TRANSFORMATION TWENTY-ONE TOTAL TECHNOLOGY NEXT GENERATION (T4NG)
PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Mobile Technology and Endpoint Security Engineering

VA Enterprise Mobility Management

Date: May 17, 2018
TAC-18-49377
Task Order PWS Version Number: 16.0

Contents

1.0 BACKGROUND

The Department of Veterans Affairs (VA) has a need for a secure cloud-based Enterprise Mobility Management (EMM) system. The purpose of having a single provider of a cloud-based ‘out-of-the-box’ Software as a Service (SaaS) implementation is to reduce implementation complexity as well as future upgrade complications. This also will enable consolidation and automation of EMM processes, increase efficiencies, lower costs, and provide the ability to devote more time to innovation and creation of customer-focused solutions. The cloud-based tool should improve business performance by providing VA end users with expanded and new capabilities that reflect industry standards.

The SaaS EMM solution under this Performance Work Statement (PWS) will satisfy the requirement of having a fully managed out-of-the-box EMM system, including all turnkey operations and Tier 4 support.

VA currently runs an EMM system for management of mobile devices hosted at IBM Terremark in the VA’s private cloud environment in a Federal Information Security Management Act (FISMA) High environment. The EMM implementation consists of two separate environments. One is a User Acceptance Testing (UAT) environment where software patches, changes and code review occurs, and the second is the Production environment. VA is planning to migrate to a Federal Risk and Authorization Management Program (FedRAMP) Moderate environment as VA’s requirements have shifted. The EMM environment currently includes the on-premise version of VMware AirWatch 9.1.4 (Yellow Suite) software to manage devices as well as an internal Application (App) Store. The environment contains 45,000 AirWatch licenses with approximately 45,000 devices (iOS, Windows mobile, and Android phones and tablets) currently enrolled. The current environment consists of 45 Virtual Servers with a mix of Windows Server 2008 R2 and Red Hat Enterprise Linux (RHEL) 6 / Cent OS. The total capacity is 325 Gigahertz (GHz) processor, 660,800 Megabyte (MB) random access memory (RAM), and 20,000 gigabyte (GB) storage. VA is currently testing a certificate based authentication based on National Institute of Standards and Technology (NIST) 800-157 and AirWatch Derived Personal Identity Verification (PIV-D). The PIV-D system uses VA’s active directory system today as VA migrates to a new Certificate Management System and will use that in the future.

VA requires a fully migrated and operational VA EMM system by September 12, 2018. This shall be at a new Contractor-provided location that is fully functional. VA will allow the incoming Contractor to continue operation of the current environment for up to three months after September 12, 2018 to allow for a longer transition to the new SaaS.

2.0 APPLICABLE DOCUMENTS

The Contractor shall comply with the following documents, in addition to the documents in Paragraph 2.0 in the T4NG Basic PWS, in the performance of this effort:

1. VA, Office of Information and Technology (OI&T), Corporate Data Center Operations (CDCO), Austin Information Technology Center (AITC), Handbook 6500.02, “Computer and Network Security Incident Response”, 2012
2. VA, OI&T, Service Delivery and Engineering (SDE), “VA Enterprise Disaster Recovery Service Tiers and Technology Solutions Standards”, Version 1.0, September 2012.
3. VA, OI&T, Office of Cyber Security (OCS), “VA Authority to Operate Requirements”, April 2013
4. Office of Management & Budget (OMB) Memorandum M-12-20, “FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” October 2, 2012
5. VA Directive 6517, Cloud Computing Services, February 28, 2012
6. FedRAMP, “FedRAMP Standard Contractual Clauses”, June 2012
7. NIST Special Publication 800-145, NIST Definition of Cloud Computing, September 2011
8. NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, May 2012
9. Security Content Automation Protocol (SCAP) automation capabilities (see NIST SP 800-126, “The Technical Specification for the SCAP”, Version 1.2 September 2011.)
10. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
11. Attachment 1, Cloud Computing Service Level Agreement (SLA)
12. Attachment 2, Chapter One: Cloud Computing Security Requirements Baseline
13. Attachment 3, Authorization Requirements Standard Operating Procedures

3.0 SCOPE OF WORK

The Contractor shall provide a managed solution for a cloud hosted out-of-the-box EMM SaaS solution for all VA-issued mobile devices including iOS, Windows mobile, and Android phones and tablets. The managed solution shall include all hosting, software, hardware, and operations and maintenance (O&M) required to create and maintain an operational VA EMM system as described in this PWS. The Contractor can assume turnkey operations of the current environment while planning the move to an alternate FedRAMP Moderate environment. Upon time of the Government’s agreement, the Contractor shall move the system from the current environment to the Contractor’s proposed environment. The Contractor shall migrate device data and any required technical operating structures from the current hosted environment (IBM/Terremark) to the new hosted location as required to support uninterrupted service. The Contractor shall also move all documentation and Assessment and Authorization (A&A) materials from the current environment to a new repository that the Contractor shall manage for the duration of the Task Order (TO). Once the move to the new cloud is complete, the Contractor shall provide O&M for the turnkey operations of the application and all systems. The Contractor shall provide training and maintain standard operating procedures for all devices and operating systems managed under the solution.

The Contractor shall ensure that the system uptime meets the SLAs as dictated in Attachment 1.

The EMM system shall be hosted in a FedRAMP Moderate approved private cloud supporting mobile device management software for 45,000 devices scaling up to 100,000 devices by the end of the Period of Performance (PoP). The solution shall include an internal App Store.

The Contractor shall be responsible for the migration of all 45,000 devices and provide direct user support (via phone) to each user to meet the necessary migration deadlines. This includes removing the current solution and provisioning the new solution for all 45,000 devices.

The Contractor shall provide a working certificate-based authentication solution, a working EMM based email solution which connects to VA's Office 365 instance, a working application threat monitoring solution, and a working application vetting solution as part of the total EMM solution.

3.1 APPLICABILITY

This TO effort PWS is within the scope of paragraph(s) 4.2.4 Enterprise Application/Services, 4.2.5 Cloud Computing, 4.2.13, Current System and Data Migration, 4.8 Operations and Maintenance, 4.9 Cyber Security, and 4.10 Training of the T4NG Basic PWS.

3.2 ORDER TYPE

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

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The PoP shall be 12 months from date of award, with four 12-month option periods inclusive of optional tasks described below.

4.2 PLACE OF PERFORMANCE

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

4.3 TRAVEL OR SPECIAL REQUIREMENTS

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. Include all estimated travel costs in your FFP line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program-related meetings for this effort is four per year. Anticipated locations include the following, estimated at three days in duration:

1. Hines, IL
2. Washington, DC

4.4 CONTRACT MANAGEMENT

All requirements of Sections 7.0 and 8.0 of the T4NG Basic PWS apply to this effort. This TO shall be addressed in the Contractor's Progress, Status and Management Report as set forth in the T4NG Basic contract.

4.5 GOVERNMENT FURNISHED PROPERTY

Note: the Government will not provide any laptop computers for this TO.

The VA Program Manager (PM) will provide the following Government furnished items for performance of this TO:

1. Existing EMM infrastructure documentation.
2. Access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), Agiliance RiskVision).
3. AirWatch licenses provided as part of VA Enterprise License Agreement (ELA).

4.5.1 CONTRACTOR ACQUIRED EQUIPMENT

The Contractor shall perform the following for the purchase of up to 30 laptops throughout the period of performance of the TO.

If the Contractor requires access to the VA network via VPN, the Contractor shall procure laptops that meet VA requirements and submit them to VA for the "Gold" image for Windows.

Prior to any purchases, the Contractor shall coordinate with the COR in order to determine which devices are approved for VA requirements for imaging. At the conclusion of the PoP, the laptops shall be returned to VA as VA-owned equipment through the COR. This task requires approval by VA COR prior to purchase.

The Contractor shall provide documentation to include the final purchase order and invoices for each purchase to the COR, the VA PM, VA CO/Contract Specialist and their assigned technical representatives.

The Contractor shall include a quarterly summary of purchases to date and balance remaining according to Section B in the Contractor’s Progress, Status and Management Report.

4.6 SECURITY AND PRIVACY

All requirements in Section 6.0 of the T4NG Basic PWS apply to this effort. Specific TO requirements relating to Addendum B, Section B4.0 paragraphs j and k supersede the corresponding T4NG Basic PWS paragraphs, and are as follows:

j. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.

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

4.6.1 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	□	□	☒
5.7	□	☒	□
5.8	☒	□	□
5.9	□	□	☒
5.10	□	□	☒
5.11	□	□	☒
5.12	☒	□	□
5.13	□	□	☒

5.14	☒	□	□
5.15	□	☒	□
5.16	□	□	☒

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. These requirements refer to task numbers, but also to all staff working on items related to the correlating environments for task numbers.

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 this TO effort. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the TO. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 TECHNICAL KICKOFF MEETING

The Contractor shall conduct a technical kickoff meeting with the VA PM, Contracting Officer’s Representative (COR) and the Contracting Officer (CO). The meeting shall be held within ten calendar days after TO award. The kickoff meeting shall be a face-to-face meeting in a VA or VA-approved Contractor facility lasting for three full business days. 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 kickoff meeting. The kickoff meeting shall address post award topics and shall present the Contractor’s draft plans and approach for meeting PWS requirements to include:

1. Detailed review of the CPMP. The VA PM/COR will provide detailed comments on the CPMP, which shall be incorporated in the operational CPMP. The CPMP shall be updated based on input provided at this meeting.

2. Detailed reviews of the Contractor's draft Test, Implementation, Transition Plans and Migration Procedures for both UAT and Production EMM environments.

3. Detailed list of staff that will be working each of the different deliverables along with status of their background investigation/VA clearance and biographies in an initial Personnel Contractor Manpower Report.

5.1.3 CONTRACTOR STAFFING PLAN AND STAFFING MANAGEMENT

The Contractor shall provide project management support for day-to-day operations and activities for the scope of this entire TO. This project management support shall provide a sole point of contact on all tasks related to EMM operations as well as migration of the solution and all user devices, cloud hosting, supporting hardware, operating system and software infrastructure. Project management support shall identify and respond to issues relating to EMM operations on a daily basis.

The Contractor shall be responsible for the entire VA EMM SaaS solution and integration pieces. The Contractor shall provide a Staffing Plan that ensures its successful management of any subcontractors or cloud providers, including all software, hardware and network components comprising the solution.

The Contractor shall provide a Staffing Plan to ensure established staffing levels are maintained on each task, monitor performance, and report any deviations. The Contractor shall also include staff loss/gains in the CPMP, as well as a staffing schedule for the upcoming month. The Contractor shall provide a Staffing Plan, to include project organization chart, project team roles, project responsibilities, number of staff required per assignment, estimated start dates, breakdown in terms of staff's Full Time Equivalent (FTE) for each role, contact information for all TO participants, and identification of key risk points and mitigation plans. The Staffing Plan shall be included in the Monthly CPMP.

The Contractor's staffing approach shall comply with VA 6500 guidelines around separation of duties and least privileges. The Contractor shall ensure adequate coverage for implementation and O&M to support all environments in compliance with VA 6500's guidelines around separation of duties and least privilege. The Contractor shall ensure consistent coverage for all support requirements including backup staffing that is readily available. The Contractor shall use VA's implementation of Service Now for all server interruptions, user support, information technology (IT) support, and any other service type tickets.

The Contractor shall:

1. Ensure staffing levels provide non-interrupted support 24 hours a day, seven days a week, and 365 days a year during emergencies or staffing issues.
2. Ensure Contractor staff is trained and oriented on EMM Support Service processes within two weeks of being assigned.
3. Ensure Contractor skill sets are maintained as required to support current technology platforms included in the EMM solution.
4. Notify the COR in writing by email of any staff changes on work associated with this TO 10 business days in advance of any staff change. The written notification shall outline the reason for the change, the impact expected by the change and mitigation strategy to reduce the impact by the staff change.

5.1.4 WEEKLY STATUS UPDATE

The Contractor shall support weekly status meetings as required to discuss status, issues, proposed resolutions, plan moves/add/changes, plan upgrades, and resolve tickets. These meetings can be conducted via teleconference.

5.1.5 CONTRACT TRANSITION: PHASE-IN

The Contractor shall support transition activities including phase-in services to ensure continuity of services. The Contractor shall provide migration services for the data being migrated from the current solution to the Contractor’s proposed EMM solution environments.

