**Mobile Services Category Team (MSCT)**

**Enterprise Mobility Management**

**MDM/MAM/MCM**

**Functional Requirements Document - FRD**

May 2019

1 Introduction 4

1.1 Background 4

1.2 Objective 6

1.3 Approach to EMM -- MDM/MAM/MCM Acquisitions 6

1.4 Overview 6

1.5 Solution Security 6

1.6 Solution Requirements 7

1.6.1 Mobile Device Management (MDM) 7

1.6.1.1 MDM Detailed Requirements 7

1.6.1.2 Additional MDM Requirement Descriptions 16

1.6.1.2.1 FISMA Requirements 16

1.6.1.2.2 FIPS Requirements 17

1.6.1.2.3 Containerization 17

1.6.1.2.4 IPv6 Support 17

1.6.1.2.5 User Authentication / Web Management 17

1.6.1.2.6 User Compliance 18

1.6.1.2.7 Alerts and Notifications 18

1.6.1.2.8 Data Collection 19

1.6.1.2.9 Inventory Management 19

1.6.2 Mobile Application Management 20

1.6.2.1 MAM Detailed Requirements 20

1.6.2.2 Additional Descriptive Mobile Application Management Requirements 22

1.6.2.2.1 (Optional) MAM Software Integration Services 22

1.6.2.2.2 Application Deployment 22

1.6.2.2.3 Mobile Application Store (MAS) 22

1.6.2.2.4 Mutual Authentication 23

1.6.2.2.5 Application Installation Control 23

1.6.2.2.6 Blacklisting / Whitelisting 23

1.6.2.2.7 Application Environment Requirements 23

1.6.2.2.8 Application Signing 23

1.6.2.2.9 (Optional) Third-Party Application Mutual Authentication 23

1.6.3 Mobile Content Management 24

1.6.3.1 MCM Detailed Requirements 24

1.6.3.2 Additional Descriptive MCM Requirements 24

1.6.3.2.1 Privacy 24

1.6.3.2.2 Continuity of Operations and Disaster Recovery 25

1.6.3.2.3 File Management 25

1.6.3.2.4 Personal Information Management 25

1.6.3.2.5 Security Content Automation Protocol (SCAP) Support 25

1.6.3.3 Audit and Reporting Detailed Requirements 26

1.6.3.4 Additional Descriptive Audit and Reporting Requirements 27

1.6.3.4.1 Device Inventory Reports 27

1.6.3.4.2 System Performance Reports 27

1.6.3.4.3 MDM Security / Compliance Reports 28

1.6.3.5 (Optional) Quality of Service (QoS) 28

1.6.3.5.1 (Optional) Classified Data 28

1.6.3.5.2 PIV / CAC Support 29

1.6.3.5.3 (Optional) Biometric Support 29

1.6.3.5.4 (Optional) Network Monitoring 29

1.6.4 Service Delivery Model 29

1.7 Support Requirements 30

1.7.1.1 Project Management 30

1.7.1.2 Deployment / Migration / Transition 30

1.7.1.3 Enterprise Systems Integration 31

1.7.1.4 Training 31

1.7.1.5 Help Desk 31

1.7.1.6 Demonstration Platform 31

1.7.1.7 (Optional) Enterprise Configuration 31

1.7.1.8 (Optional) Integration with FSSI Wireless Portal 32

1.7.1.9 (Optional) Telecommunications Expense Management System (TEMS) 32

1.7.1.10 (Optional) Device Replacement / Refresh 32

1.7.1.11 (Optional) Device Disposal & Reporting 32

2 Pricing 33

# Introduction

## Background

The Federal Government is becoming increasingly reliant upon mobility, now with approximately 1.5 million mobile devices in service costing the government over $1 billion annually for service alone. Mobility usage across the government has a wide range of diverse profiles from general business use to mission critical, high security. There is an increasing need for the Federal Government’s mobile device management processes to be further improved due to increased security risks and broader use of mobile solutions.

The Category Management Leadership Council (CMLC) and the Office of Management and Budget (OMB) established and began the implementation of a Category Management strategy across the federal government identifying 19 Common Government Spending Categories. In 2016, OMB established the Mobile Services Category Team (MSCT), made up of Agency representatives across the Federal Government, to address cross-government requirements for next generation mobility. The MSCT is tasked with, among other responsibilities, establishing requirements for both core and sub-components of mobility. As such, it is the responsibility of the MSCT to establish the minimum baseline Enterprise Mobility Management requirements.

The primary purpose of this document is:

* State the minimum set of requirements across the Federal Government for Mobile Device Management, Mobile Application Management, and Mobile Content Management under the broader umbrella of Enterprise Mobility Management (EMM)

This document establishes minimum EMM requirements government-wide. Individual agencies determine the full extent of requirements for their respective device management, security needs, and mobility software. Within this context, it is also important for the Federal Government to continue to reduce costs and both improve and simplify the acquisition process for mobility and related services.

This requirements document includes documentation from the previous Managed Mobility RFTC solicitation in 2013 as well as a previous Department of Homeland Security 2015 DHS mi-5 Enterprise Mobile Device Management Baseline Initiative Report. The DHS report development included a thorough process of documenting and assessing DHS Component Agency needs and requirements for MDM and app management to establish an Enterprise MDM Baseline.

