploy jobs in the development enclave, and observe the results of those jobs. Services that are faulted due to an external entity shall have trouble tickets logged by the MACM Contractor with the responsible party, with all outage time attributable to the MACM Contractor until the ticket is logged with the responsible external entity. If any outage is later determined to not be the fault of the external entity, then the fault is attributed to the MACM Contractor. Services that are unavailable due to upstream maintenance must have an outage notification to all VA stakeholders prior to the maintenance window for attribution to the upstream team. The Contractor shall have access to the Government's published maintenance window times and dates upon award. An automated test, IAW the approved SLA Monitoring Plan, and the logged

reports of execution, including timing details, of that test shall be provided in the VA MACM SLA Report.

Development Environment Availability: The Mobile Application Development Environment shall be available during normal VA business hours (7 am – 9 pm EST). An external entity shall be able to log into the environment, execute build and deploy jobs in the development enclave, and observe the results of those jobs with no less than 99.9% availability. An automated test, IAW the approved SLA Monitoring Plan, and the logged reports of execution, including timing details, of that test shall be provided in the VA MACM SLA Report.

Service Availability: All deployed services shall be available and functional to serve user requests at no less than 99.9% availability. An external entity shall be able to access and receive a successful response to all services deployed to this platform at all times. As available on a per service basis sample transactions or health check endpoints that are exposed to external entities shall be evaluated to determine if the response is successful. Services that are faulted due to an external entity shall have trouble tickets logged with the responsible party, with all outage time attributable to this team until the ticket is logged with the responsible entity. An automated test, IAW the approved SLA Monitoring Plan, with an execution frequency of no more than 300 seconds, and the logged reports of execution, including timing details, of that test shall be provided in the VA MACM SLA Report. Any faulted services attributed to an external entity shall include a record of the trouble ticket that was issued to the responsible party. This record shall include the time that it was filed, and if resolved, the time of resolution. Any maintenance window outages shall include a record of the notification that was distributed to VA Stakeholders, and the time which the record was distributed.

S**ervice Uptime:** Services run on this platform shall remain online no less than 99.9% of the time. All scheduled services will remain active and able to serve requests. An automated test, IAW the approved SLA Monitoring Plan, with an execution frequency of no more than 300 seconds, and the logged reports of execution, including timing details, of that test shall be provided as a report to the VA. All scheduled services and their associated uptime shall be provided in the VA MACM SLA Report.

Service Reachability: Services on this platform shall be reachable by outside entities no less than 99.9% of the time. All required routing and proxying services are correctly functioning and forwarding traffic. Services that are faulted due to an external entity shall have trouble tickets logged with the responsible party, with all outage time attributable to this team until the ticket is logged with the responsible entity. Services that are unavailable due to upstream maintenance must have an outage notification to all VA stakeholders prior to the maintenance window for attribution to the upstream team. The Contractor shall have access to the government's published maintenance windows times and dates upon award. An automated test, IAW the approved SLA Monitoring Plan, and the logged reports of execution, including timing details, of that test shall be provided in the VA MACM SLA Report.

5.3.2 SECURITY

5.3.2.1 SECURITY OPERATIONS AND MONITORING AND MANAGEMENT

The Contractor shall provide support for security operations and monitoring of VA MACM.

The Contractor shall:

a. Assign a Security officer to manage all security related task.
b. Provide 24x7x365 on call staffing for response to alerts from Network Operations Center (NOC) and/or Security Operations Center (SOC).
c. Create 24x7x365 automated monitoring and alerting
d. Continuously monitor and report the security status of the system on a regular and ad-hoc basis.
e. Provide Remediation and documentation of findings in the security assessment reports as requirement.
f. Identify and report any incidents using existing tools and strategies IAW the VA incident handling policies (VA Handbook 6500.5)
g. Conduct regular infrastructure, network and code scanning/penetration to report any security vulnerabilities based on result reports with a recommendation and/or corrective plan of action.
h. Conduct yearly security game day exercise.
i. Update security documentation.
j. Create a monthly Security Assessment Report that includes:
    - Number of Incidents
    - Number Anomalies
    - Results of Penetration test
    - System down time
    - Provide Remediation and documentation of findings in the security assessment reports as requirement.