The Contractor shall deliver phase-in services as described below:

1. **Initial Phase-In.** The Contractor shall collaborate with VA personnel (Government and Contractor) and the current VA EMM Contractor and their cloud service provider to accomplish a seamless migration of all EMM devices, and system and user information in the existing environment(s) to the new EMM solution. During transition, the Contractor shall maintain VA’s current implementation. If devices must be re-enrolled, the Contractor shall provide a special Tier 1 staffed help desk available 8 a.m. Eastern Standard Time (EST) to 8 p.m. EST, seven days a week during the transition to work with VA staff to migrate their device(s) to the new EMM. This help desk shall facilitate and support all VA locations with completing the un-enrollment from the current VMware AirWatch EMM infrastructure to the new VMware AirWatch EMM infrastructure (if VA name space matching cannot be provided) and provide support to re-enroll all devices to the proposed EMM system, as required. Migration of all devices to a new EMM is estimated to be approximately 45,000 hours.

   The Contractor shall ensure that full turnkey operations ensue on the current system no later than September 12, 2018, while the Contractor plans a migration to the new EMM solution and cloud environment. The Contractor shall provide a

Migration Plan that includes detailed instructions to transition from the current EMM environment to the new environment. The Contractor shall ensure that all configurations are coordinated with VA, the current VA EMM Contractor and their cloud provider to ensure no interruption of services.

2. **Phase-In Plan:** A Phase-In Plan shall be created detailing the Contractor's roles and responsibilities in this process. The Phase-In Plan shall address the following areas:

    a. Procedures to migrate VA data, infrastructure and other information required for seamless migration from the existing EMM implementation to the new EMM solution being provided by the Contractor. This migration plan must be acceptable to the Government.
    b. Procedures to introduce VA Staff to the Contractor's tools, methodologies, and business processes (and how they will differ from existing procedures).
    c. Basic training on call directing and ticket routing guidelines for VA National Service Desk personnel.
    d. Basic training on contact information and Tier 4 Help Desk scripts for EMM.
    e. Information related to the Contractor's strategy, timeline, and planned approach for personnel staffing and training during the migration period. This includes reference material (including any on-line help) that describes how to use any tools or dashboards.
    f. An overall phase-in migration timeline including VA activities.
    g. The Contractor's Phase-In Migration Checklist identifying migration tasks and timelines.
    h. If current devices must be re-enrolled, procedures to migrate all current VA mobile devices from enrollment from the current AirWatch EMM to the proposed EMM. The procedures should cover the detailed steps required of VA and of the Contractor for un-enrollment of the current EMM product on every existing device and re-enrollment into the proposed EMM as well as reinstatement of VA-critical apps.
    i. Procedures to migrate/recreate all server settings, user profiles, user permissions, system administration permissions, communication channel, compliance settings, and console settings from the current EMM environment to the new EMM environment.
    j. Procedures for re-training VA staff and contractors.

Deliverables:

A. Migration Plan
B. Phase-In Plan including Migration Checklist

5.2 CURRENT EMM MANAGED SOLUTION

The current EMM managed solution is hosted at an IBM Terremark data center (refer to Section 1.0 Background for additional details). The Contractor can assume ownership from the previous vendor of the cloud-based EMM solution in the IBM Terremark data center while planning the move to host the EMM elsewhere. Regardless of how the Contractor chooses to provide the EMM solution, the Contractor shall provide a fully operational turnkey solution that meets all of the EMM requirements in this PWS by September 12, 2018. Within three months from September 12, 2018, the Contractor shall migrate to a fully operational SaaS environment.

5.3 EMM MANAGED SOLUTION

The Contractor shall deliver and host a cloud-based EMM solution as a full turnkey solution including all hardware, software, certificates, hosting, installation services, operations, maintenance and full system documentation along with resources and staff to run and administer the system including Tier 4 help desk support.

The Contractor shall provide hosting, software licenses and associated maintenance required to support the EMM requirements outlined below. With the exception of AirWatch licenses described in PWS paragraph 4.5, all licenses proposed in support of the EMM requirements shall require procurement, installation, renewal and maintenance during the PoP to ensure uninterrupted service. AirWatch licenses will be provided by VA via the ELA; the Contractor shall install and maintain ELA licenses required in support of the EMM solution.

The EMM solution shall be hosted in a FISMA Moderate private cloud where there shall be full interconnectivity back and forth to VA systems for an EMM solution. The Contractor shall consider that if any proposed Cloud Service Providers have access to the Equinix Cloud Exchange (ECX) or is operating out of Azure Public, Azure Federal Private, or Amazon Web Services then infrastructure is already available for rapid provisioning. Otherwise, the Contractor shall be responsible for creating and establishing connectivity to VA.

The Contractor shall support an internal App Store, using AirWatch, for mobile applications to be used by enrolled devices, which is internal to VA only. This internal App Store is currently hosted by VA's current EMM provider AirWatch. The EMM solution currently delivers a native mail experience through an Email Gateway like system; the new EMM solution shall provide the same functionality to support Mobile Email Management with gatekeeping to VA's Microsoft Exchange environment. Currently, VA is on a hybrid Exchange 2010/Office 365 infrastructure. The future email system will be Office 365, and the Contractor shall provide the resources and staff required to configure and connect the new EMM to function correctly with Office 365. The Email system shall support VA's PIV-only authentication requirement. User accounts are locked down to require certificate-based authentication. Username and password is not available for authorization of any accounts. The Contractor shall provide a solution to VA that functions correctly under these parameters. The solution must meet all existing Trusted Internet Connection (TIC) 2.0 requirements. All traffic must traverse through the TIC and cannot be directly accessible from the internet without first passing through the TIC.

5.3.1 EMM FUNCTIONALITY

The Contractor shall provide an EMM solution that meets the technical and functional capabilities specified in Appendix A: EMM Capabilities. The EMM shall provide functionality to support VA's mobile environment and shall include enterprise mobility management, internal mobile app catalog, email functionality, a secure content solution, secure browsing and a secure workplace (dual persona) environment. Additionally, the EMM shall fully support application threat applications. The EMM shall also provide full certificate-based authentication functionality as detailed in this PWS.

The Contractor's solution shall provide the required high level functionality listed below which are further detailed in Appendix A and throughout the PWS:

1. Provisioning: ability to enroll a device in EMM and initially secure that device.
2. Security: ability to secure the mobile environment.
3. Profile: ability to create, edit, push and manage profiles.
4. Management: ability to search devices, review histories, track device changes.
5. Compliance: ability to set up compliance rules as well as activate/deactivate rules and wipe compromised devices.
6. Alerts: to let users know they are out of compliance or have a compromised device.
7. Reporting: to enable administrators to check device compliance with VA policies and profiles.
8. Mobile App Deployment: a mechanism for VA to distribute internal custom applications.
9. Operational Efficiency: features and functions to further secure the devices and help VA effectively manage the environment.
10. Email Integration: to provide email filtering and routing to provide secure email communication to VA devices.
11. Integration with the Contractor-provided mobile application threat system
12. Full integration with the Contractor-provided certificate based authentication system.
13. User and admin log on using VA Active Directory, including two factor authentication

The Contractor shall implement and maintain the following environments within the EMM solution:

1. **User Acceptance Testing (UAT):** This is the EMM's UAT environment which is used as a production copied test environment for the entire EMM environment testing, as well as device and product testing. This environment is used by VA to contain only those development/testing resources needed to verify proper functioning software within this environment. This environment mirrors the

Production environment exactly and is used to test potential changes to the Production environment. The UAT environment is solely for the Contractor and engineering staff to test out functionality and compatibility of features and patches.

2. **Production (Prod)**: This is the production EMM environment currently running AirWatch 9.1.4 which is currently managing approximately 45,000 devices.

5.3.1.1 EMM INTERNAL APP CATALOG

The Contractor shall deliver and implement, as part of the EMM solution, an internal, VA staff-facing App catalog. This internal staff-facing App catalog shall deliver commercial off-the-shelf (COTS) and custom VA apps to mobile devices managed using the EMM software solution over the air (OTA) including iOS, Android, Windows, and Blackberry.

The App catalog shall be hosted in the EMM cloud environment. The App catalog shall be accessible by VA and shall be for the sole, private use of VA. This App catalog shall meet the App catalog technical and functional requirements as specified in the Mobile App Deployment section of Appendix A: EMM Capabilities.

The VA internal staff-facing App catalog shall allow the EMM users to download VA Enterprise Apps, as well as provide a pass-through for accepted commercial Apps. The Contractor shall provide App catalog support to streamline App downloading capabilities to approximate commercial download speeds. The Contractor shall migrate management responsibilities for the current App catalog to the new App catalog.

5.3.2 EMM TECHNICAL ENVIRONMENT

The EMM solution shall, upon initial delivery, support 45,000 mobile devices concurrently, with capabilities of supporting up to 100,000 concurrent devices, while maintaining compliance with all technical and functional requirements and maintaining 99.9% availability.

The Contractor shall ensure the EMM solution provides capacity, software, hardware, licenses, certificates and all other infrastructure required to support the usage, technical and functional requirements for an initial load of 45,000 EMM licenses and approximately 45,000 devices with anticipated growth over the five year period to support up to 100,000 devices in total. In addition to this, the Contractor shall deliver flexible, scalable processing, memory, support staff, and storage capacity necessary for the operation of each project/initiative environment in the Cloud that provides a reconfigurable technical foundation. Any solution provided by the Contractor shall meet the SLA parameters as defined in Attachment 1.

The Contractor shall provide the following functionality:

1. The ability to provide persistent, high availability, high performance storage for the EMM environments with a warm disaster recovery site.

2. The ability to provide adequate flexibility for increasing resources to support a growing number of mobile devices and administrators.
3. The ability to provide tiered backup and recovery for information stored on the cloud storage infrastructure to meet the related SLA in Attachment 1.
4. The ability to provide all retrieved data in the original or other VA agreed-upon format, including all original meta-data.

The EMM environment shall provide capacity and uptime required to meet the SLAs as detailed in Attachment 1. Capacity required for any Contractor-defined approaches to meeting security requirements, Active Directory integration, System Monitoring, or other requirements shall be provided by the Contractor with no impact to capacity allocated to VA.

<u>Cloud Hosting:</u>
The EMM shall be hosted in a cloud that meets FISMA Moderate and FedRAMP Moderate requirements for standardized security controls and assessments of cloud products and services.

The EMM environment shall be fully managed by the Contractor as a turnkey operation, and provide uptime required by the SLAs. Additionally, the Contractor shall stand up whatever is required to fully integrate back to the VA environment.

<u>Certificates:</u>
The Contractor shall supply and install VA-approved and compatible certificates for the entire EMM solution including all environments. The Contractor shall provide either individual or wildcard certificates to meet VA requirements, as needed. The certificates must be backwards and forwards compatible with all systems and devices required by VA.

5.3.3 EMM CONNECTIVITY TO VA NETWORK

Communication between the cloud hosted EMM solution and VA is currently done through a firewall port opening with the VA Business Partner Extranet (BPE) connection. The EMM environment contains Personally Identifiable Information (PII), but no Protected Health Information (PHI) is permitted.

The Contractor shall coordinate with VA Service Delivery and the VA Network and Security Operations Center (NSOC) to establish this secure Virtual Private Network (VPN) and shall be responsible for establishing and monitoring connectivity. The Contractor shall communicate to the VA PM/COR all necessary ports, protocols and Internet Protocol (IP) addresses required for successful EMM operation to ensure that the necessary ports and protocols will be opened after an internal security review. The Contractor shall provide a closed network at the location of the solution. All equipment used in support of the solution must be dedicated to VA use only. The EMM shall connect to the Internal Business Partner Extranet (iBPE) at the VA TIC gateways. VA will retain responsibility for all Wide Area Network (WAN) activity capacity and management. The Contractor shall be responsible for providing support in transitioning and testing the circuit transition, as well as troubleshooting connectivity issues. Furthermore, the Contractor shall provide the following capabilities:

1. The ability to provide network connectivity that complies with Federal Information Processing Standards (FIPS) 140-2, Section 1, Table 1, up to and including Security Level 2. The ability to provide a redundant, secure encrypted network solution that provides connectivity between a primary and secondary site. This network solution shall meet the requirements of the applicable SLAs outlined in Attachment 1. The ability to provide network connectivity to VA-provided circuits that use point-to point Internet Protocol Security (IPsec) Tunnels, with initial bandwidth of 10 Gigabits per second (Gbps). VA will provide EMM access for communication to other VA business partners and mission oriented Internet based services through the VA TIC. The Government anticipates the entry into the EMM to be a physically diverse path to mitigate any risk of a localized event disrupting communications. The Contractor shall provide two 10 Gbps connections to the WAN, through the VA Gateway TIC via BPE.
2. The ability to provide dedicated firewalls and load balancers.
3. The ability to provide public, private and VA private IP addresses reserved and assigned to enable interaction between internal and external VA systems (e.g., National Archives and Records Administration (NARA) and other VA applications).
4. The ability to support IP version 6 (IPv6) as well as IP version 4 (IPv4). The Contractor's solution shall support the latest IPv6 based upon the directive issued by the OMB on September 28, 2010 (https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/transition-to-ipv6.pdf). NIST SP 800 series applicable compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration.
5. The ability to provide Network Configuration Diagrams for both primary and secondary sites for the EMM cloud environment which detail all aspects of the Network Configuration.
6. The ability to route all outbound and inbound traffic to/from the EMM environment to the VA Enterprise through the VA TIC. The EMM environment shall connect only to the VA network.
7. The Contractor shall provide support to VA for additional software/dashboards (i.e. connectivity to ServiceNow and VA command center dashboards). The Contractor shall work with VA entities to support the data interaction between the EMM product and VA tools.