This FRD differs from the DHS mi-5 Enterprise Mobile Device Management Baseline Initiative Report in that the DHS report has a primary focus upon MDM and security due to its purpose of addressing DHS managed devices. The requirements identified within the FRD included more in the areas of MAM and MCM. The intent of this document is to provide a broad approach and minimum requirements across MDM, MAM and MCM. However, it would be both a redundancy in process and inefficient use of resources not to use findings from the DHS report and the RFTC to establish government-wide EMM requirements. Government agencies that contributed requirements information to the DHS baseline included CBP (Customs and Border Protection), FEMA (Federal Emergency Management Administration), ICE Immigration and Customs Enforcement, HQ CISO (Headquarters – Chief Information Security Officer), HQ ITSO (Headquarters - Information Technology Services Office), TSA (Transportation Security Administration), USCG (United States Coast Guard), and USCIS (United States Citizenship and Immigration Services).

This document has three primary components as a part of the Enterprise Mobility Management (EMM) across the Federal Government:

1. Mobile Device Management (MDM)
2. Mobile Application Management (MAM)
3. Mobile Content Management (MCM)

This document also specifies a set of optional services contained within each.

The EMM solutions must meet a broad set of requirements that address the following set of criteria:

* 1. Qualified Secure, Scalable Solutions – Technical solutions that address the existing mobile device, application, and content management needs of government mobile technology including minimum level security and policy management. The solutions shall have the ability to scale to the extremely large and evolving nature of federal government cabinet-level agency organizations.
  2. Evolutionary and Flexible – The management needs of the Federal Government Mobility are evolving with increased mobile adoption, new mobile applications, enhanced needs for remote access, and emerging policy and security requirements in an increasingly threatening external environment. As a result, the solutions will continue to assess future requirements to ensure the ongoing Federal Government needs of MDM, MAM, and MCM are adequately met. The MSCT intends to re-assess both the Enterprise Mobility Management requirements and solution providers on a periodic basis in response to mobility evolution. This will provide government agencies with on-going, updated qualified solution providers.
  3. Shared Mobility Community – The solution providers are expected to monitor and bring forth new industry developments, identify Managed Mobility best practices in both industry and government, and to present these best practices to government. The Managed Mobility space is in a state of rapid change, making it challenging and resource-intensive for agencies to stay properly informed and to adequately maintain and manage mobility within their respective agencies.

By centralizing requirements gathering, establishing government-wide minimal requirements, and conducting solution assessments; the MSCT intends to reduce the burden on agencies while increasing the quality of their options.

## Objective

The Federal Government must address agency’s mission needs in a secure, cost-effective manner. This objective is driven by the MSCT as directed by The Office of Management and Budget (OMB). Enterprise Mobility Management is a core capability for effectively scaling the secure deployment and management of mobile devices, mobile applications, enterprise data on mobile devices, mobile security, and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to government agencies.

The MSCT defines the functional framework, and Government agencies should be able to work with all components of the framework seamlessly in an easy to use, secure, integrated solution. For example, if a user reports losing a device, the IT device manager should be able to enter the user name, retrieve the device ID, disable it, and notify the network provider to stop service and billing – all within a single interface. A proposed mobility solution set may incorporate multiple tools due to the complexity of the requirements and the rapid evolution of the managed mobility marketplace.

Since mobile security covers a broad spectrum of requirements and services, this document does not specifically include mobile security as a standalone set of requirements except as it pertains to the securing of devices through MDM and data through MAM and MCM.

## Approach to EMM -- MDM/MAM/MCM Acquisitions

This requirements document identifies EMM (MDM/MAM/MCM) platform(s) capable of satisfying the government’s device, applications, and content management needs specified and developed by the Mobility Services Category Team. It is recommended that individual agencies use this set of minimum guidelines, add any additional requirements to meet specific needs of their respective Agency and then, obtain provider information and capabilities to meet the entire set of MDM, MAM, and MCM needs. When agencies obtain information and capabilities from service providers it is also recommended that Agencies request that the providers map their offerings to the government acquisition vehicles to streamline the acquisition process.

## Overview

Enterprise Mobility Management, as previously stated, is a service portfolio of mobile device management, mobile application management, and mobility content management. The baseline requirements of each are shown separately under their respective category headings and subsections.

## Solution Security

While security is not a specific requirement category to itself for the purposes of this requirements document, security is both implied and evident within many of the individually stated technical requirements. Security must be addressed through data at rest encryption, data in transit encryption (VPN), and secure applications, which are included in the requirements for the EMM: MDM-MAM-MCM solution. The solution requirements may be met through separate products, which are then integrated into the complete EMM: MDM-MAM-MCM solution.

## Solution Requirements

### Mobile Device Management (MDM)

#### MDM Detailed Requirements

MDM refers to device management and other mobile management functions that control the mobile device and the activities that may be performed on the device. It is recognized that MDM may be on the device or in some product frameworks may also be in the cloud.

Below is a set of detailed MDM requirements, each marked as either Critical (C) – the solution *shall* meet this requirement or Important (I) – the solution *should* meet this requirement or be a future feature of the solution. The detailed requirements are then followed by a series of additional descriptive requirements (indicated as either optional or required), which should also be evaluated by Agencies in assessing their overall needs.