Deliverable:

A. Monthly Security Assessment Report

5.3.2.2 AUTHORITY TO OPERATE (ATO)

The Contractor shall develop and maintain Application/Infrastructure security documentation in support of achieving and maintaining an ATO at MACM (major application) and GSS levels.

The Contractor shall:

a. Comply with VA ATO process.
b. Use VA FISMA control tracking system as the security documentation repository to complete and update security controls.
c. Coordinate with the VA security office and adhere to its policies.
d. Complete all VA required training (i.e. on-boarding, security, ethics, etc.) as well as provide certificates of completion to the COR.
e. Create, as directed, a wide variety of National Institute of Standards and Technology (NIST) SP800-Series security artifacts per FISMA requirements for VA systems.
f. Enter data into the VA security documentation repository, which is currently known as RiskVision and runs on a Trusted Agent FISMA application.
g. Manually review upcoming due dates for security artifacts and work with system maintainers or appropriate representatives to ensure artifacts are updated annually.
h. Support, and develop annual attestation documentation in conjunction with the system maintainer and business owner.
i. Peer review security artifacts and provide feedback to document authors.
j. Coordinate and lead quarterly familiarization exercise for Contingency Plan and Incident Response Plan.

k. Provide security documentation reporting to PMs, Information Security officers (ISO), and others.
l. Update existing Privacy Impact Analysis (PIA), System Security Plan (SSP) documents and create new PIA documents as required in support of VA apps.
m. Update ATO package as necessary

Deliverable:

A. ATO Package Documentation

5.3.2.3 SECURITY INCIDENT MANAGEMENT

The Contractor shall facilitate and triage response to security incidents reported using existing tools and strategies IAW VA Incident Handling policies (VA handbook 6500.8). The Contractor shall provide on call support 24x7x365.

5.3.2.4 SECURITY CONTROL ASSESSMENT (SCA)

The Contractor shall proactively prepare for and actively participate in interviews, examinations, testing and reviews from the auditing community. This supports external and internal audit activities, Office of Inspector General (IG) audits, FISMA audits, third-party audits and self-assessments. The Contractor shall also support evolving VA automated security requirements such as open controls, security compliance masonry.

5.3.3 DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

The Contractor shall support Disaster Recovery (DR) of all MACM environments and apps hosted in the MACM environments and shall create and enact all procedures to support continuity of operations IAW all applicable VA handbooks and rules.

The Contractor shall:

a. Develop and implement a DR and Backup Plan for VA MACM, its environments, and hosted apps supplied using industry best practices which ensures no more than 15 minutes of service disruption and is fully compatible with and leverages the VAEC CSP Environment capabilities. The DR and Backup Plan shall include at a minimum:
    a. Organizational preparedness including roles, responsibilities, and contact information
    b. DR management and escalation processes including notification, declaration and testing guidelines, and notifications
    c. DR Test Schedule
b. Participate in disaster recovery test/exercises (scheduled and unscheduled simulations as well as real situations) and report the results in an After Action Report (AAR).
c. In order to minimize cloud services costs and optimize operations the Contractor shall utilize VAEC GSS services when available and applicable
d. Provide system details that includes a detailed representation of key infrastructure and networking configurations and requirements
e. Document failover and failback procedures that includes a step-by-step recovery and restoration process in the DR and Backup Plan
f. Collaborate in the design and implementation of a data backup solution and includes the analytics and identification of data sizes of all systems such as databases and hots, data retention, backup window/scheduling and archiving needs using results to create/update a design of a backup solution

g. Develop a Continuity of Operation (COOP) Plan

The Contractor's VA MACM SLA Report shall capture data as specified in the Deliverable Metrics/SLAs.

Deliverables:

A. DR and Backup Plan
B. DR Test Schedule
C. AAR
D. COOP Plan

DELIVERABLE METRICS/SLAs:

Data Recoverability Point Objective (Data RPO): In the event of a catastrophic failure there shall be no more than 15 minutes of data lost.

Data Recoverability Time Objective (Data RTO): In the event of a catastrophic failure it shall take no longer than 24 hours to recover the data.

Data Restoration: In the event of a catastrophic failure it shall take no longer than 24 hours to restore the data.