The Contractor shall be responsible for the creation and follow-up of all Enterprise Security Change Control Board (ESCCB) tickets for the management of network ports and IP ranges through VA's NSOC and BPE teams. The tickets shall have accurate and up-to-date information. The Contractor shall also be responsible for updating tickets in a timely fashion if more information is required. The Contractor shall attend all implementation calls of ESCCB tickets with the BPE and Gateway teams.

5.3.4 MONITORING

The Contractor shall deliver and support automated monitoring, collection of pertinent data for trending information, and reporting to ensure all aspects of the EMM solution are operating within the SLA parameters outlined in Attachment 1.

The Contractor shall ensure automated monitoring provides the following:

1. Security Content Automation Protocol (SCAP) automation capabilities (see NIST SP 800-126, "The Technical Specification for the SCAP", Version 1.2 September 2011.)
2. Performance, resource (network, VMs, VM storage, and shared storage), status and utilization, and events within the provider's boundary (failure of service, degraded service, availability of the network, storage, and operating systems). VA may opt to have the Contractor deploy VA's Command Center Enterprise monitoring tool in addition to Contractor provided tools. The Contractor shall be responsible for installation and initial configuration of the monitoring tool as well as initial configuration of the monitoring dashboard.
3. Provide the above real-time to a Dashboard that is available 24 hours a day, seven days per week in accordance with the SLA in Attachment 1. The dashboard shall:
   a. Present automated alerts and present metrics for the most recent 24-hour period. In addition, a rolling average shall be maintained for each metric and retained for an additional 90 days. Logs shall be retained for 90 days.
   b. Provide an interface that allows the configuration of alerts and setting of alert thresholds at a VA-defined user group level.
   c. Present and organize information only for and relevant to the user's assignments for monetary credit back to VA for the Contractor's inability to meet the SLA.
   d. Support user defined alerts that trigger on metrics and thresholds specified by the user and send an e-mail to the users with the alert information (Contractor Format).

In addition to the above monitoring, the Contractor shall install, configure, and manage a VA provided monitoring agent. The agents shall report enterprise level visibility and monitoring.

5.3.5 IDENTITY AND ACCESS MANAGEMENT FUNCTIONS

Within the Cloud itself and the EMM, the Contractor shall provide the following:

1. The ability to authenticate and perform centralized management for each user and administrator by fully integrating with a VA Active Directory system.

2. Update or replace and maintain some or all of the existing VA approved certificates in the EMM solution as required to meet Active Directory integration requirements, as well as individual project and application requirements. All

Active Directory and certificate work must be coordinated with the appropriate VA teams to ensure minimum downtime.

3. Provide an EMM solution that has full capability to integrate with current and future releases of the VA Identity and Access Management (IAM) systems.

4. Integrate with VA’s two factor authentication for all system accounts and all elevated privileges. The two factor authentication solution must either integrate with VA’s existing solution for USB etoken or one-time password six digit Personal Identification Number (PIN) tokens (currently provided by Safenet).

5.3.6 DATA SECURITY

The Contractor’s facilities shall have management, operation, and technical controls in place (NIST 800-53, FedRAMP Moderate, and Statement on Auditing Standards (SAS) 70 Type II) for the protection of data.

5.3.7 EMM DISASTER RECOVERY

The Contractor must meet the uptime of 99.9% for the EMM solution and all EMM Disaster Recovery models must meet all of VA’s requirements as detailed in Attachment 1.

5.3.8 EMM BACKUP AND RECOVERY

The Contractor shall provide for the backup and recovery of information stored by the EMM solution to meet the related SLAs in Attachment 1.

5.3.9 AUDIT COOPERATION

The Contractor shall cooperate with all VA audits, including Office of the Inspector General (OIG), Continuous Readiness in Information Security Program (CRISP), Office of Information Security (OIS), and others in the areas of facilities access, audits, security incident notification, and hosting location. These audits could be yearly or impromptu audits at VA’s request. The Contractor will be expected to provide support on demand, including after hours.

Specifically, the Contractor (and any Subcontractors) shall:

1. Provide the CO, COR, VA Project Manager, and representatives of the agency's auditors, full and free access to the Contractor's (and Subcontractors') facilities, installations, operations documentation, databases, and personnel used for contract hosting services. This access shall be provided to the extent required to carry out audits, inspections, investigations, or other reviews to ensure compliance with contractual requirements for IT and information security, and to safeguard against threats and hazards to the integrity, availability, and confidentiality of agency information in the possession or under the control of the Contractor (or Subcontractor).

2. Fully cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the CO or the agency auditors as described in subparagraph 1 above. Full cooperation includes, but is not limited to, prompt disclosure (within two business days) to authorized requests of data, information, and records requested in connection with any audit, inspection, investigation, or review, making employees of the Contractor available for interview by auditors, inspectors, and investigators upon request, and providing prompt access (within two business days) to Contractor facilities, systems, data and personnel to the extent the auditors, inspectors, and investigators reasonably believe necessary to complete the audit, inspection, investigation, or other review.

5.4 VALIDATE EMM MANAGED SOLUTION

5.4.1 EMM TEST PLANNING

The Contractor shall deliver an EMM Test Plan/Procedure to demonstrate an EMM cloud hosted solution that meets the requirements of this PWS. The EMM Test Plan/Procedure shall define detailed acceptance test procedures/scripts to demonstrate full compliance with the technical and functional capabilities outlined in the Appendix A: EMM Capabilities. This shall include timelines, facility, power, equipment requirements, application servers, middleware, and back-end data servers. The EMM environment will contain PII or other sensitive data that shall be appropriately secured by the Contractor.

Deliverable:

A. EMM Test Plan/Procedure

5.4.2 EMM PRELIMINARY TEST

The Contractor shall conduct a thorough preliminary test of the EMM cloud hosted functionality in accordance with the Government approved EMM Test Plan/Procedure delivered under paragraph 5.4.1 above to determine if the application(s) is ready for a formal Acceptance Test. This demonstration/test shall:

1. Be conducted after implementation of the EMM cloud environment.
2. Be conducted at a VA test lab facility in a test environment.
3. Be planned and coordinated to provide at least three calendar days advance notice to the VA PM/COR before test start.
4. Be fully witnessed by the VA PM/COR and other VA designated representatives.
5. Be conducted in strict compliance with the procedures/script approved by the VA PM/COR to discretely address every functional/technical requirement defined by in Appendix A: EMM Capabilities.
6. Provide the ability to make any corrections to the EMM, as required.

The Contractor shall prepare an EMM Demonstration/Preliminary Operational Test Report documenting the results of the test, delineating each failed or incomplete requirement.

Should there be non-compliant items resulting from the Preliminary Test, the Contractor shall make corrections and shall re-test the full product within five calendar days. This repeat test shall be a full test in accordance with this section – not simply a test of the failed features. The Contractor shall ensure all failures are corrected and that all corrections are acceptable to VA.

The Contractor shall provide a Cloud Test Plan that describes how the cloud will comply with the FedRAMP requirements and FISMA certification, security, functional, availability and performance requirements outlined for the entire system and associated environments. The Cloud Test Plan shall address timelines, facility, power, equipment requirements, application servers, middleware and back-end data servers. The Cloud Test Plan shall describe how the Cloud shall handle data that may contain PII, Sensitive Personal Information (SPI), Privacy Act, Payment Card Industry (PCI) or other VA sensitive data. The Cloud Test Plan shall describe how to ensure data is appropriately secured by the Contractor and the required A&A documentation and testing, based on VA Handbook 6500. The Cloud Test Plan shall be submitted by the Contractor to the VA PM/COR.

The COR, in coordination with the VA technical teams, will review the Cloud Test Plan in detail at the initial kickoff meeting and will provide specific, detailed comments before conclusion of the meeting. The Contractor shall update the Cloud Test Plan in response to any comments.

Deliverable:

A. EMM Demonstration/Preliminary Operational Test Report
B. Cloud Test Plan

5.4.3 EMM OPERATIONAL ACCEPTANCE TEST

The Contractor shall conduct Operational Acceptance Test of the EMM solution at VA facilities in Hines, IL after completion of the EMM Preliminary Test, performed under paragraph 5.4.2 above. The Contractor shall install the EMM, network configuration, integrating with Active Directory environment including each of the 33 domains inside of the Contractor-provided or VA.gov Active Directory forest, establishing the configurations and provisioning services and hosting the solution. Installation and operations shall comply with the EMM Security Requirements in accordance with Appendix A: EMM Capabilities.

This test shall be performed in accordance with the Government approved EMM Test Plan/Procedures delivered under paragraph 5.4.1 above. This Operational Acceptance Test shall:

1. Prove that the EMM solution meets the technical and functional requirements of this PWS and its appendices and attachments.
2. Be planned and coordinated to provide at least three business days advance notice to the COR before test start.

3. Be fully witnessed by the COR and other VA designated representatives.
4. Demonstrate all security thresholds are met in order to allow connectivity between the EMM solution and VA's network.
5. Be conducted in strict compliance with the procedures/script approved by the COR to discretely address every functional/technical requirement defined by this PWS including Appendix A: EMM Capabilities.

The Contractor shall prepare an EMM Operational Acceptance Test Report documenting the results of the test, delineating each failed or incomplete requirement.

Should there be non-compliant items resulting from the Operational Acceptance Test, the Contractor shall make corrections and shall re-test the full product within five business days. This repeat test shall be a full test in accordance with this section – not simply a test of the failed features.

The Contractor shall conduct Acceptance Testing of the Cloud. This test shall comply with the Government approved Cloud Test Plan delivered under paragraph 5.4.2 above. The Contractor shall provide at least three business days advanced notice to the COR before the start of testing. This test shall:

1. Demonstrate all security thresholds are met in order to allow connectivity between the Cloud and VA's network.
2. Be conducted in a VA facility. The Contractor shall coordinate with the COR at the kickoff meeting to determine specific location and facility requirements in accordance with the SLA, Attachment 1.
3. Demonstrate to the VA PM/COR and other VA designated representatives that the Cloud solution meets the technical and functional requirements of this PWS.

The Contractor shall prepare a Cloud Acceptance Test Report documenting the results of the test, delineating each failed or incomplete requirement.

Should there be non-compliant items resulting from the Cloud Acceptance Test, the Contractor shall make corrections and shall re-test the application(s) within five business days. This repeat test shall be a full test in accordance with this section – not simply a test of the failed features.

Deliverable:

A. EMM Operational Acceptance Test Report
B. Cloud Acceptance Test Report

5.4.4 TEST DEVICE STANDUP FROM VA CURRENT EMM TO CONTRACTOR PROVIDED EMM

The Contractor shall test that all models of currently issued VA devices can be successfully migrated to the new EMM solution. The Contractor shall create a device migration plan for COR review, including appropriate validation methodology of test results. The Contractor shall conduct a test migration and review results with the

COR/PM. The Contractor shall prepare a detailed device migration plan for full migration following successful demonstration of the test migration. Once the test migration is done, the Contractor shall provide the full migration to the new system.

After full migration, the users and devices shall be functioning on the new EMM platform with the same profiles, policies and settings. The Contractor shall provide console and device screenshots demonstrating successful migration.

5.4.5 PROVIDE ATO DOCUMENTATION AND SUPPORT

The EMM system shall be hosted on a FedRAMP Moderate certified cloud solution. The Contractor shall provide a copy of the FedRAMP Moderate Certification issued granting Authority to Operate (ATO) to the cloud provider that is hosting the EMM solution. The Contractor shall maintain its security authorization throughout the TO PoP. The FedRAMP certificate is a Provisional ATO, and shall employ the appropriate security controls for systems with FISMA information system impact levels of Moderate, as specified by NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

The Contractor shall provide A&A support required to achieve and maintain full A&A certification in compliance with the most current versions of VA Handbook 6500, VA Handbook 6500.6 (Section 3), and VA Handbook 6500.3.