Table 2.5.1

|  |  |  |
| --- | --- | --- |
| **#** | **MDM Requirement** | **Priority** |
| 1 | The solution shall offer support for the use of Microsoft Active Directory (AD) as its user information repository (This is a specific DHS requirement; There may be different repositories also to be supported for other Agencies) | C |
| 2 | The solution shall be capable of connecting to and using multiple AD forests for different user populations. | C |
| 3 | The solution shall support a Role-based Access Control (RBAC) model whereby users are assigned roles, which authorize them to perform non-privileged (e.g., user self-service) or privileged (e.g., device enrollment, policy definition, or view usage, logs, and GPS data) actions. | C |
| 4 | The solution shall support the automated assignment of roles to users based on group memberships in an enterprise Lightweight Directory Access Protocol (LDAP) directory service. | C |
| 5 | The solution shall offer support for policies to control native device screen capture capabilities. | C |
| 6 | The solution shall support a “de-centralized” administration model, whereby administrators may be granted administrative privileges within a limited scope or partition of the system (e.g., enabling control of an organizational unit within the organization). | C |

|  |  |  |
| --- | --- | --- |
| **#** | **MDM Requirement** | **Priority** |
| 7 | The solution shall support policies to lock or automatically erase all or select enterprise data from the device under the following conditions:  • The device is running an unsupported operating system or version  • The user has exceeded a threshold of failed authentication attempts  • The device has not contacted the MDM server for a configurable time interval • The device OS has been compromised or “jailbroken”  • The device is in violation of configuration policies  • The device is in violation of configuration policies For container solutions, deletion of the container storage is sufficient.  Removable storage must also be wiped, unless the solution provides other safeguards preventing the storage of enterprise data on removable devices. | C |
| 8 | Both the MDM server and enrolled mobile devices must display the required system use notification banner to all users attempting to authenticate to the system. | C |
| 9 | The solution shall support policies to configure an inactivity lock interval for the device screen (or the container) after which the user will be required to re-authenticate. | C |
| 10 | The solution shall support policies to control the display of message/alert notifications on the device lock screen. | C |
| 11 | The solution shall allow the user to place emergency calls (e.g., 911) without unlocking the device. | C |
| 12 | The solution shall support one or more remote access mechanisms such as a VPN (provided either device-wide or to apps within a container) or an access gateway provided by the MDM server. | C |
| 13 | The solution shall support policies requiring the use of VPN for packet data. For whole-device solutions this should apply to all network traffic sent by the device; for container solutions, it should apply only to apps inside the container. | C |
| 14 | The solution shall offer support for policies to disable cellular data connections. | C |
| 15 | The solution shall offer support for policies to disable Wi-Fi. | C |
| 16 | The solution shall offer support for policies to disable Bluetooth. | C |
| 17 | The solution shall offer support for policies to disable wireless access point (“hotspot”) functionality. *(Note: Security requirement added to baseline)* | C |
| 18 | The solution shall offer support for policies to configure Wi-Fi security settings, including specifying known enterprise networks, provisioning network credentials, and selecting supported wireless security protocols. | C |
| 19 | The solution shall offer support for policies to restrict the use of Bluetooth profiles and to require the use of encrypted Bluetooth connections. | C |
| 20 | The solution shall offer support for the grouping of devices into logical groups, and the application of policies and other security settings to devices based on these groups. | C |
| 21 | The solution shall support policies to require specific apps (e.g., anti-malware) to be installed on registered devices. | C |
| **#** | **MDM Requirement** | **Priority** |
| 22 | The solution shall provide at-rest encryption of data stored on enrolled devices either by encrypting all local storage, or through the use of an encrypted container protecting all enterprise applications and data. | C |
| 23 | The solution shall provide the ability to monitor and restrict the use of OS-native cloud-based data storage, backup, and synchronization services. | C |
| 24 | The solution shall support the configuration of profiles by user group/role and assignment of policies and apps specific to that role. | C |
| 25 | The solution shall support configuration of allowed user remote self-service actions including the ability to lock, locate, track, and wipe content on the user's device. | C |
| 26 | The solution shall create audit records of security-relevant actions on the device, to include password changes, failed authentication attempts, and connections to enterprise resources. | C |
| 27 | The solution shall create audit records of access to the administrative console and all administrator actions such as policy definition and modification, manual requests to wipe devices, and modifications to device and user information. | C |
| 28 | Audit records shall contain at a minimum the event ID, timestamp, location information, event source, event description, and identity of the device and, if known, the user. | C |
| 29 | To enable event log correlation, the solution shall support synchronizing both the MDM server(s) and managed devices with agency designated Network Time Protocol (NTP) server. | C |
| 30 | The solution shall control access to audit records in order to preserve the confidentiality and integrity of audit data. | C |
| 31 | The solution shall protect logs against unauthorized modification (e.g., through the use of digital signatures). | C |
| 32 | The solution shall protect the confidentiality and integrity of audit records and reporting information transmitted from devices to the MDM server. | C |
| 33 | The solution shall meet all security control requirements of the Digital Government Strategy Federal Mobile Computing Security Baseline. While many controls will depend on implementation details and not be provided directly by the solution, the design of the solution must not preclude or impede implementation of any of the baseline controls. | C |
| 34 | If the solution is provided as a cloud service offering, it must be granted an Approval to Operate (ATO) through the GSA FedRamp program. | C |
| 35 | The solution shall produce hardware and software asset inventory reports for enrolled devices. | C |
| 36 | The solution shall monitor devices and report compliant and non-compliant settings to the MDM server. The solution shall automatically configure the defined settings to the extent possible. | C |
| 37 | The solution shall support identifying devices that have not reported to the MDM server in a configurable time period. | C |