5.3.4 MONITORING AND ALERTING

The Contractor shall support VA requirements for monitoring VA MACM, using the VAEC supported monitoring tools and processes as they exist and evolve over time. Monitoring tools will include native CSP monitoring tools (See Attachment 003 for additional details). Additionally, the Contractor shall integrate all logs with appropriate monitoring tools such as Grafana, Prometheus, Splunk, and/or ElasticSearch. The Contractor shall create queries to support dashboards, reporting, and proactive alert generation based on system, operations, security and business needs.

The Contractor shall:

a. Create synthetic scripts to obtain real-life metrics and statistics and create dashboards, monitoring, API reporting, and proactive alerting based on synthetic script monitoring tools utilized.
b. Utilize monitoring plugins and agents to monitor numerical metrics provided by external services, servers, or equipment to collect more in-depth metrics.
c. Use Email, Short Message Service (SMS), and other methods, such as Pagerduty or VictorOps, for alerting schedules, escalation policies and services that escalate system, infrastructure, or security issues to a VA MACM on-call engineer. The Contractor shall acknowledge all alerts and remediate all issues IAW VA requirements
d. Establish and participate in monitoring of other VA upstream partner systems.
e. Assist application development teams to identify proper reporting metrics and alerts to isolate external decencies from internal services.
f. Provide assistance to internal and external teams to resolve issues during outages affecting external systems.
g. Provide an Application Response Time Monitoring Report, appended to the Monthly Status Report, that provides application response time frames at the 50th, 75th, 95th, and 99th percentiles.

DELIVERABLE METRICS/SLA:

Data Collection Monitoring: The Contractor shall collect data from all instrumented sources, with an aggregate frequency loss of no more than 300 seconds over a 24-hour period. An automated test, IAW the approved SLA Monitoring Plan, and the logged reports of execution including timing details of that test shall be provided in the VA MACM SLA Report.

5.3.4.1 COST AND COMPUTE OPTIMIZATION AND REPORTING FOR MOBILE CLOUD SYSTEMS

The Contractor shall review all usage of cloud computing services provided by VA. Plans shall be submitted and implemented quarterly on how to best optimize the environment to reduce the costs associated with resource utilization. The Contractor shall provide a breakdown of all costs by application, environment, and utilization and shall report on utilization of each class of resource as a percentage of provisioned capacity in a Monthly Utilization Report.

The Contractor shall, as part of its VA MACM SLA Report, include the total infrastructure expenditure and total number of request services for Cloud Resource Optimization.

Deliverables:

A. Quarterly Resource Utilization Optimization Plan
B. Monthly Utilization Report

5.3.5 SOFTWARE LICENSE MANAGEMENT (T&M)

The Contractor is responsible ~~at the direction of VA~~ to procure, manage, migrate, modify, and terminate ~~and procure~~ VA MACM software licenses required for its solution ~~for the benefit of VA~~. ~~These software licenses may include recurring costs and renewals which shall be the responsibility of the Contractor.~~ The Contractor shall coordinate with other contractors and vendors as necessary to support the ~~acquisition~~ procurement, management, migration, modification, and termination of the software licenses. Any licenses procured for the VA MACM solution shall be licenses for the benefit of VA. ~~The current manufacturer for each product is listed below; however different/equivalent brands are acceptable.~~ The ~~items listed~~software licenses may change over time and ~~items~~ may be substituted for more current versions, quantities, via modification to the contract. ~~All software licenses procured by the Contractor on behalf of VA in support of MACM shall be transferred to the Government at the end of the period of performance. The current software licenses procured for the VA MIS platform include:~~

The Contractor may choose to utilize for its solution existing licenses currently in use for the VA MIS platform or propose equivalent software licenses for its VA MACM solution. In the event the Contractor utilizes existing software licenses it will be responsible for recurring costs and renewals. Below is a list of software licenses currently utilized for the VA MIS platform.

a. Licenses for 2,000 users of Atlassian Jira and Confluence for collaboration, project and issue tracking in the VAMF enclave.
b. Licenses for 500 users of Atlassian Stash for supporting Git repositories in the VAMF enclave.
c. An unlimited user license of Atlassian Crowd for single sign-on to application lifecycle management (ALM) suite in the VAMF enclave.