The Contractor shall be responsible for maintaining an ATO for the life of the TO for the EMM solution. The A&A process is the end-to-end process for ensuring new VA information systems adhere to and follow FISMA.

Throughout the A&A process, the Contractor shall work with its assigned Information Security Officer (ISO) to obtain an ATO. The process entails gaining access to the Governance, Risk and Compliance (GRC) tool, RiskVision, to serve as the management tool for the A&A process. The GRC tool is used to document accreditation requirements including technical testing/scans, security documentation, and actions identified during the Security Control Assessment.

The Contractor shall ensure all security assessments are completed using VA-provided tools to include Agiliance RiskVision. RiskVision Control Questions shall be answered and evidence documents uploaded no later than 90 days after delivery of the proposed EMM SaaS solution.

The Contractor shall perform the tasks and sub-tasks designated as the “system steward” and system owner or “delegate” in the most recent version of the Authorization Requirements Standard Operating Procedures (refer to Attachment 3). The Contractor shall enable VA vulnerability scanning and prioritize corrective actions to mitigate identified weaknesses and vulnerabilities. The Contractor shall perform risk assessments and risk handling to include mitigating discovered vulnerabilities. The Contractor shall perform continuous monitoring per VA’s CRISP. The Contractor shall develop and submit all required Security Document Artifacts.

The Contractor shall ensure any findings produced as a result of the security assessments are remediated in order to support A&A. The Contractor shall ensure all other security requirements are met specific to the FIPS 199 categorization documented as a result of the Risk Assessment and applicable VA policy. The Contractor shall ensure all requirements of the Authorization Requirements Standard Operating Procedures (most current version) are met throughout the project lifecycle.

The Contractor shall support audits regarding the implementation of these policies and assist in the collection and preparation of related compliance evidence. The Contractor shall retain and maintain referenced, applicable documents and deliverable documentation and make it available for review.

The Contractor shall provide support to assist in meeting security requirements including:

1. The Contractor shall be available for an interview and provide documentation or allow an onsite inspection for an A&A audit.
2. For any items that failed or demonstrated other than stratified controls identified by any auditing activity, the Contractor shall provide a Plan of Action and Milestones (POA&M) addressing each issue noted in accordance with the failure classification levels: High, Medium, and Low. Contractor remediation shall follow the following schedule:
    a. High = 60 calendar days
    b. Medium/Moderate = 90 calendar days
    c. Low = 120 calendar days

The Contractor shall perform bi-weekly reviews of the POA&M with the VA PM/COR to ensure backlog is scheduled and prioritized for remediation, and to verify that defined milestones will be achieved. The Contractor shall perform monthly reviews of Risk Based Decisions with the VA PM/COR to ensure remediation to outstanding risks or path forward is identified and achievable.

Anything not remedied during the referenced timeframes must be escalated to the VA PM for further review. The Contractor shall be available for an interview and provide documentation or allow an onsite inspection upon a mutually agreed schedule to validate its Security Test and Evaluation Plan for compliance with VA requirements. The Contractor shall conduct a risk assessment of the Federal and private environments. Actions are to be documented on the POA&M listing and reported to the VA PM. The Contractor shall allow for independent security controls assessment activities and scanning of any devices with prior notice. The Contractor shall provide copies of all policies and procedures and any other deliverables required to conduct a Security Controls Assessment at least 30 calendar days prior to the scheduled assessment. The Contractor shall, prior to the deployment of each EMM application or major upgrade, perform the A&A activities required to assure that addition of the application or major upgrade to the EMM solution does not violate the conditions of the EMM’s ATO.

Deliverables:

A. FedRAMP Moderate Certification
B. RiskVision Control Questions
C. Security Document Artifacts
D. Plan of Actions and Milestones

5.4.6 ENVIRONMENT AND DOCUMENTATION VALIDATION

The Contractor shall provide an Environment Validation Report to document that all technical, functional, operational, and security requirements for the EMM solution have been met. The following elements shall be included in the Environment Validation Report:

1. Technical: Validation of network configurations of both primary and secondary sites for the EMM cloud environments.
2. Functional: Validation of the Functional Requirements
3. Operational:
    a. Validation of the resource capacity (SaaS).
    b. Verification that Disaster Recovery approach has been approved by VA PM/COR.
    c. Verification that Backup and Retention approach has been approved by VA PM/COR.
    d. Verification that Phase-In Migration Plan is complete and provided to VA PM/COR.
4. Security:
    a. Verification that Event Escalation Plan is complete and provided to VA PM/COR.
    b. Verification that Security concept of operations is complete and provided to VA PM/COR.
    c. Verification that A&A Certification Package is complete and provided to VA PM/COR.
    d. Verification that all draft Architecture, Configuration and System artifacts associated with A&A activities are complete and provided to VA.
    e. POA&Ms identifying security findings and vulnerabilities identified during A&A activities listed in this TO.
5. Authorities to Operate:
    a. Verify completion of documentation and processes required to obtain/maintain ATO for the EMM solution and environments stood up during the duration of this TO, as well as ATO documentation for all cloud services at both the primary and secondary sites.

Deliverable:

A. Environment Validation Report

5.5 IMPLEMENT EMM MANAGED SOLUTION

5.5.1 EMM IMPLEMENTATION PLANNING

The Contractor shall deliver an EMM Managed Solution Implementation Plan that includes:

1. All technical and physical requirements for hosting, housing, operating and maintaining the EMM.
2. All requirements associated with initial installation/implementation.
3. Security processes and procedures to ensure compliance with the EMM Security Requirements in accordance with Appendix A: EMM Capabilities.
4. Security processes and procedures to ensure compliance with the Cloud Computing Security Requirements Baseline as detailed in Chapter 1 of Proposed Security Assessment & Authorization for U.S. Government Cloud Computing Security Requirements Baseline, Attachment 2.
5. Tasks required to obtain an Interim or Full Authority to Operate for the EMM managed solution including EMM ATO and Cloud Hosting Facility ATO
6. All tasks and timeline for migration of existing devices
7. Maintenance and upgrade timelines.
8. Procedures and metrics for ensuring compliance with the EMM SLA: Attachment 1.

Deliverable:

A. EMM Implementation Plan

5.5.2 EMM DOCUMENTATION

The Contractor shall provide Standard Operating Procedures for the EMM. These Standard Operating Procedures shall pertain to O&M of the EMM. Diagrams, and engineering artifacts describing the architecture, components and processes, shall be delivered as part of the EMM Solution Documentation. The Contractor shall manage and administer the maintenance of all required documentation supporting the implementation, sustainment and transition of the EMM system. The Contractor shall also provide, as part of the EMM Solution Documentation, the documentation and implement processes and procedures to comply with each item required by NIST SP 800-53 Rev. 4 below:

1. Access Control Policy and Procedures
2. Security Awareness and Training Policy and Procedures
3. Security A&A Policy and Procedures
4. Contingency Planning Policy and Procedures
5. Identification and Authentication Policy and Procedures
6. Incident Response Policy and Procedures
7. System Maintenance Policy and Procedures
8. Media Protection Policy and Procedures
9. Physical and Environmental Protection Policy and Procedures
10. Security Planning Policy and Procedures

11. Risk Assessment Policy and Procedures
12. System and Services Acquisition Policy and Procedures
13. System and Communications Protection Policy and Procedures
14. System and Information Integrity Policy and Procedures
15. EMM End User and Admin Instructions for provisioning permitted devices in the EMM.

All documentation shall be delivered to the VA PM/COR prior to actual implementation/deployment and updated as required to reflect changes to the technical environment.

Deliverables:

A. EMM Standard Operating Procedures
B. EMM Solution Documentation
C. EMM End User and Admin Instructions

5.5.3 EMM HELP DESK SCRIPTS

The Contractor shall create documentation to support implementation of online help desk functionality to support VA users of the EMM. The Contractor shall provide help desk scripts, with active hyperlinks between the system documentation, including administration and users manuals and guides.

5.5.4 PREPARE THE EMM PLATFORM FOR FULL PRODUCTION

After successful completion of the Operational Acceptance Test and written acceptance by the COR, the Contractor shall, in full compliance with the VA-approved EMM Implementation Plan required in Paragraph 5.5.1 above, implement/deploy the EMM in the EMM Environment. The Contractor shall provide Standard Operating Procedures, custom software code, and licenses (currently 45,000) for all software included in the EMM prior to actual implementation. VA will provide the AirWatch licenses via the ELA.

The Contractor shall provide all labor and technical support services to implement and support the EMM solution, including primary interaction with VA resources required to bring the system online. The Contractor shall coordinate through the COR with VA team members to set up and troubleshoot connectivity, to publish required certificates, establish Domain Name System (DNS) entries, entering and tracking tickets to open required ports through Enterprise Security Change Control Board (ESCCB), and interface with Microsoft Exchange and implement changes required.

5.6 ONGOING EMM MANAGED SOLUTION TECHNICAL SUPPORT

5.6.1 QUARTERLY PROVISION OF MOBILE DEVICES FOR VA ASSESSMENT AND TESTING

The Contractor shall purchase and deliver “new in box” mobile tablets, phone devices, wearable devices and accessories as requested by VA every 90 days throughout the PoP to support mobile applications development, configuration, test, and training activities. Devices shall be delivered within 14 days of VA request. VA plans to assess devices reflective of those in use by VA and estimates that each quarterly purchase will not exceed $12,000 plus the Contractor handling fee. Prior to any purchases, the Contractor shall coordinate with the COR in order to determine which devices are required as well as their unique specifications. The tablet/phone/wearable devices shall represent the four major mobile operating system platforms: Android, iOS, Blackberry, and Windows tablets (full Windows 8, 10 and beyond) or phones. All cables, cases, approved Bluetooth devices (keyboards, mice); docking station, manuals and software shall be included with these devices. These mobile devices shall have the ability to utilize cellular data networks such as 3G, 4G, and LTE. A cellular subscription is not included in this requirement. The Contractor shall price out the cost for the devices plus any handling fees ($12,000 shall be used for the devices, not any other costs). In addition, the Contractor shall ensure the devices will be enrolled by the seller into the manufacturer's corporate device enrollment plan, and be shipped to a site of the Government's choosing.

The Contractor shall provide Mobile Device Documentation to include the final purchase order and invoices for each purchase relating to this $12,000 to the COR, the VA PM, VA CO/CS and their assigned technical representatives.

The Contractor shall include a monthly summary of purchases to date and balance remaining from the $12,000 allotment for each 90-day period in the Contractor's Progress, Status and Management Report.

Deliverable:

A. Mobile Devices Documentation

5.6.2 EMM ADMINISTRATION AND PRODUCT ASSESSMENT

The Contractor shall support provisioning profiles, supporting actions on lost devices, creation and submission of compliance reports, and coordinating with various VA entities as required. The Contractor shall manage the VA App catalog regarding posting new Apps, sun setting Apps, and validating App metadata.

The Contractor shall maintain testing space and equipment to test EMM upgrades and updates. The Contractor shall test and recommend upgrades and updates within seven business days of their release. The Contractor shall then make recommendations to VA on the installation of these upgrades and updates. With VA's concurrence and approval, the Contractor shall then implement the concurred recommendations.

The Contractor shall provide quarterly product assessments of EMM's ability to handle changes/upgrades to state of the art, commercially available tablet/phone devices. The Contractor shall upgrade or create new EMM configurations and ensure device compliance with VA requirements based on evaluations of new device technologies and operating systems.

A summary of each quarterly product assessment shall be documented in a Mobile Device Product Assessment Report. Where any or all of the devices directly impact the ability of the EMM to perform its required functions, the Contractor shall create and implement an upgrade/update to the EMM within 30 calendar days of mobile device delivery. Where upgrade/update is not required, the Contractor shall notify the COR in writing as part of the Mobile Device Product Assessment Report.

Any upgrades to EMM processing shall be tested with test results reviewed and approved by the COR prior to release. Test results shall be included in the Mobile Device Product Assessment Report.

Deliverable:

A. Mobile Device Product Assessment Report

5.6.3 CONTINUE SUPPORT FOR ATO

The Contractor shall continue preparing, updating and maintaining the documentation required for full ATOs for the EMM application and the EMM cloud hosting facility.