|  |  |  |
| --- | --- | --- |
| **#** | **MDM Requirement** | **Priority** |
| 38 | The solution shall support automated installation of required apps on registered devices, and if possible prevent end-users from removing them. *(Note: Security requirement added to baseline)* | C |
| 39 | The solution shall support configuration policies for devices’ native web browser to control security settings such as password storage and form auto-fill. | C |
| 40 | The solution shall support detailed reporting for enrolled devices to include compliant and non-compliant settings, OS and MDM agent versions, installed apps, and changes to configuration or installed apps. | C |
| 41 | The solution shall support policies restricting access to enterprise services based on compliance status. | C |
| 42 | The solution shall offer support for policies to disable voice-activated query features such as Apple’s Siri, Google Now, and Microsoft Cortana. | C |
| 43 | The solution shall offer support for policies to disable location services. | C |
| 44 | The solution shall offer support for policies to disable device cameras. | C |
| 45 | The solution shall offer support for policies to disable device microphones. | C |
| 46 | The solution shall offer support for policies to disable infrared communications. | C |
| 47 | The solution shall offer support for policies to disable removable media (e.g., MicroSD) ports. | C |
| 48 | The solution shall offer support for policies to disable General Purpose Input/ Output (GPIO) pins. | C |
| 49 | The solution shall support policies to disable debugging. | C |
| 50 | The solution shall be able to report the installation status of required apps on registered devices. | C |
| 51 | The solution shall support tracking devices by geolocation. | C |
| 52 | The solution shall support policies restricting access to enterprise services based on the device hardware, OS, or MDM agent version. | C |
| 53 | The solution shall support restricting enrollment based on device model, OS version, IMEI, Serial Number, or UDID. | C |
| 54 | The solution shall support/enable a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities, with synchronization of files and data between the device and file servers through an encrypted connection | C |
| 55 | The solution shall support configuration policies for devices' native web browsers to restrict access to websites using blacklists/whitelists and content rating. | C |
| 56 | The solution shall protect the confidentiality and integrity of device backups. | C |
| 57 | The solution shall provide OTA reset and re-provisioning of a locked or compromised mobile device. | C |
| 58 | The solution’s administration interface shall authenticate MDM administrators through one of the following mechanisms: client Transport Layer Security (TLS) authentication using a Personal Identity Validation (PIV) card, acceptance of a Security Assertion Markup Language (SAML), or Integrated Windows Authentication. | C |
| **#** | **MDM Requirement** | **Priority** |
| 59 | Solutions that manage the entire mobile device must require device users to enter a password or Personal Identification Number (PIN) in order to unlock the device when the screen has been manually locked, after automatic lock due to inactivity, and after initially booting the OS. | C |
| 60 | Container solutions must require device users to enter a password or PIN in order to access any apps in the secure container. | C |
| 61 | The solution must include support for authentication of users to back-end agency applications and services including SharePoint and other web applications. | C |
| 62 | The solution must be integrated with the enterprise PKI for the purposes of Non-Person Entity (NPE) certificate authentication of the mobile device throughout the certificate lifecycle, to include provisioning and revocation. | C |
| 63 | The solution shall provide mutually authenticated communications between devices and the MDM services, including during initial device enrollment. | C |
| 64 | The solution must enable administrators to remotely reset device passwords/PINs, as well as any profile passwords used to prevent users from removing device profiles. | C |
| 65 | The solution shall be capable of managing the cryptographic keys and X.509 certificates on enrolled devices, including the provisioning of keys and certificates to the device and deletion of keys and certificates. Provisioning of client certificates may involve key generation on the device and submission of a Certificate Signing Request (CSR) to a Secure Certificate Enrollment Protocol (SCEP) server or proxy, or the provisioning of keys and certificates to the device in an encrypted file container (e.g., P12 file). | C |
| 66 | The solution must support policies governing the length, complexity, age, and reuse of passwords/PINs. For container solutions, these rules should apply to the container password. | C |
| 67 | The solution shall support multi-factor authentication of device users to enterprise services such as e-mail and back-end applications through the use of cryptographic credentials. This may be accomplished through a device key and issued certificate unlocked by the user’s PIN or password that is used to authenticate to the MDM server, or through PKI credentials issued to the user and provisioned to the mobile device (i.e., derived credentials). | C |
| 68 | All solution components including the MDM server and any device agent must perform certificate validation including trusted path validation and revocation checking using Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP). Certificate status information may be cached only until its expiration period. | C |
| 69 | The solution must not transmit passwords in plain text. | C |
| 70 | The solution must not store passwords in plain text. | C |
| 71 | The solution must support policies defining a timeout for cached keystore or smart card passwords between 15 and 120 minutes. | C |
| 72 | The solution must mask passwords during entry in the administrative interface, and must also support policies requiring password masking on enrolled mobile devices. | C |
| **#** | **MDM Requirement** | **Priority** |
| 73 | The solution shall ensure that the key store is password protected. Solutions using the OS native key store must also support policies to ensure that the device password is set and meets policy requirements. Solutions providing their own key store implementations must use FIPS 140-2 validated libraries and encrypt the key store using a key securely derived from the key store password. | C |
| 74 | The solution shall flush encryption keys and decrypted data from device memory when the device or container is locked, except for decrypted data needed by background processes. | C |
| 75 | The solution shall support policies to configure the network proxy settings for enrolled devices. | C |
| 76 | All solution components creating or validating digital signatures must support the use of Secure Hash Algorithm 2 (SHA-2) digital signatures. | C |
| 77 | All components of the solution that perform cryptographic operations must use FIPS 140-2 validated cryptographic libraries. | C |
| 78 | The solution shall control the cryptographic algorithms used for e-mail encryption and digital signatures. | C |
| 79 | The solution shall be capable of managing the trusted Certificate Authority certificate stores on mobile devices. | C |
| 80 | The solution must provide a mechanism to encrypt removable storage devices (e.g., Micro Secure Digital [MicroSD] cards) attached to enrolled mobile devices, unless the solution provides other safeguards preventing the storage of enterprise data on removable devices. | C |
| 81 | The solution shall require user authentication to the device before decrypting enterprise data. | C |
| 82 | The solution shall be capable of advertising and pushing updates and patches to mobile OSs, MDM agents, and enterprise apps. | C |
| 83 | The solution must be able to integrate with the enterprise Security Event and Incident Management (SEIM) systems, including the ability to export audit events in standard formats. | C |
| 84 | The solution shall check the integrity of the device to detect whether it has been compromised or “jailbroken.” Detection should include checking for common indicators of rooted devices (e.g., superuser utilities). | C |
| 85 | The solution shall check the integrity of the device to detect whether it has been compromised or “jailbroken.” Detection should include periodic validation of key files and processes. | C |
| 86 | Container solutions shall provide mechanisms to protect the integrity of the container and detect tampering by compromised OSs and applications operating outside the container. | C |
| 87 | The solution shall support policies restricting access to enterprise services based on OS integrity compromise. | C |
| 88 | The solution shall employ encryption to protect the confidentiality and integrity of configuration profiles, commands, and software updates transmitted to devices from the MDM server. | C |
| **#** | **MDM Requirement** | **Priority** |
| 89 | The solution shall check the integrity of the device to detect whether it has been compromised or “jailbroken.” Detection should include the use of a secure boot process and verification of its integrity. | C |
| 90 | The solution shall provide a single, integrated management console to create, update, and manage policies and apps for all managed devices. | C |
| 91 | The solution shall provide Document Editing for common file formats (PDF, MS Word, MS Excel, etc.) for managed applications and services. | C |
| 92 | The solution shall provide data loss prevention capabilities | C |
| 93 | The solution shall provide Over The Air (OTA) device provisioning | C |
| 94 | The solution shall provide Over The Air (OTA) registration and enrollment of devices to the MDM. | C |
| 95 | The solution shall support mobile devices with the following operating systems: MS Windows Phone 8.x and later, Apple iOS 8.0 and later, Google Android 4.0 and later | C |
| 96 | The solution shall interoperate with Agency EaaS | C |
| 97 | The solution shall provide OTA re-provisioning of mobile devices for issuance to a different user. | C |
| 98 | The container solution shall support policies that limit collection of personal information and app data stored outside the managed container. | C |
| 99 | The solution shall support user-initiated password reset requests for managed apps and services. | C |
| 100 | The solution shall support the Department's hierarchical organizational structure within the solution, and support multiple configurations for each MDM requirement | C |
| 101 | The solution shall provide configurable notification alerts to report organization-defined security and non-security events, problems, or issues, and compliance violations to the MDM administrator or Agency management. | C |
| 102 | The solution shall provide configurable reports on alerts, usage, and compliance status. | C |
| 103 | The solution shall capture, track, and retain pertinent device information, including UID, Serial Number, phone number, and Device Group Assignment. | C |
| 104 | The solution shall support scheduled and ad hoc system performance reports. System performance reports include:  Concurrent Connections,  Number and size of updates,  Peak Time Usage,  Active/inactive user and device counts,  Bandwidth utilization,  Authentication processing times,  Email/Calendar/Contact sync durations,  Connection failure rate to/from device for the MDM system | C |
| 105 | The solution shall provide management dashboards for real-time viewing of organization-defined information on devices, usage, device assignments, location, etc. | C |
| **#** | **MDM Requirement** | **Priority** |
| 106 | The solution shall support 10,000 or higher devices per server | C |
| 107 | The solution shall support 10,000 concurrent users | C |
| 108 | The solution shall support concurrent XX,XXX policy updates | C |
| 109 | The solutions shall support concurrent XX,XXX enrollments | C |
| 110 | The solution shall support multiple cost models based on use case and rapid addition and removal of devices and users. | C |
| 111 | The solution *should* send alerts via e-mail or Short Message Service (SMS) to a configurable set of recipients if the auditing system experiences a failure preventing the generation of audit records. | I |
| 112 | The MDM *should* support the reporting in SCAP format [specifically: CPE, CVE, CCE] | I |
| 113 | The solution *should* offer support for policies to disable SMS and Multimedia Messaging Service (MMS) messaging. *(Note: Added deferred security requirement.)* | I |
| 114 | The solution *should* offer support for policies to disable Universal Serial Bus (USB) tethering. *(Note: Added deferred security requirement.)* | I |
| 115 | The solution *should* support configuration policies to control access to media content by content rating. | I |
| 116 | The solution *should* create backups of all user and system information on enrolled devices, and provide a mechanism for restoring backed-up data to devices. At minimum, the solution should create backups of all managed apps and information. These backups are limited to device information, and not including PII, email, or application data. | I |
| 117 | The solution *should* include support for the retrieval of other enterprise users’ S/MIME certificates via LDAP to enable sending encrypted messages to them. *(Note: Added deferred security requirement.)* | I |
| 118 | The solution *should* provide configuration profile templates. | I |
| 119 | The solution *should* support multiple email/calendar/contact configurations per profile. | I |
| 120 | The solution *should* support setting profile start and end dates, and notification to administrator when a profile is expiring and no other profile has been defined to replace it. | I |
| 121 | The solution *should* support multiple profiles being applied to a single device. | I |
| 122 | The solution *should* support applying multiple policies to a device; when multiple security policies conflict, the most restrictive policy takes precedence. | I |
| 123 | The solution *should* support data synchronization between managed devices and allowed file shares and content repositories. | I |
| 124 | The file sharing and content repository solution *should* support document viewing functions including search, bookmarks and hyperlinks for common file formats. | I |
| 125 | The solution *should* provide the ability to manage select enterprise data for government-owned and non government-owned devices | I |
| 126 | The solution *should* allow for a store and forward approach to data access to allow local content to be manipulated and stored in a secure way for automatic upload when network connection is restored. | I |
| **#** | **MDM Requirement** | **Priority** |
| 127 | The solution should provide usage rate information associated with apps hosted in the enterprise App Store. | I |
| 128 | The solution *should* support app management workflow to enable Business Units to delegate and authorize the installation of select restricted applications. | I |
| 129 | The solution *should* provide tool-tips in app/device to provide on the fly device/app/solution training to users unfamiliar with the solution. *(Note: May be device- or app-specific, not MDM configurable)* | I |
| 130 | The solution should allow the enrollment of a device before applying any policy (null policy) |  |
| 131 | The solution should allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or groups under the MDM |  |
| 132 | The solution should allow the implementation of controls at either the device or application / content level |  |
| 133 | The solution should use an existing MDM user attribute repository for enrollment to the new MDM system |  |
| 134 | The solution shall lock, erase, or reset the device - (‘erase’ (wipe) pertains to ONLY the managed data on a device under the following conditions:   * + Blacklisted operating system or version (policy)   + Exceeding a set number of failed access attempts to the device or MDM application (policy)   + Exceeding defined interval for contacting MDM (policy)   + Detection of OS jailbreaking or application tampering (policy)   + Any other policy violation   + Remote / over the air instruction from MDM (manual) |  |
| 135 | The solution should provide detailed Inventory tracking capabilities |  |
| 136 | The solution should provide for the ability to restrict or control local data storage |  |
| 137 | The solution should enable viewing the current GPS location of a device or logical grouping of devices on a map or to provide other location identification services achieving the same or more. |  |
| 138 | The solution should Enforce enterprise rules while allowing Agency/Bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities |  |