d. Licenses for 100 users of Atlassian Fisheye and Crucible for code search, visualization and review in the VAMF enclave.
e. Licenses for the open source Jenkins software as a continuous integration tool in the MAE enclave.
f. Open source licenses for the development and production implementation instances of Drupal as a content management tool for the External App Store
g. Licenses for a systems monitoring tool for all Virtual Machines inside of all of the ECE/MAE/VAMF enclaves and associated environments.
h. Licenses for 100 users of the Sonatype Nexus Pro repository manager.
i. 14 Licenses for MongoDB Enterprise Advanced Subscription database system with 512GB RAM Server, unlimited users, 24x7x365 support w/30 minute SLA, Commercial License, MMS On- Prem, On-Demand Training, Advanced Security.
j. VA enterprise license agreement (ELA) for Fortify Static Code Analyzer (SCA) to perform static code analysis on all development products.
k. SmartBear LoadComplete, LoadTest and QAComplete test scripts, cases, and configurations
l. Open source Apache, NginX, NodeJS, and Java JDK/JRE

VA Enterprise License Agreements include:

a. RedHat Enterprise Linux
b. Microsoft Enterprise
c. Intersystems Cache
d. Oracle Weblogic
e. Oracle Database
f. Fortify SCA

All software licenses procured by the Contractor in support of VA MACM shall be transferred to the Government at the end of the period of performance.

5.3.6 ENGINEERING TECHNICAL SUPPORT

The Contractor shall provide the following:

a. Technical guidance to the product owner and development teams deploying apps. This shall include support using VA MACM and tooling provisioned by the Contractor
b. Support for integrating with external VA systems required for application operation
c. Support for utilizing shared services deployed internal to VA MACM
d. Access to logs and information from Build tools
e. Access to debug environments
f. Assistance in production access for troubleshooting
g. Providing support to product teams utilizing the CI/CD platform to deliver software to VA MACM.

DELIVERABLE METRIC/SLA:

Ticket Response: Tickets opened for this team for action related to the development environment receive a timely response. The 95th percentile of tickets has a response time less than minimum acceptable performance level which is one day. The calculated metrics shall be

provided VA MACM SLA Report, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary

Ticket Time to Close: Tickets opened for this team for action related to the development environment receive a timely resolution. The 95th percentile of tickets has a resolution time less than minimum acceptable performance level which is 3 days. The calculated metrics shall be provided in the VA MACM SLA Report, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

5.3.7 GENERAL ENGINEERING SUPPORT

The Contractor shall provide general engineering support to the app product owner and development teams deploying apps. This shall include:

a. Providing operational testing support including performance testing support and provide recommendations for performance enhancement in a Performance Enhancement Report appended to the Monthly Status Report.
b. Defining architectural changes as needed based on industry best practices.
c. Defining best practices and approach for utilizing/implementing the CI/CD platform.
d. Troubleshooting and resolving issues that arise within the CI/CD platform
e. Providing integration engineering support.

5.4 RELEASE AND DEVELOPMENT MANAGEMENT

5.4.1 CONFIGURATION MANAGEMENT

The Contractor shall manage and store all configuration items in the change management system.

5.4.2 CHANGE MANAGEMENT

The Contractor shall administer change requests according to the existing VA change management process. The Contractor shall schedule, communicate, and manage new or changed functionality into the MACM infrastructure. The Contractor shall facilitate the operating of the infrastructure Engineering Change Control Board (ECCB), by providing coordination, meeting planning, facilitation, collaboration facilities, and providing Technical SMEs to assist ECCB. Follow up meeting minutes with action items and decisions are maintained and delivered immediately with 24 hours to the stakeholders.

Deliverable:

A. Meeting Minutes

DELIVERABLE METRICS/SLAs:

Change Control Ticket Response: Tickets opened for this team for change control action receive a timely response. The 95th percentile of tickets has a response time less than the minimum acceptable performance level of one day. The calculated metrics shall be provided in the VA MACM SLA Report, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

Change Control Ticket Resolution: Tickets opened for this team for change control action receive a timely resolution. The 95th percentile of tickets has a resolution time less than the minimum acceptable performance level of 1 day. The calculated metrics shall be provided in the

VA MACM SLA Report, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

5.4.3 ENGINEERING CHANGE CONTROL BOARD (ECCB)

The Contractor shall support the ECCB for the VA MACM environments.