5.7 OPERATIONS AND MAINTENANCE

Following successful operational acceptance test and implementation of the EMM, the Contractor shall provide full, turnkey O&M of all EMM components. This shall include O&M of all hardware, software, administration, cloud environment troubleshooting, services, materials, licenses, certificates and documentation required for the EMM environments and EMM communication with devices. The Contractor shall test new functionality as released through the EMM upgrades and interaction with device operating systems and update training materials for administrators and end users when any procedures have changed or new processes are created.

The Contractor shall function as the primary project team responsible for the operation and maintenance of all components, and shall coordinate with all stakeholders, including VA and EMM licensing providers to provide customization required to support the VA mission. The Contractor shall interface with EMM supporting applications and supporting services project teams, security, database and network administrators, ISOs, operations support staff, and System Administration support staff as required during the course of operations and maintenance work. The Contractor shall manage the VA EMM solution, providing full turnkey O&M for this EMM solution for every server and resource hosted in the EMM environments. The Contractor shall coordinate with the VA ELA project team to ensure that the current licenses are procured.

The Contractor shall oversee all components of the EMM to ensure the system is functioning at required performance levels and available to all users of both environments (UAT and Production) in accordance with the SLA in Attachment 1. The Contractor shall be responsible for all O&M required to support EMM environments, including hardware and software. The Contractor shall include a summary of all operations and maintenance activities, issues, and actions taken in the Weekly Status Update Meeting described in PWS Task 5.1.4.

The Contractor shall provide and maintain all certificates, including server and device, allowing all functions of the environment to be properly certified. The Contractor shall work with the VA certificate authority to ensure that the certificates used are acceptable to VA.

The Contractor shall maintain current user and admin instructions and technical documentation, logging changes that occur as a result of fixes/updates to the EMM solution including any and all system interconnections.

VA COR/PM requires review and approval through the current VA EMM Change Control Board (CCB) of all actions impacting the production environment.

For general maintenance, the Contractor shall provide support from 8 a.m. EST to 8 p.m. EST Monday through Friday excluding Federal holidays. For issues impacting the EMM SLA and for environment upgrades, the Contractor shall provide coverage 24 hours a day, seven days a week until the issue is resolved.

The Contractor shall provide functions including, but not limited to:

1. Project Management services
2. Engineering-level support (Tier 4)
3. All hardware and software, as well as any and all upgrades and patches to both the hardware and software.
4. All O&M support of
    a. Patching of both cloud environment and any hardware, software, operating systems, infrastructure and servers that reside in the Cloud.
    b. Patching of all operating systems based on vulnerability scans, regular patch cycles, and operating system updates, to remain compliant with VA policy regarding timelines for patching.
    c. Daily health checks- health of operating system, network connectivity, storage, RAM and processors.
    d. Setup of servers to VA standards (Anti-Virus, Firewall, Simple Mail Transfer Protocol (SMTP), monitoring tools (System Center Configuration Manager (SCCM)/BigFix, and Encase) and monitor the systems in each of these tools to ensure they remain compliant.
    e. Creation of admin accounts
    f. Creation of organizational groups
    g. Apply profiles and policies to groups
    h. Research new methods to streamline current EMM processes, and propose/implement new options for VA to use as a new standard process.
5. Manage Active Directory environments
6. Centralized monitoring
7. Security scanning and remediation coordination

8. Web Application Security Assessment (WASA) scanning and remediation
9. Centralized log management and review
10. Coordinate all VA required routine, non-routine associated fixes and updates to the EMM solution.
11. Work with third parties (e.g., warranty, services, suppliers) when required, to successfully accomplish the tasks in this PWS.

The Contractor shall provide all VA-specific configuration items and coding created for enterprise implementation and deployment of the EMM solution, which shall all be fully transferrable to VA at the end of this TO.

5.7.1 O&M PLANNING AND REPORTING

The Contractor shall:

1. Create a new O&M Plan. The O&M Plan shall include the Contractor's concepts, processes, procedures and resources that shall be utilized to provide the required O&M support for the EMM environments as described in the tasks below.
2. Develop procedures to ensure the EMM has the best practices for deployment and maintenance for all pieces of this enterprise system, including devices enrollment and credentialing, end of life, and app management.
3. Perform all O&M activities identified below in accordance with the approved O&M Plan.
4. Provide a summary of monthly O&M activities and statistics as part of the Contractor's Progress Status and Management Report.

Deliverable:

A. O&M Plan

5.7.2 TIER 4 SUPPORT

The Contractor shall provide Tier 4 support in complex problems in managing accounts, access to the environments, creating and maintaining profiles, implementing certificates, making moves/adds/changes, providing testing and upgrades, and configuring and responding to alerts. Tier 4 support shall cover all aspects of EMM device and user issues raised by the Tier 3 admin staff (approximately 20 Tier 3 administrators). VA and other contractors will provide Tier 1, 2, and 3 support.

The Contractor shall use the VA ServiceNow ticket system to monitor and manage tickets and deliver a summary of the trouble ticket log which shall be submitted as part of the Weekly Status Meeting. The trouble ticket log shall log the date and time of the original call, date and time of initial response, detailed description of action(s) taken, including date and time of each action, name of technician, and date and time of final resolution. Reports should be available upon request on all service actions, history, trends, open tickets and other relevant data.

5.7.3 MANAGEMENT OF ENVIRONMENT AND APPLICATIONS

In order to maintain an ATO, all NIST requirements from 800-53 must be met as part of the standup, O&M. All of the components shall meet the SLA requirements as detailed in Attachment 1.

5.7.4 CHANGE AND CONFIGURATION MANAGEMENT

The Contractor shall lead and fully manage the EMM change control processes. The Contractor shall maintain hardware and software documentation for the infrastructure, environments, virtual machines, and infrastructure, platform and security applications and software provided by the Contractor supporting the Cloud/EMM SaaS cloud. VA will maintain decision approval authority while the Contractor shall plan and lead all actions and meetings in support of change control for all components of the TO. The Contractor shall provide:

1. Infrastructure configuration management – tracking configuration changes to baseline definitions of provisioned resources, networking components, and interconnectivity back and forth to the VA intranet from the entire cloud and all associated environments.
2. Key event scheduling – scheduling, reviewing, publishing, and tracking infrastructure events.
3. EMM release management – managing the release of new and existing EMM service versions and patches.
4. Operating System Management – tracking configuration changes to baseline of the operating system to ensure continued adherence to VA security baselines.
5. Vulnerability Scanning and Remediation to include application level for associated environments.
6. Support Configuration Management
7. Notification of designated VA Points of Contact (POCs) for all supported projects/initiatives of any scheduled/unscheduled service interruptions (outages) 24 hours in advance. The Contractor shall provide any required software or tools to aid in communication of service interruptions to all required internal and external stakeholders. Service Interruption Notifications shall include:
    a. Periodic (hourly) outage updates with estimated time to resolution
    b. Final resolution
    c. Root cause analysis including any corrective/preventive steps taken to avoid future outages
    d. Statement of credit related to any outage for loss of service to be applied to VA account due to the outage if any
    e. Participation in VA Swift Action Team (SWAT) calls
8. Establish a CM system for virtual network changes received from VA designees.
9. Facilitate and support the ad hoc EMM CCB tickets, which shall include:
    a. Processing tickets with CCB actions and ensure they are updated accurately.
    b. Notifying submitter if their change was approved, or if not, why.

c. Submitting tickets to Solution Delivery (SD) and ITOPS National CCB (NCCB) for review and approval during weekly calls.
d. Working with existing VA CCB ticket system and perform moves/add/changes for all EMM administrators. The Contractor shall be responsible for adding and removing EMM administrators as part of the Tier 4 support.

Deliverable:

A. Service Interruption Notifications

5.7.5 NETWORK ADMINISTRATION

The Contractor shall administer the EMM network configuration. The network connectivity shall meet the SLAs as dictated in Attachment 1. The Contractor shall:

1. Coordinate any changes, updates or address performance issues with all interconnections both internal to VA as well as external to outside entities.
2. Create and update ESCCB tickets for management of network ports and IP ranges through the VA's NSOC and BPE teams. The Contractor shall ensure that tickets are accurate and up-to-date. The Contractor shall update tickets in a timely fashion if more information is required.
3. Attend implementation sessions for ESCCB tickets with the BPE and Gateway teams.

5.7.6 RELEASE MANAGEMENT

The Contractor shall ensure the planned and controlled deployment of software updates into the EMM solution. The Contractor shall:

1. Provide release management support and documentation links to users and support personnel.
2. Provide notifications on release and its status to stakeholders.
3. Test and recommend pertinent upgrades and updates within 14 days of releases. The Contractor shall then make recommendations to VA in writing on the installation of these upgrades and updates to the VA environment. With VA's concurrence and approval, the Contractor shall then implement the concurred recommendations.
4. When performing related tasks for O&M work, the Contractor shall perform all tests to assure that there is no detrimental effect on the systems involved before, during, and after work is completed. Testing shall address: interoperability, user interface, enterprise security, data security, privacy and data security, 508 compliance, systems performance impact assessment, enterprise architecture, usability and compatibility with related systems and supporting services.

5.7.7 SECURITY MANAGEMENT

The Contractor shall have overall responsibility for implementation of policies, standards and procedures to ensure the protection of the organization's assets, data, information and IT services from harm due to failures of confidentiality, integrity and availability in order to meet all security requirements in accordance with NIST regulations, VA 6500 as well as VA directives, SLA Attachment 1 and Authorization Requirements Standard Operating Procedures Attachment 3. The Contractor shall:

1. Perform recurring security activities required to ensure that the EMM solution remains in compliance with VA/ATO security requirements.
2. Maintain Interconnection Security Agreements (ISAs)
3. Maintain Privacy Impact Assessment (PIA)
4. Maintain Risk Assessment
5. Maintain Security Configuration Checklists
6. Maintain Security Plan
7. Ensure Firewall Security
8. Ensure Physical Security of Facility
9. Generate Reviews and Audit Reports
10. Manage and Review Application Access Logs
11. Maintain ATO
12. Perform Security Audits
13. Perform Security Controls Testing
14. Validate Application Security Measures
15. Perform Vulnerability Scanning

The Contractor shall comply with the requirements for incident management and responses documented in the SLA attached to this PWS in Attachment 1 are met and that monitoring services are in place per the SLA to properly respond to all incidents as they arise during the course of this TO.

The Contractor shall coordinate appropriate resources to address incidents and communicate incident related information for situational awareness within two hours of the incident. The Contractor shall:

1. Assess Knowledge Base to Identify Potential Solutions.
2. Document Incident Escalation Procedures.
3. Escalate Incidents/Requests.
4. Issue Incident Response Messages (IRMMs) and/or Automated Notification Reports (ANR) Messages for Critical Maintenance.
5. Log and Track Incidents/Requests.
6. Notify COR of Incident.
7. Perform Triage for Incidents/Requests.
8. Provide Incident Reporting and Distribution.
9. Respond to Incidents/Requests.
10. Identify hosting or application changes required to ensure similar incidents will not occur.
11. Implement hosting or application changes upon approval of the COR.

5.7.8 STORAGE MANAGEMENT

The Contractor shall comply with VA 6500 on storage management requirements. The Contractor shall work with VA to make sure that application data is separated via a different storage partition from the application data. The ongoing storage will be sufficient to meet the SLA

5.7.9 SYSTEM ADMINISTRATION

The Contractor shall provide system administration for the EMM solution. The Contractor shall ensure that the system meets the SLAs as dictated in Attachment 1. The Contractor shall:

1. Ensure that all components of the EMM solution are maintained at an established baseline and updated with the latest security patches, upgrades, and encryption as required.
2. Grant, monitor and remove administrative rights to servers and peripherals in accordance with VA policy.
3. Provide access control and admin account creation for admin staff.
4. Abide by all established administration processes and procedures as listed in the VA 6500 as well as NIST, as well as any appropriate systems administration processes and procedures provided by VA.
5. Manage and coordinate all Access Control activities across all environments covered under this TO.
6. Review, coordinate, and route access requests for signatures to COR, ISO, and System Owner for all access control requests.
7. Perform all administration of Active Directory environment, including account management, group policy management, and server baselining for all operating systems.
8. Implement and audit all access.
9. Follow Role-based access control (RBAC) methodology, as well as related NIST 800-162, VA 6500 and other guidance provided by VA.

The Contractor shall provide the following system administration tools:

1. A user account management capability.
2. Ability to deactivate inactive user accounts.
3. An automated function to create reports to depict user account management information.

5.7.10 PLATFORM MONITORING

The Contractor shall setup a VA-approved automated system monitoring tool on all machines stood up in support of the EMM solution. The Contractor shall coordinate client installations, setup triggers and alerts as required to monitor the EMM SLA as dictated in Attachment 1.