|  |  |  |
| --- | --- | --- |
| **#** | **MDM Requirement** | **Priority** |
| 139 | The solution should allow a device to be assigned to more than one user group |  |
| 140 | The solution should allow viewing of the required applications from the Mobile Application Store (MAS) |  |
| 141 | View required applications from the Mobile Application Store (MAS) |  |
| 142 | Support a Software Development Kit (SDK) or Application Programming Interface (API) Framework to integrate with existing or future Enterprise Applications |  |
| 143 | Integrate certificates from the solution’s internal PKI system to mobile devices as well as third party public PKI providers. |  |
| 144 | MDM to perform its functions from within a secure VPN used to transport all enterprise data (i.e.: no MDM control data transported unencrypted across the open internet). |  |
| 145 | The Solution shall support the following WiFi settings and requirements: - Multiple Wi-Fi configurations for multiple profile's  - Manage device Wi-Fi settings via a MDM policy  - For a profile: Control Wi-Fi Security Type: None, WEP, WPA/WPA2, Enterprise (any) |  |
| 146 | The Solution shall support the following VPN settings and requirements:  - For a profile: Ability to support multiple VPN configurations for a profile.  - For a profile: Support VPN Connection (or Policy) Type: IPSec (Cisco), Juniper SSL, FS SSL, and Custom SSL, etc.  - For a profile: Ability to support a VPN connection Proxy for a VPN configuration |  |