The Contractor shall establish a SOP including:

a. Submitting and reviewing a change request by the identified approval authorities.
b. Tracking the full lifecycles of the change request, and provide both regular and ad-hoc reports of duration in state, as well as absolute time and total count of all change requests.
c. Maintaining availability of historical change requests and provide access to the VA or designated individuals for review, and auditing purposes.
d. Establishing a process for change requests and associated implementations.
e. Establishing a regular cadence for board meetings.
f. Facilitating the board meeting and record and maintain minutes for all meetings.

Deliverables:

A. ECCB SOP

5.4.4 CHANGE CONTROL COMPOSITION

The Contractor shall create and maintain documentation on acceptable change policy as dictated by VA. Access to this shall be provided to any party which is required to submit change requests to the ECCB.

5.5 TIER 4 HELP DESK SUPPORT (OPTIONAL TASK) - LABOR- HOUR

The Contractor shall provide Tier 4 support on an as needed basis to the existing VA Mobile Help Desk to resolve all issues that are not resolvable by the Tier 3 VA Mobile Help Desk support team.

Tier 4 support shall include:

a. VAEC Cloud Infrastructure troubleshooting
b. Application troubleshooting
c. Assist other teams in resolving security issues such as access rights management
d. Capacity utilization, and configuration errors
e. Participating collaboratively with other VA staff and contractors to resolve platform, network and application issues.

DELIVERABLE METRICS/SLAs:

Development Trouble Ticket Response: Tickets opened for this team for action related to the development environment receive a timely response. The 95th percentile of tickets has a response time less than minimum acceptable performance level which is 1 day. A report of the calculated metrics shall be provided to the VA, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

Development Trouble Ticket Time to Close: Tickets opened for this team for action related to the development environment receive a timely response. The 95th percentile of tickets has a

response time less than minimum acceptable performance level which is 3 days. A report of the calculated metrics shall be provided to the VA, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

5.6 CONTRACT TRANSITION (OPTIONAL TASK)

The Contractor shall support the transition of essential knowledge and work products to and from other contractors as directed to VA to ensure the continuity of operations, its related components, and work flows.

5.6.1 TRANSITION-OUT PLAN

The Contractor shall prepare a Transition-Out Plan. The Contractor's plans shall define transition efforts to be conducted, documentation, and information to be transferred to and reviewed with other relevant contractors. Transition-Out Plan will be reviewed by and require approval of the VA Program Manager and COR prior to execution of any contract transition support optional task.

The Transition-Out Plan shall, at a minimum, address the following:

a. Transition schedule.
b. Phase-Out Migration Checklist (Contractor format).
c. Delivery of final deliverables; artifacts; VA MACM documentation, including VA MACM Standard Operating Procedures (SOP), Tooling Support Plan, and Developers Guide; and lessons learned.
d. Delivery of software, release/code versions, processes, artifacts, and documents supporting each task area of the PWS in a format that is usable by VA.
e. Outputs of automated test results and pass/fail results.
f. Delivery of performance, security, and browser testing results.
g. Training of relevant Government and Contractor personnel.
h. Communication on, and delivery of, security concerns such as badges, tokens, and accounts,
i. Plan for ensuring that, prior to termination or completion of this effort, the Contractor/Subcontractor does not destroy any information in any form received from VA, or gathered/created by the Contractor in the course of performing this effort without prior written approval by VA PM/COR. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done IAW National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitation.
j. An orientation phase to introduce the successor Cloud Services Provider personnel, programs, and users to the incumbent team, explaining tools, methodologies, and business processes.
k. Providing signed transition agreements in the VA designated format.

The Contractor shall archive all final documentation and materials in a secure location as directed by the VA COR.

Deliverables:

A. Transition-Out Plan

5.6.2 TRANSITION-OUT SERVICES

In accordance with the Government-approved transition-out plan, the Contractor shall assist the Government in implementing a complete transition from this contract to a new support provider. This shall include formal coordination with Government staff as well as successor staff and management. The Contractor shall also include delivery of copies of all VA MACM artifacts, software licenses, existing policies and procedures, data, source code, baseline metrics and statistics, and any additional VA MACM documentation or information.

Successful transition is defined as 100% completion of all work defined in the Government-approved Transition-Out Plan.

Upon the completion of the transition period, the Contractor shall provide closeout certifications that include a statement that the contract is complete, all deliverables have been provided, all services are complete, and there are no outstanding contractual issues.