The Contractor shall provide all technical resources required to install, configure, maintain and support the system monitoring. The Contractor shall issue alerts and notifications to VA when the SLAs are not being met.

The Contractor shall:

1. Coordinate with VA to identify triggers requiring alerts.
2. Provide a method of communication of alerts to Contractor and VA staff.
3. Institute a procedure to ensure availability of Contractor staff to respond to alerts within the guidelines established by the SLA in Attachment 1.

The Contractor shall also monitor any specific machines which are stood up in VA for the sole purposes of supporting the Contractor’s approach for any of the tasks previously stated (e.g., the current EMM software requires approximately four machines inside of the VA intranet for Active Directory communication to the EMM software for the purposes of user account management and assignment. These critical pieces of infrastructure shall be managed to maintain the health of the EMM solution). This also includes, but is not limited to, coordination with the ESCCB to enable those systems to connect back to the dashboards and reporting servers as necessary.

5.7.11 SOFTWARE LICENSE MANAGEMENT

The Contractor shall:

1. Maintain a software inventory for all EMM software installed.
2. Perform patch management to ensure all software is up to date and meeting applicable security and baseline standards.
3. Monitor expiration dates of all software licenses in the environment and renew licenses to ensure no outages during the period of performance.
4. Provide support throughout the PoP for technical issues related to all licenses provided by the Contractor.
5. If the chosen solution is AirWatch, the Contractor shall work with the VA ELA team to ensure the correct number of licenses have been procured.

5.8 CERTIFICATE BASED AUTHENTICATION

The Contractor shall provide a solution to provide certificate based authentication for mobile devices.

The certificate based authentication is also known as a derived credential, and as such must be able to meet the requirements of NIST SP 800-157.

The solution shall be fully integrated into the EMM solution so that the end user is able to use this certificate for authentication, encryption, and signing on all applications including native applications, first party EMM provided applications, and any and all second and third party applications as provided. This same certificate shall be able to be used by any applications that are built in-house or side loaded onto the device as required.

The creation of the certificate used for certificate based authentication must be able to meet Level 3 Level of Assurance (LOA) for authentication based on NIST SP 800-63-2. This means the end user can use their existing PIV card for creation of the user certificate, and cannot create the certificate with any other means.

The certificate based authentication solution is a critical piece of the overall EMM solution.

VA is currently using ActivIdentity to create its PIV cards but hopes to be migrating off to another more modern solution in the near future. When that happens, this certificate based authentication solution must also be migrated to support the new PIV backend.

The solution shall have the ability to integrate with any of the leading products currently on the market for certificate based authentication and change if the requirements of VA change, as VA cannot be vendor locked into a single solution and managed.

The solution shall provide the ability for the credential to be created on the device rather than created elsewhere and transmitted to the device to prevent any possible man-in-the-middle attacks. This also helps to make sure the certificate that is created is not exportable off of the single instance on the device itself.

The solution shall have to ability to be used as the client certificate to authenticate against VA's current mobile VPN application Cisco AnyConnect for authentication.

The Contractor shall provide an EMM solution that has the ability to deploy user certificates in accordance with NIST specifications that allow for usage on iOS and Android mobile devices for authentication and encryption. The solution should be either a component of the EMM solution or a secondary system that works in conjunction with the EMM solution to provide these certificates to the mobile device. This solution must be currently available and on the market, and have no components that are awaiting a future release date. The solution must have the ability to deliver these certificate based authentication certificates to the native keystore of iOS, and Android, as well as the EMM keystore, and third party keystores. The solution must be fully compliant to Identity Assurance Level (IAL) 2 from NIST SP 800-63-3.

Certificate based authentication solution must support multiple COTS solutions providers using the same application as well as the same interface. Having multiple solutions creates unnecessary complexity for administration as well as end user enrollment and management as the Government is unable to predict if external factors would require migration from one system to another. The single application / single interface also help the VA to make sure that functionality and updates are timely across the total solution and not fragmented across multiple applications / interfaces.

Certificate based authentication solution must support authentication across all iOS native applications, EMM software development kit (SDK) applications as well as third party applications. As VA is currently shifting its solution for multiple pieces of its portfolio the CBA authentication must be able to work in any number of solutions from the EMM vendor or from native or third party applications to shift as VA leadership as well as technical requirements shift. Mail for example is an area where the VA is currently shifting off of Good for Enterprise as that application has become end of life. VA is exploring Apple Native Mail as well as EMM provided solutions and may take a multiple app approach based on business case. The CBA solution must be able to support all of these approaches.

The CBA solution shall be able to support accessibility of the certificate via iOS profile management to support third party VPN solutions. VA currently uses Cisco AnyConnect as its primary VPN client across iOS devices. The solutions shall also be able to be used for authorization for Wi-Fi profiles, and Single Sign On profiles as needed.

5.8.1 INTEGRATION WITH VA’S CURRENT AND FUTURE CERTIFICATE AUTHORITY

The certificate based authentication solution shall integrate with VA’s Certificate Authority. This includes integrating with VA’s future solution when VA migrates in the future. Currently VA is migrating from Secure Hashing Algorithm (SHA)-1 to SHA-256 root certificates. These are Microsoft CA’s hosted inside of VA.

The future solution that VA will migrate to is to use the Department of Treasury’s USAccess solution which will also provide our root Certificate Authority. Treasury uses Entrust’s solution for their root Certificate Authority.

5.8.2 HOSTING OF SOLUTION

If this is a third party solution, and not a core component of the EMM itself, the certificate based authentication solution shall also need to meet the requirements of FedRAMP Moderate and FISMA Moderate.

5.8.3 USAGE OF CERTIFICATE BASED AUTHENTICATION CERTIFICATES ON MOBILE DEVICES

The Contractor shall setup and work with VA to make sure the certificates being generated are interoperable with mobile applications.

5.8.3.1 OFFICE 365

The Contractor shall make sure that the certificate based authentication certificates being generated are able to be consumed by Office 365 for mobile authentication on iOS and Android devices.

5.8.3.2 SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)

The Contractor shall work with VA to ensure that the certificate based authentication certificates being generated are able to be used for S/MIME encryption on the mobile devices for both native mail, as well as third party mobile email solutions such as Good for Enterprise on iOS and Android.

5.9 EMAIL

The Contractor shall provide a working Email delivery system where email is retrieved from VA's current email infrastructure and delivered to devices enrolled in the EMM system. The email delivery must function in VA's two factor environment and provide the following functions:

1. Email application must support Modern Authentication.
2. Certificate Based Authentication
3. Basic Authentication
4. The email application must support sending push notifications to end users.
5. The email application must support running in the background.
6. The EMM provided mail solution must support Azure Rights Management System (RMS).
7. Ability to encrypt with S/MIME
8. RMS Messages
9. Support Email Classification

5.10 MOBILE THREAT PREVENTION AND APP VETTING

The Contractor shall provide a working Malware Detection Solution integrated with EMM functionality, including all licenses and turnkey management. This Malware Detection Solution shall include a mobile threat prevention/Application Analysis tool that meets the following requirements:

1. A web repository of the analysis of applications, including the top 2,500 apps from the iOS and Android stores.
2. The ability for the Government to customize the rating of the applications based on VA's risk designation. These ratings shall include, but not be limited to:
   a. Access to Device Storage
   b. Access to Cloud Storage
   c. Access to Location use
   d. Access to Camera
   e. Access to Photo library
   f. Advertisements
   g. Malware
   h. Communication to application programmer
   i. Communication to outside the United States
   j. Access to contacts
   k. Access to calendar

    l. Trustworthiness of application developer
3. The tool shall have a web based interface.
4. The tool shall integrate into the EMM implementation and shall meet the following performance requirements:
    a. Seamless, already established, integration into VA's current version of EMM.
    b. Ability to recognize when applications are downloaded onto a device.
    c. Send automated alerts to VA designated staff as well as user, if risk rating is higher than VA's threshold.
    d. Automatically remove the application from a mobile device, if risk rating is higher than VA's threshold.
    e. Provide total risk analysis of an application.
    f. Have the capability to take remediation actions when necessary.
    g. Have the capability to send out notification and perform compliance checks in conjunctions with the VA's Enterprise Mobility Manager.
    h. Be an enterprise solution which can perform centralized policy management.
    i. Ability to customize risk rating.
5. The Contractor shall provide training via online web training specific to VA's installation.
6. A solution which can investigate suspicious activity on corporate owned devices.
7. A solution which can research threats in real-time and provide in-depth analysis.
8. A solution which can investigate malicious applications that can threaten highly sensitive mobile infrastructure.
9. A solution which can detect and investigate mobile fraud.
10. A solution which has the capability to understand application behaviors that may harm networks through inefficient use of network and ability to understand app-driven traffic.

Integration services, support and training:

1. The Contractor shall provide on-site setup, installation and end user training of the solution in coordination with OI&T in the base year of the contract.
2. Onsite installation shall be conducted at Hines, IL and completed within 30 calendar days of award.
3. The Contractor shall provide advanced web training for a minimum of five VA IT professionals.
4. This training shall include advanced level installation and operations of the required solution.
5. This training shall be provided within 10 calendar days of completion of the integration services.
6. The Contractor shall provide access to the solutions knowledge base, product manuals, and product admin/user guides.
7. All manuals, admin/user's guides shall be in Portable Document Format (PDF) format.
8. The Contractor shall provide ongoing software product maintenance, upgrades, and support.

9. The Contractor shall provide software updates, hotfixes, and releases.
10. The Contractor shall provide deliver bug fixes and patches
11. The Contractor shall procure and provide to VA any and all required security certificates from a VA Approved Vendor or VA Trusted Vendor as they relate to these associated deliverables.
12. Per NIST guidance, Self-Signed certificates shall not be acceptable.
13. Certificates must be able to support iOS and Android.
14. Technical support provided by telephone 8 a.m. ET to 4 p.m. ET Monday through Friday.
15. Continuous efforts problem resolution engineering upon request for Severity A cases.
16. All software updates, hotfixes, and software releases need to be made immediately available to VA, as well as notification via email on all updates to associated projects.

5.11 FULL DEVICE MIGRATION (OPTIONAL TASK)

This task would only be needed if the Contractor changes the current system in a way that requires current devices to be re-enrolled. If VA chooses to exercise this Optional Task, the Contractor shall perform the following. The Contractor shall provide full, turnkey migration from the current VA EMM cloud service provider and mobile device management software to the Contractor provided cloud hosted EMM solution following the Phase-In Plan and Migration Checklist developed in PWS task 5.1.5. The Contractor shall expand the Plan and Checklist to create a detailed EMM Migration Plan and Procedures for review and approval by the COR outlining Contractor, VA IT, and facility responsibilities for migration.

The Contractor shall provide a full migration of the existing EMM devices to the new EMM solution and App Catalog including all servers, certificates, client agents, console, administrator settings, user setting, profiles, policies, compliance, organizational groups, and EMM settings. The Contractor shall ensure that all pre-provisioning on the server side is done ahead of a user transition.

The Contractor shall be responsible for the migration of all current VA devices to the new EMM solution. VA estimates the number of devices to be migrated at approximately 45,000 at the time of migration with users of varying levels of technical skills. The Contractor shall work with various VA entities to ensure successful migration of all ports, DNS entries, and current policies.

At the conclusion of migration activities, the Contractor shall provide EMM Migration Acceptance Results to validate successful completion of system/data/device migration and standup of the new EMM solution. The Contractor shall complete the full migration from the current VA EMM cloud service provider and mobile device management software to the Contractor provided cloud hosted EMM solution by September 12, 2018.

Deliverables:

A. EMM Migration Plan and Procedures
B. EMM Migration Acceptance Results

5.12 EMM MANAGED SOLUTION – SUPPORT FOR ADDITIONAL CAPACITY AND SCALABILITY (OPTIONAL TASK)

If this Optional Task is exercised by VA, the Contractor shall be able to scale the environment to support up to 55,000 additional devices (for a total of 100,000 devices) as required over the course of the TO. The Contractor shall provide additional EMM solution support as required to match growth in the EMM customer base. The Contractor shall provide hosting, software, hardware, operations, and maintenance support for additional capacity of 5,000 devices for each time the optional task is exercised. The Contractor shall make the additional support available within seven business days of receipt of request. This optional task shall not be exercised more than 11 times throughout the entire PoP of this TO.