#### 

#### Additional MDM Requirement Descriptions

##### FISMA Requirements

The MDM solution shall be certifiable at a FISMA (Federal Information Security Management Act) Moderate Impact level (NIST SP 800-53 Moderate or DoD 8500.2 MAC II) or higher. The solution may include proof of certification such as NIAP, Accreditation, or Authorization to Operate (ATO) in a federal environment, or a plan and timeline for achieving certification and/or Authority-To-Operate (ATO). Agencies should be aware that a service provider might offer two solutions – one that is NIAP compliant, and one that is not NIAP compliant. Each Agency must determine its level of requirements regarding NIAP compliance due to the likely cost differentiation.

##### FIPS Requirements

Solutions shall protect control and management data in transit between the MDM and the device using FIPS 140 certified cryptographic modules.

It is recommended that agencies request from any potential service provider proof of the solution’s FIPS 140-2 certification for cryptographic modules. All encrypted communications must use a cryptographic module certified in accordance with a NIST Certified Cryptographic Module Validation Program under FIPS 140-2, level 1, certification. All solutions must provide evidence of NIST Certified Cryptographic Module Validation Program compliance, or that cryptographic operations in the solution rely on FIPS certified modules in the environment or operating system.

##### Containerization

Solutions shall have containerization functionality and must describe how the container meets the following requirements:

1. FIPS 140-2 encryption of data at rest
2. Remote and local (action-triggered) secure erasure of container data without impact the rest of the device
3. Protection of container from other applications; because of varying platform capabilities, this must be described on a platform-by-platform basis

Some solutions address data control through the use of containers on the mobile device that serve to separate enterprise and personal data, and protect data from access by uncontrolled applications. This is particularly helpful for Bring Your Own Device (BYOD) scenarios, where the enterprise intends to limit interaction between agency and personal data. This approach is also used to protect data at rest if the underlying platform does not encrypt all data on the device.