Deliverables:

A. Closeout Certifications

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 ONE-VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. 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 the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

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

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at:
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf,
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

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

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's MVI to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems. https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846

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

6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (https://www.nist.gov/programs-projects/usgv6-technical-basis-next-generation-internet), the Technical Infrastructure for USGv6 Adoption (http://www-x.antd.nist.gov/usgv6/index.html), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack (IPv6/ IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

6.1.5 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 365 ProPlus and Windows 10. However, Office 365 ProPlus and Windows 10 are not the VA standard yet and are currently approved for limited use during their rollout, we are in-process of this rollout and making them the standard by OI&T. Upon the release approval of Office 365 ProPlus and Windows 10 individually as the VA standard, Office 365 ProPlus and Windows 10 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP)

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products

6.1.7 PROCESS ASSETT LIBRARY (PAL)

The Contractor shall utilize PAL, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles,

artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

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

Contractor Responsibilities:

- 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.
- The Contractor shall bear the expense of obtaining background investigations.
- 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 ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
- The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
  - Optional Form 306
  - Self-Certification of Continuous Service
  - VA Form 0710
  - Completed Security and Investigations Center (SIC) Fingerprint Request Form
- The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
- The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).

- 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.
- 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), training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." 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 the Office of Personnel Management (OPM).
- 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.
- 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.
- Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

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

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.

Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

b. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.

c. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed SIC Fingerprint Request Form

The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).

d. 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.

e. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's

network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.

f. 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.

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.

Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort. The Deliverable Metrics/Service Level Agreements (SLA) as described in the Performance Work Statement (PWS) are separate from the below Performance Standards, but the Contractor's performance in meeting the SLAs will impact the level of performance rating achieved for each performance objective set forth in the table below.

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

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.4.1 DELIVERABLE METRICS/SERVICE LEVEL AGREEMENTS PERFORMANCE

The Contractor shall meet the required Deliverable Metric/SLA as described in the Performance Work Statement (PWS). However, if the Contractor's performance falls below a required service level, the Contractor shall only be paid for the lower service level provided. Please be advised that the VA's payment for the lower service level provided in no way waives the Government's right to pursue any remedies available by law, including, but not limited to, termination for breach of contract. Please be further advised that failure to meet the Deliverable Metrics/Service Level Agreements as set forth in this PWS shall be considered a condition endangering contract performance and may provide grounds for default termination. The Government will conduct a monthly review of the defined SLAs against the Contractor's performance/solution. If a lower service level is assessed in a particular month, the Contractor shall provide an itemized invoice detailing the lower service level price (percentage and amount) and deducting that lower service level price from the total monthly price of the applicable Contract Line Item Number in the following month's invoice. The Contractor will not be faulted for lower service levels that occur due to external circumstances beyond the Contractor's control.

For any PWS task in which there are multiple SLAs, payment will be calculated for the lowest service level provided. Furthermore, each metric stands alone, therefore, if a single event impacts multiple SLAs across PWS Tasks, the Contractor shall be paid for lower service provided to both tasks.

SLAs are set forth in PWS Firm-Fixed-Price tasks 5.3.1, 5.3.3, 5.3.4, 5.3.6, and 5.4.2. The following table provides the calculation and measurement of each Firm-Fixed-Price (FFP) Deliverable Metric/SLA specified. Measurement of Deliverable Metrics/SLAs shall begin 30 days after Government acceptance of the VA MACM MVP.

SLA ID	PWS Task	SLA	SLA Metric	Percentage of FFP monthly payment by the Government
1	5.3.1	System Availability	Aggregate uptime for all MACM components no less than 99.9%.	100% of FFP payment
			Aggregate uptime for all MACM components between 99.8% and 99.5%.	90% of FFP payment
			Aggregate uptime for all MACM components between 99.4% and 99.1%.	80% of FFP payment
			Aggregate uptime for all MACM components at and below 99.0%.	70% of FFP Payment
2	5.3.1	Development Environment Availability	Availability no less than 99.9%.	100% of FFP payment
			Availability between 99.8% and 99.5%	90% of FFP payment
			Availability between 99.4% and 99.1%	80% of FFP payment
			Availability at and below 99.0%.	70% of FFP Payment
3	5.3.1	Service Availability	Availability no less than 99.9%.	100% of FFP payment
			Availability between 99.8% and 99.5%	90% of FFP payment
			Availability between 99.4% and 99.1%	80% of FFP payment
			Availability at and below 90.0%.	70% of FFP Payment
4	5.3.1	Service Uptime	Services remain online no less than 99.9% of the time.	100% of FFP payment
			Services remain online between 99.8% and 99.5% of the time.	90% of FFP payment
			Services remain online between 99.4% and 99.1% of the time.	80% of FFP payment
			Services remain online below at and below 90.0% of the time.	70% of FFP Payment
5	5.3.1	Service Reachability	Services reachable by outside entities no less than 99.9% of the time.	100% of FFP payment
			Services reachable by outside entities between 99.8% and 99.5% of the time.	90% of FFP payment