5.13 OPTIONAL TASKS FOR EMM USER SUPPORT

5.13.1 EMM TRAINING (OPTIONAL TASK)

If the Optional Task is exercised by VA, the Contractor shall provide an EMM Training Program to train VA users on the EMM. This shall include development of an EMM Training Plan that outlines a structured approach for conducting EMM training and specific schedules for each training event, development and delivery of training materials, and performance of training sessions as described below. The EMM training program shall include in-person training; computer based training and in-person transition training. Following COR approval of the EMM Training Plan, the Contractor shall deliver fully customized course curriculum including EMM Instructor Guides and Student Materials for each course required below and defined in the plan. This Optional Task will be exercised by VA no more than once per year throughout the PoP for a class size of no more than 30 users.

Deliverables:

A. EMM Training Plan
B. EMM Instructor Guides and Student Materials

5.13.2 EMM IN-PERSON ADMINISTRATOR TRAINING (OPTIONAL TASK)

If the Optional Task is exercised by VA, the Contractor shall provide training on its proposed EMM solution for 30 administrators, at Hines, IL. , listed in Paragraph 4.3, Travel. The initial training event shall consist of a three-day session. The training shall include all aspects of the EMM solution, including hosting, operations, and App catalog integration. This Optional Task can be executed up to five times throughout the PoP of the TO.

5.13.3 EMM COMPUTER-BASED TRAINING (CBT) (OPTIONAL TASK)

If the Optional Task is exercised by VA, the Contractor shall provide three EMM CBT Training Modules: one for EMM users, one for the IT support team, and one for administrators. All CBT training modules shall be capable of being used by the following web browsers:

1. Microsoft Internet Explorer (versions 7, 8 and 9)
2. Mozilla Firefox
3. Google Chrome
4. Apple Safari (3 and 4)

The CBT training shall be 508 compliant per paragraph 6.2 of this PWS, and include text, audio and video training for all VA employees including those that are hearing or sight impaired. The training shall be customized to VA.

All CBT materials shall be delivered to the VA PM/COR for verification, acceptance and publication on VA's internal training website.

Deliverable:

A. EMM CBT Training Modules

5.13.4 EMM IN-PERSON TRANSITION TRAINING (OPTIONAL TASK)

If the Optional Task is exercised by VA, VA will require in-person training on EMM operations at the end of the PoP to support transfer and transition of EMM operations. The Contractor shall provide live in-person transition-related training not later than the last 30 days prior to the end of the PoP of this TO. The Contractor shall provide training on its EMM solution for 25 administrators at one designated VA location listed in Paragraph 4.3, Travel. This shall include training of VA administrators so that VA may continue the O&M of the solution.

5.14 CONTRACT TRANSITION: PHASE OUT (OPTIONAL TASK)

If the Optional Task is exercised by VA, the Contractor shall support transition activities including phase-out services to ensure continuity of services for up to 60 days prior to expiration of the effort. The Contractor shall provide support services to the incoming Contractor or Government entity for EMM migration from the current solution and to any future VA/Cloud/EMM environment.

The Contractor shall deliver phase-out services as described below:

1. **Phase-Out Plan**: All or any part of the EMM solution and environments utilized under this TO may require migration to a new EMM, and/or future cloud service provider (Government or Contractor) or VA entity, due to expiration or termination of this TO or for any other reason at the sole discretion of VA. The Contractor shall provide an overall plan describing the specifics for the phase-out. All

migration actions shall be completed prior to the expiration or termination date of this TO. The Phase-Out Migration Plan shall address the following areas:

a. An inventory and migration of historical data (generally, Virtual Machine (VM) definitions and configurations) relating to the specific EMM.
b. Techniques for ensuring that all retrieved data supplied is provided in the original or other VA agreed-upon format.
c. Procedures to migrate all current VA mobile devices from enrollment in the current EMM to the new EMM.
d. Procedures to migrate/recreate all server settings, profiles, communication channel, compliance settings, console settings from the current EMM to the new EMM.

2. 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 in accordance with NARA requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization.
3. Providing an orientation phase to introduce the successor (EMM/future cloud service provider) personnel, programs, and users to the incoming team, explaining tools, methodologies, and business processes.
4. Providing the Contractor’s strategy and planned approach for personnel staffing and training during the transition period to a new provider shall begin upon exercise of this optional task.
5. Providing a Phase-Out Migration Checklist (Contractor format).
6. Providing signed turnover agreements.
7. The Contractor shall coordinate with the COR during the last 60 calendar days of the effort to transition all environments, applications, configurations and data residing on the managed EMM solutions to VA or VA designated site.
8. The Contractor shall provide copies of EMM data in a format that is exportable by the Contractor and importable by VA and partners at the replacement site in Secure Export Data Files.
9. The Contractor shall deliver white glove transfer of existing tapes from the current storage location to a VA Medical Center (Hines, IL or Albany, NY) or the replacement Contractor’s storage facility as required by VA.

Deliverables:

A. Phase-Out Plan including Migration Checklist
B. Secure Export Data Files

5.15 OPTION PERIODS ONE THROUGH FOUR

If Option Period is exercised by VA, all tasks in the following sections and sub-sections shall apply: 5.1 Project Management (except 5.1.2 Technical Kickoff Meeting), 5.3 EMM Managed Solution, 5.6 Ongoing EMM Managed Solution Technical Support, 5.7 Operations and Maintenance, 5.8 Certificate Based Authentication, 5.9 Email, 5.10 Mobile Threat Prevention and App Vetting, and if exercised optional tasks 5.11 through 5.14 including all subparagraphs.

6.0 GENERAL REQUIREMENTS

6.1 PERFORMANCE METRICS

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

Performance Objective	**Performance Standard**	**Acceptable Levels of Performance**
A. Technical / Quality of Product or Service	1. Shows 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. Quick response capability 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 TO 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 QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.2 SECTION 508 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

The following Section 508 Requirements supersede Addendum A, Section A3 from the T4NG Basic PWS.

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

☒ § 1194.21 Software applications and operating systems
☒ § 1194.22 Web-based intranet and internet information and applications
☐ § 1194.23 Telecommunications products
☐ § 1194.24 Video and multimedia products
☐ § 1194.25 Self-contained, closed products
☐ § 1194.26 Desktop and portable computers
☒ § 1194.31 Functional Performance Criteria
☒ § 1194.41 Information, Documentation, and Support

6.2.1 EQUIVALENT FACILITATION

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

6.2.2 COMPATIBILITY WITH ASSISTIVE TECHNOLOGY

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

6.2.3 ACCEPTANCE AND ACCEPTANCE TESTING

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment.

Deliverable:

A. Final Section 508 Compliance Test Results

6.3 SHIPMENT OF HARDWARE OR EQUIPMENT

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Ship To and Mark For:

	Primary		Alternate
Name:	Punit Patel	Name:	Saleem Newsome
Address:	Edward Hines Jr. VA Hospital 5th Ave & Roosevelt Rd Building 37 – Room 128 Hines, IL 60141-7008	Address:	Albany OIFO 113 Holland Ave Albany, New York 12208
Voice:	(708) 786-7850	Voice:	518-449-0655
Email:	Punit.Patel@va.gov	Email:	Saleem.Newsome@va.gov

Special Shipping Instructions:

Prior to shipping, Contractor shall notify Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of hardware to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall bear the VA IFCAP Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO number shall indicate total number of containers for the complete shipment (e.g. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: ____________ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))
Project Description: (e.g. Tier I Lifecycle Refresh)

Total number of Containers: Package ___ of ___. (e.g., Package 1 of 3)

APPENDIX A: EMM CAPABILITIES

Provisioning:

1. Ability to set a Target Platform (Apple, Android, etc.) for profile provisioning
2. Ability for Target Device Model to be used for profile provisioning
3. Ability for Target Minimum Operating System to be used for profile provisioning
4. Ability for Target Device Ownership (GFE, Personal etc.) to be used for profile provisioning
5. Ability to set Profile Removal Permission
6. Ability to edit any provisioning field for a "live" or "active" profile
7. Ability to enroll a device before applying any policy
8. Ability to provision a device as either a shared device or a single user device
9. Ability to provision iOS devices with Apple configurator
10. Ability to provision iOS devices via Apple Device Enrollment Program procedures where users do not have known password (via six digit PIN in lieu of username and password)
11. Ability to stage a mobile device to a preset configuration prior to end user enrollment.
12. Ability to stage mobile devices using Apple Configurator utility
13. Ability to integrate with Apple's Device Enrollment Program to support pre-enrollment of devices
14. Ability to provision a device using the EMM agent
15. Ability to provision a device "agentless"
16. Ability to provision a device remotely via a web enrollment on the remote device
17. Ability to provision a device into "locked down/single app" state
18. Ability to use VA Active Directory environment to import and synchronize user account details for end user enrollment
19. Ability to set a default Device Ownership type upon enrollment for different groups
20. Ability to use internal User list for enrollment for different groups
21. Ability to set support email and phone information for registration messages for different groups
22. Ability to edit an enrollment activation notification message to the user or group of users (email and/or SMS)
23. Ability to send a user or group an activation enrollment message (email)
24. Ability to perform and manage bulk enrollments

Security:

1. Ability to create Whitelist for device enrollment to include specific iOS devices as well as other operating system models and configurations
2. Ability to restrict enrollment to known users when needed
3. Ability to use an Active Directory user repository for enrollment

4. Ability to view the current Global Positioning System (GPS) location of devices on a map
5. Ability to remotely lock a targeted device by manual process and by automated compliance rules
6. Ability to add/edit the Certificate Authorities available for profiles
7. Ability to view and add/edit the Certificate Authorities for a group
8. Ability to view and add/edit the Certificate templates based on group membership
9. Ability to deliver multiple Credential payloads per profile
10. Ability to deploy certificates with one or many profiles
11. Allow multiple Simple Certificate Enrollment Protocol (SCEP) configurations per profile
12. Ability to execute a corporate wipe when a device has a disallowed operating system
13. Ability to execute full device wipe when a device has a disallowed operating system
14. Ability to enforce a passcode policy on the device
15. Ability to determine if an enrolled device is encrypted
16. Ability to wipe device after set number of invalid attempts
17. Ability to natively detect, report, and alert on compromised devices and take action based upon compliance rules (to include jailbroken, rooted, etc.)
18. Ability to report application inventory on devices
19. Ability to determine which user/admin made a configuration change
20. Ability to determine which user/admin made a configuration change to a profile
21. Ability to configure each Exchange ActiveSync profile/configuration for a device to use a certificate
22. Ability to configure each Wi-Fi profile/configuration for a device to use a certificate
23. Ability to configure each VPN as well as Cisco AnyConnect profile/configuration for a device to use a certificate
24. Ability to proxy SCEP requests for device certificates
25. Ability for the EMM to act as a proxy for an Enterprise’s Certificate Authority
26. Ability for the EMM to act as an intermediate Certificate Authority for the main root enterprise Certificate Authority
27. Capable of enforcing enrolled devices to set and use complex passwords for device authentication. Minimum requirements are six characters with numeric or alphanumeric, special characters, and upper/lower case.
28. Capable of enforcing enrolled devices to set and use password timeout after inactivity (e.g. device passcode must be used after 15 minutes of inactivity)
29. Ability to limit maximum password attempts as well as actions based on too many incorrect attempts in a row (e.g. enrolled device will be full device wiped after 10 incorrect attempts.)
30. Ability to Enterprise/Corporate Wipe a remote device from the EMM console. Remote Enterprise/Corporate Wipe command securely deletes all EMM managed corporate data (personal user data, pictures etc. not erased)

31. Ability to deploy FIPS 140-2 compliant container for secure storage of corporate data on devices. Ability to update and edit content inside of secure container with ability to synchronize back to the corporate network OTA.