##### IPv6 Support

IPv6 compliance is important for this request. On-premise portions of the MDM solution shall support IPv6 for network communications. Controls on network communications at the device must apply to both IPv4 and IPv6 communications, including VPNs, logging/auditing and network black/white-listing. The solution must provide a description of the IP based components of their solution and the status (compliant or non-compliant) of Solution providers.

##### User Authentication / Web Management

Solutions for the device must support multi-factor authentication. Solution providers must describe each of the different types of authentication supported by the solution as well as new authentication types in development with rollout over the next 18-24 months. Policy should also be able to enforce a device PIN.

Solution providers must include a web management portal as part of Solution providers, and the web management portal shall be capable of PIV / CAC (or acceptance of a Security Assertion Markup Language (SAML) for primary authentication as indicated in HSPD-12 standards and guidance. Password fallback for specific accounts may be configurable; however they must employ a second factor (SMS, voice response, etc.) to authenticate.

Solution providers shall state how their proposed solution is capable of offering or supporting multi-factor authentication. Multifactor authentication involves authentication with any two of the following three authentication types:

* Shared Secret – PIN or password
* Token – something a user possesses such as a cryptographic key such as an RSA token (soft or hard), a challenge / response token, a PIV or CAC, or a key generator device like UbiKey
* Biometric – a sufficiently unique physical characteristic of the user, such as a fingerprint, voice, iris or facial image

Additionally, the solution shall provide for installation and configuration (update, revocation checking, revocation) of individual and group soft authentication certificates for the following purposes:

* + Email (S/MIME) signing and encryption
  + WiFi Configuration
  + VPN Configuration

##### User Compliance

Solution providers must demonstrate the following capabilities. The requirements below are Critical to the solution to enable the:

1. Set up compliance rules to include custom compliance rules for profiles, devices, groups, and whitelist/blacklist
2. Activate / deactivate a compliance rule
3. Specify user and group rules for application compliance, such as required or prohibited applications on a device.
4. 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

##### Alerts and Notifications

The following alert and notification capabilities are required to notify agency operations staff about devices under management. Solution providers are to provide a description of each type of alert for which the solution is capable. The solution must demonstrate the following capabilities:

1. Set up custom alerts to users and management based upon various parameters
2. Send custom alerts to one or more user roles including administrators
3. Specify a creation policy for custom alerts to include having various alert severity levels
4. Have automated alerts for security issues such as compromised devices
5. Create alerts based upon device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.
6. View alerts pending acknowledgement
7. Acknowledge alerts and track acknowledgement
8. Search and run reports on alerts

##### Data Collection

The solution shall be able to collect and report on the following data:

1. Roaming status
2. Last policy update time
3. Last synchronization time
4. Jailbreak / root status
5. Available program memory
6. Available storage memory

##### Inventory Management

The solution must include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information. At a minimum the solution should be able to record, track and manage the following information:

1. Device Manufacturer/Model
2. Government Furnished (GFE) or personal (BYOD) device
3. Carrier
4. Wireless Number
5. MAC Addresses
6. International Mobile Equipment Identity (IMEI)
7. SIM module data
8. Storage capacity
9. OS and Version
10. Device up time
11. Encryption Capability
12. User Name
13. Email
14. Phone number
15. Agency information
16. Supervisor contact information

The solution must also have the ability to extend or expand the schema.

### Mobile Application Management

#### MAM Detailed Requirements

MAM describes software and services required for the provision and control of mobile applications, which are commercially available through app stores or are available through custom private app stores. These applications must be managed on either government owned or employee owned devices.

Below is a set of detailed MAM requirements, each marked as either Critical (C) – the solution *shall* meet this requirement or Important (I) – the solution *should* meet this requirement or be a future feature of the solution. The detailed requirements are then followed by a series of additional descriptive requirements (indicated as either optional or required), which should also be addressed in the capabilities response.

Table 2.5.2

|  |  |  |
| --- | --- | --- |
|  | **MAM Requirements** | **Priority** |
| 1 | The solution shall support policies controlling inter-app communication to restrict which apps can share data with each other. In a container-based solution, this may simply entail preventing apps inside the container from communicating with those outside the container and vice versa. | C |
| 2 | The solution shall support policies to restrict enhanced location services access to details such as Wi-Fi SSIDs in range. | C |
| 3 | The solution shall support policies preventing the installation of apps that do not have a valid cryptographic signature, including the ability to limit installation to apps signed by specific developer keys. | C |
| 4 | The solution shall support restricting the use of default apps included with the native mobile OS (e.g., preventing use of the native browser or e-mail client). | C |
| 5 | The solution shall support application “blacklist” policies prohibiting the installation of specific apps. | C |
| 6 | The solution shall support application “whitelist” policies that identify specific apps that may be installed and prohibiting the installation of all other apps. | C |
| 7 | Container-based solutions shall support the use of both whitelist and blacklist policies, such that only whitelisted apps may be installed inside the container and blacklisted apps may not be installed on the device (inside or outside the container). | C |
| 8 | The solution shall support policies disabling the use of commercial app stores, permitting devices to install apps from the enterprise app store only. | C |
| 9 | If the solution supports PKI credentials, it must provide or incorporate a PKI-enabled web browser. | C |