			Services reachable by outside entities between 99.4% and 99.1% of the time.	80% of FFP payment
			Services reachable by outside entities at and below 90.0% of the time.	70% of FFP Payment
6	5.3.3	Data Recoverability Point Objective	No more than 15 minutes of data lost.	100% of FFP payment
			No more than 20 minutes of data lost.	90% of FFP payment
			No more than 25 minutes of data lost.	80% of FFP payment
			No more than 30 minutes of data lost.	70% of FFP Payment
7	5.3.3	Data Recoverability Time Objective	No longer than 24 hours to recover data.	100% of FFP payment
			No longer than 30 hours to recover data.	90% of FFP payment
			No longer than 36 hours to recover data.	80% of FFP payment
			No longer than 48 hours to recover data.	70% of FFP Payment
8	5.3.3	Data Restoration	No longer than 24 hours to restore data.	100% of FFP payment
			No longer than 30 hours to restore data.	90% of FFP payment
			No longer than 36 hours to restore data.	80% of FFP payment
			No longer than 48 hours to restore data.	70% of FFP Payment
9	5.3.4	Data Collection Monitoring	Average frequency loss of no more than 300 seconds per day.	100% of FFP payment
			Average frequency loss between 301 and 360 seconds per day.	90% of FFP payment
			Average frequency loss between 361 and 420 seconds per day.	80% of FFP payment
			Average frequency loss more than 421 seconds per day.	70% of FFP Payment
10	5.3.6	Ticket Response	No less than 95% of tickets have a response time of less than one day.	100% of FFP payment
			Between 94% and 92% of tickets have a response time of less than one day.	90% of FFP payment
			Between 91% and 90% of tickets have a response time of less than one day.	80% of FFP payment
			Below 90% of tickets have a response time of less than one day.	70% of FFP Payment
11	5.3.6	Ticket Time to Close	No less than 95% of tickets have a response time of less than three days.	100% of FFP payment
			Between 94% and 90% of tickets have a response time of less than three days.	90% of FFP payment

			Between 89% and 85% of tickets have a response time of less than three days.	80% of FFP payment
			Below 85% of tickets have a response time of less than three days.	70% of FFP Payment
12	5.4.2	Change Control Ticket Response	No less than 95% of tickets have a response time of less than one day.	100% of FFP payment
			Between 94% and 92% of tickets have a response time of less than one day.	90% of FFP payment
			Between 91% and 90% of tickets have a response time of less than one day.	80% of FFP payment
			Below 90% of tickets have a response time of less than one day.	70% of FFP Payment
13	5.4.2	Change Control Ticket Resolution	No less than 95% of tickets have a resolution time of less than one day.	100% of FFP payment
			Between 94% and 90% of tickets have a resolution time of less than one day.	90% of FFP payment
			Between 89% and 85% of tickets have a r resolution time of less than one day.	80% of FFP payment
			Below 85% of tickets have a resolution time of less than one day.	70% of FFP Payment

6.5 FACILITY/RESOURCE PROVISIONS

6.6 GOVERNMENT FURNISHED PROPERTY

The Government will provide cloud credits to the VAEC-AWS environment.

The VA Program Manager (PM) will provide the following Government Furnished Items (GFI) for performance of this contract:

a) Project data for mobile applications projects and for the data center
b) VA-owned software for App Stores and App catalog products
c) Access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG))
d) VA Enterprise License Agreements
    a. RedHat Enterprise Linux
    b. Microsoft Enterprise
    c. Intersystems Cache
    d. Oracle Weblogic
    e. Oracle Database
    f. Fortify SCA