Profile:

1. Ability to create a profile that isn't used (e.g. draft and or inactive profiles)
2. Ability to edit a "live" or "active" profile
3. Ability for an edited profile to automatically push and install to devices that currently have the profile
4. Ability to determine devices that don't have a profile applied and automatically push the profile to those devices
5. Ability to push a profile to any individual qualifying device
6. Ability to automatically remove profiles from devices whose state move from qualifying to not. This happens as a result of changing a profile to be more exclusive.
7. Ability to support multiple profiles being applied to a single device
8. Ability to delete a profile
9. Ability to set a description for a profile
10. Ability to manage all passcode settings made available by all versions of Apple iOS via an EMM policy
11. Ability to manage all passcode settings made available by Android 4.2 and higher via an EMM policy
12. Manage the following via a profile: Require passcode on device and define length and content
13. Manage the following via a profile: Grace period for device lock
14. Manage the following via a profile: Maximum failed log in attempts
15. Manage the following via a profile: Allow installing apps
16. Manage the following via a profile: Control use of camera
17. Manage the following via a profile: Control use of FaceTime
18. Ability to support Samsung Knox profile settings for Android devices
19. Allow multiple Wi-Fi configurations for multiple profiles
20. Ability to manage device Wi-Fi settings via an EMM policy
21. For a profile: Support Wi-Fi Security Type: None, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)/WPA2, Enterprise (any)
22. For a profile: Ability to support multiple VPN configurations for a profile
23. For a profile: Support VPN Connection (or Policy) Type: IP Security (IPSec) (Cisco), Cisco AnyConnect, Juniper SSL, FS SSL, and Custom SSL
24. For a profile: Ability to support a VPN connection Proxy for a VPN configuration and support for per-app VPN
25. Allow multiple Web Clip configurations per profile
26. Ability to manage profiles to devices across an enterprise size organization, without relying on Active Directory user groups
27. Ability to exclude devices and locations from receiving certain profiles
28. Ability to create interactive profiles
29. Ability to manage application

30. Ability to convert an unmanaged application into a managed application.

Management:

1. Ability to stop managing a device by removing its profile
2. Ability to offer support for ruggedized devices and full remote control and management of Windows Mobile and Windows CE devices
3. Ability to see message or communication details between the device and the EMM
4. Ability to wipe/reset a remote device
5. Ability to determine the number of qualifying devices a profile will apply to
6. Ability to wipe/reset a remote group of devices by logical grouping such as type of devices, iOS, or assigned groups
7. Ability to determine the number of qualifying devices a profile is currently applied to
8. Ability to display a group of devices (or any type of logical grouping such as user, ownership, grouping, profile, compliance status, etc.)
9. Ability to see details on the qualifying devices a profile will apply to
10. Ability to display identity and display which profiles and certificates are on a device
11. Ability to review the GPS history of a device
12. Ability to clear the passcode to a targeted device
13. Ability to sign profiles for individual and groups
14. Ability to encrypt profiles
15. Ability to edit the Device Sample time for application, certificate, profile, and compliance
16. Ability to search for a device or group of devices by User ID, serial number, ownership, or other logical parameter
17. Ability to see a detailed list of daily device cellular usage for selected location group(s) within a selected time frame for devices that are on Wireless WAN
18. Ability to see a detailed list of devices that have been inactive for a selected number of days for selected group(s)
19. Ability to create new granular/custom roles for administration of the EMM and provide the ability to edit the permissions for the existing roles
20. Ability to grant access to an administrator at an organizational level
21. Ability to create new granular/custom roles for users of the EMM and provide the ability to edit the permissions for the existing roles
22. Ability to create user's account by querying Active Directory
23. Ability to create basic accounts
24. Ability to group, manage, and enroll devices in specific location groups within a multi-tenant structure
25. Must be able to provide granular permissions to solution console. Enterprise, geographic Regions, Site levels must be configurable to allow certain permissions for each level
26. Ability to create manageable exclusions for policies, profiles, and settings by using VA defined enterprise groups through smart groups or similar technology

27. Provide a high level view of all devices with ability to drill to the device level
28. Provide Enterprise Scalability - creation of role-based groups for device management and the means to manage those devices through smart groups or similar technology
29. Support Secured Console Access - credentials integrated with Directory Services Authentication and Two Factor Authentication that support One Time Passcode devices (meeting the requirements of NIST SP 800-63 Level 3)
30. Track changes made to devices for auditing/reporting and provide a method to view changes made by administrators
31. Provide white/black list functions for devices and applications
32. Support 100,000 concurrent Exchange ActiveSync users
33. Interface with Apple App Store and Google Play Store to limit application selection
34. Ability to interface with VA's current hybrid 2010/Office 365 exchange mail and provide email filtering to allow email to authorized devices while preventing email to non-authorized devices
35. Ability to interface with higher versions of Microsoft exchange and Office 365 as VA transitions to those platforms
36. Ability to allow enrolled devices in the EMM to have access to a secure container to view and edit content directly on the mobile devices.
37. Ability to allow secure content locker to integrate with Microsoft SharePoint 2007 and higher
38. Ability to allow secure containers to edit documents on Microsoft SharePoint 2010 and higher directly on mobile devices. Ability to access personal and team share drives.
39. Supported on multiple operating system platforms (iOS, Android, and Windows Phone 8)
40. Ability to set storage quota
41. Must be FIPS 140-2 compliant
42. Ability to collaborate with external users.

Compliance:

1. Ability to set up compliance rules to include custom compliance rules for profiles, devices, groups, and whitelist/blacklist
2. Ability to activate/deactivate a compliance rule
3. Ability to detect when a device is not in compliance
4. Ability to detect when a device has been compromised.
5. Ability to notify administrators when a device has been marked as non-compliant.
6. Ability to notify the user when their device has been marked as non-compliant
7. Ability to take an action when a device is found to be out of compliance (actions include an alert, email, device lock, wipe, disable active synch, disable wireless and VPN access, removal of Enterprise App Store, etc.)
8. Ability to escalate to further actions when a device remains out of compliance for an extended period of time
9. Ability to specify application information for an application compliance rule

10. Ability to execute a corporate wipe when a device is compromised
11. Ability to execute a standard wipe when a device is compromised
12. Provide enterprise level compliance reports, including lost/wiped/inactive devices, the number of devices total, the number of devices active, how much data is sent/received by devices, connection type
13. Ability to create inclusions and exclusions for logical or geographic groups in order to handle different compliance needs
14. Ability to set up compliance actions based on device physical location (geofencing)
15. Ability to set up compliance actions based on time or date the device last checked in
16. Ability to assign a rank to any application downloaded (top 10,000 apps on iOS, Android, and Windows app stores).
17. Ability to report on any application that is above VA's approved risk rating

Reporting:

1. Ability to run reports by established parameters and device, profile, provision details, and compliance
2. Ability to create and view by compliance standards
3. Ability to subscribe to a Report based on parameters
4. Ability to schedule a Report based on parameters
5. Ability to print a Report using a printer
6. Ability to print a Report to a file
7. Ability to report on devices that haven't communicated to the EMM in a period of time
8. Ability to report full compliance status details of devices under EMM
9. Ability to view overall health of mobile environment in HTML5 dashboards from tablets or mobile devices
10. Ability to automatically pull dashboard metrics from EMM to other internal VA dashboards
11. Ability to create custom reports or modify existing reports

Mobile App Deployment:

1. Ability to add a public app to the Enterprise App Store
2. Ability to offer Integrated Enterprise App Store without the use of a third party
3. Ability to add an enterprise app to the Enterprise App Store via a graphical user interface (GUI)
4. Ability to add additional metadata to and report on metadata on any app added to the Enterprise App Store (e.g. - name, description, version, operating system, keywords, etc.)
5. Ability to specify the effective date for an internal app
6. Ability to specify the expiration date for an internal app
7. Ability to specify the minimum operating system and model for an internal app
8. Ability to download internal and public apps from Enterprise App Store

9. Ability for EMM to facilitate and distribute applications via the Apple Volume Purchase Program
10. Ability to add a public app to the Enterprise App Store via a GUI
11. Ability to specify the name and Uniform Resource Locator (URL) for a public app
12. Ability to specify a public app's platform as Android, Apple and Windows Mobile
13. Ability to specify the location, icon and comments for a public app
14. Ability to specify a public app's reimbursable status as Reimbursable, Not Reimbursable and Undefined
15. Ability to add an internal app to the Enterprise App Store via a GUI
16. Ability to specify the name for an internal app
17. Ability to specify the application ID and internal ID for an internal app
18. Ability to specify the description, current version and platform for an internal app
19. Ability to specify an internal app's platform as Android, Apple and Windows Mobile
20. Ability to specify the minimum operating system for an internal app
21. Ability to specify an internal app’s model based on device model type
22. Ability to specify the category for an internal app as the following: Book, Business, Education, Entertainment, Finance, Games, Healthcare & Fitness, Lifestyle, Medical, Music, Navigation, News, Photography, Productivity, Reference, Social Networking, Sports, Travel, Utilities
23. Ability to specify an internal app’s importance as Low, Normal or High
24. Ability to specify an internal app’s sensitivity as Low, Normal or High
25. Ability to specify the location and keywords for an internal app
26. Ability to specify the effective and expiration date for an internal app
27. Ability to specify whether an internal app uses encryption
28. Ability to specify end-user license agreement text for an internal app
29. Ability to specify an icon for an internal app
30. Ability to specify screenshots for an internal app inside the Enterprise catalog
31. Ability to view defined public applications (App Store/Play store apps)
32. Ability to view defined internal applications (Enterprise apps)
33. Ability to download public apps through App Store/Play store
34. Ability to view metadata for internal apps
35. Ability to download internal apps
36. Ability to view required and available apps
37. Ability to view available updates for internal and public apps
38. Ability to display app version, app publisher and app update date
39. Ability to audit downloads
40. Ability to filter apps by category, operating system version and operating system type, device type
41. Ability for a user to rate and review an app
42. Ability to download content other than apps (audiobooks, PDFs, etc.)
43. Compatible with Apple, Android, and Windows mobile devices
44. Ability to segment application management for different groups
45. Ability to segment internal and external approved apps
46. EMM shall be able to selectively deliver corporate apps to the tablet
47. EMM shall be able to selectively wipe corporate apps from the tablet

48. EMM must be able to prevent access to operating system app store (App Store/Play Store while still providing access to enterprise apps)
49. EMM shall be able to run in background while other apps are run
50. EMM shall be able to selectively update corporate apps

Operational Efficiency:

1. EMM shall be able to enforce enterprise rules while allowing regional/local enrollment, reporting, management, and compliance activities
2. Ability to take an AUTOMATED action when a device is found to be out of compliance (actions could include an alert, email, device lock, wipe, etc.)
3. Ability to create unique Device Blacklists for different groups (or any type of logical grouping). Organization or Smart groupings are an example
4. Ability to run reports based upon blacklist devices
5. Ability for system to require user to have read policy and acknowledge terms of use agreement for enrollment
6. Ability to set support email and phone information for registration messages
7. Ability to set a URL to redirect user to upon successful enrollment
8. Ability to edit an enrollment activation notification message to the user (email)
9. Based upon violation of established compliance rules have the automated ability to wipe/reset a remote group of devices by logical grouping such as type of devices, iOS, or assigned groups
10. Ability to review the GPS history of a device and see the GPS history of a device on a map
11. Ability to take the following action upon a group of devices from a search: Reassign to a different Organization and/or Smart Group (any type of logical grouping)
12. Ability to assign Profile to one or many Groups (any type of logical grouping). Organizational or smart groupings are an example
13. Ability to integrate with the Apple Application Volume Purchasing Program
14. EMM has ability to run reports by groups of users to include location
15. EMM solution offers a SDK Framework and app wrapping to integrate with existing or future Enterprise Applications
16. Must be able to support all licenses from a single server instance/copy of the software (without logging into multiple environments)
17. Solution must be monitored from industry standard tools (e.g. Hewlett-Packard (HP) OpenView, System Center Operations Manager (SCOM), etc.)
18. Solution shall be highly available and have a disaster recovery/redundancy strategy
19. Solution must be able to be installed on existing servers and database clusters if needed
20. Solution must support 100,000 mobile devices with the ability to expand
21. Solution must integrate and issue certificates from your internal public key infrastructure (PKI) system to mobile devices as well as third party public PKI providers such as VeriSign.

22. The Contractor must provide all certificates from an approved VA certificate vendor, and must manage these certificates in compliance with VA policies through the life of the TO. This includes procurement of new certificates and renewal of current certificate.

Email:

1. Solution must function using VA's current exchange environment consisting of a hybrid 2010/Office 365 using ActiveSync
2. Solution must include functionality to support 2010 and Office 365
3. Solution must support certificate based authentication as detailed in the Certificate Based Authentication sections
4. Solution must support moderate authentication from Microsoft.
5. Solution must be able to allow email to EMM devices, while preventing email to non-authorized devices
6. Solution must provide intelligent filtering based on EMM compliance settings
7. Capability of device identification to ensure authorization prior to connection to ActiveSync connections
8. Solution must provide email for iOS, Android, Windows phone 10
9. Must be able to read/sign (Encrypt and Signed) messages that use PKI/S/MIME encryption
10. Ability to support iOS per-message encryption
11. Ability to support and configure third party E-mail applications

Certificates and Self-Service Portal:

1. Solution must interact with VA’s internal Certificate Authority to request and push certificates to the devices
2. Solution must support certificate based authentication
3. Solution must have the ability to revoke and renew a certificate
4. Solution must support two factor authentication to the Self-Service Portal using a PIV card
5. Solution must have the ability for a Self-Service Portal