|  |  |  |
| --- | --- | --- |
|  | **MAM Requirements** | **Priority** |
| 10 | The solution shall provide a mechanism for third-party mobile applications to integrate with MDM capabilities such as authentication, remote access mechanisms, or policy distribution and management. This may be accomplished by providing a Software Development Kit (SDK) or through an app wrapping mechanism. *(Note: Security requirement added to baseline)* | C |
| 11 | The solution shall provide an enterprise app store for users to search, access, download, and install authorized iOS, Android, and Windows Phone applications on managed devices. | C |
| 12 | The solution shall support single sign on for Agency-developed apps | C |
| 13 | The solution shall support role-based access control to the Agency or Government app store. | C |
| 14 | The solution shall support management, distribution and update of custom (Agency developed) and commercial apps. | C |
| 15 | The solution shall support integration with Apple's Volume Purchase Program | C |
| 16 | The solution shall support delegated administration to allow authorized users the ability to view usage, logs and GPS data. | C |
| 17 | The solution *should* support policies to restrict enhanced location services access to details such as Wi-Fi SSIDs in range. | I |
| 18 | The solution *should* support enterprise single sign on (e.g., SAML, Kerberos, OpenID, SiteMinder) | I |
| 19 | The solution *should* include support for the use of S/MIME for e-mail signatures and encryption using a cryptographic smart card or keys and certificates stored in a software keystore. *(Note: Added deferred security requirement.)* | I |
| 20 | The solution *should* support integration and secure connections to Agency internal file shares and content repositories (e.g., SharePoint) | I |
| 21 | The solution shall support connecting to Agency-approved Secure Instant Messaging application. | I |
| 22 | The solution *should* support app development workflow and app management workflow to enable business units to delegate and authorize installation of select applications. | I |
| 23 | The solution *should* provide a test environment to assess new applications and new versions of existing applications prior to authorizing applications for use in an Agency production environment. | I |
| 24 | The MAM solution *should* support application life cycle management by providing the capability to evaluate, analyze, and manage submitted applications for approval to release to the application store. | I |
| 25 | The solution *should* support federated authentication to Agency or Government app store(s) (e.g., to allow access from State & Local partners). | I |
| 26 | The MAM solution shall have the ability to manage individual applications without the requirement of having to manage or control the device (e.g. ability to maintain control of applications on employee owned or contractor devices) | TBD |
| 27 | The solution shall Identify and detect a compromised application or one that has been threatened with possible or attempted compromise | TBD |

|  |  |  |
| --- | --- | --- |
|  | **MAM Requirements** | **Priority** |
| 28 | The solution shall clearly specify data loss prevention capabilities and enterprise level implementation options of those capabilities | TBD |
| 29 | The solution shall provide Application tunneling capabilities – ability for an enterprise to selectively determine which applications have authorization to access enterprise data behind the Agency firewall | TBD |
| 30 | The solution *should* allow for User Authentication on a per application basis | TBD |

#### Additional Descriptive Mobile Application Management Requirements

##### (Optional) MAM Software Integration Services

Some Managed Mobility users may require the need for the delivery of new or existing enterprise applications to mobile devices. One example could be making a data entry system accessible to field workers. If your solution supports these capabilities, please describe how this is accomplished.

##### Application Deployment

The solution shall support the following controls and capabilities for application deployment:

1. Commercial Application Store (iOS App Store, Google Play, etc.) (enable / disable)
2. Reporting of installed applications
3. Blocking application purchase
4. Application whitelisting / blacklisting
5. Staged/controlled application deployment (limit deployment by policy, group, location, etc. to facilitate gradual deployment of new or updated applications)

##### Mobile Application Store (MAS)

The solution shall include a Mobile Application Store to allow users to select private enterprise applications for installation on managed devices. This capability must be integrated into the Managed Mobility MDM portal, and allow application provisioning by group policy, and mandatory application deployment.

The MAS should support the following capabilities:

1. Ability to add an application from a Commercial Application Store to the MAS
2. Ability to add an enterprise application to the MAS via a web GUI
3. Ability to add additional metadata to and report on metadata on any application added to the MAS (etc. name, description, version, OS, keywords, etc.)
4. Ability to specify the effective date for an internal application
5. Ability to specify the expiration date for an internal application
6. Ability to specify the minimum operating system and model for an internal application
7. Ability to download internal and public applications from MAS
8. Ability to categorize, group or tag applications (e.g., business applications, scientific applications, etc.)

##### Mutual Authentication

MDM applications on the device and services must mutually authenticate to ensure the communications channel is not intercepted. The mutual authentication should be certificate-based, with installation-specific certificates deployed to the server during deployment and to the device during provisioning.

##### Application Installation Control

The solution shall demonstrate the solution’s process to support relevant authorizations and approvals (include change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance. This includes the ability to monitor application usage.

##### Blacklisting / Whitelisting

The solution shall provide the capability to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting). This capability should be managed through user and group policies.

##### Application Environment Requirements

The solution shall be able to detect and enforce device environment conditions such as:

1. Minimum or specific operating system versions
2. Required presence or absence of other applications
3. Absence of privilege escalation (“rooting” or “jailbreaking”)

##### Application Signing

The solution should support requiring digital signatures for application installation, from both commercial and private application stores and direct application push / deployment. It is permissible to meet this requirement through OS capabilities.

##### (Optional) Third-Party Application Mutual Authentication

The MDM solution may offer the ability provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.

### Mobile Content Management

#### MCM Detailed Requirements

MCM refers to content management capable of securing, storing, delivering, controlling, and preventing data loss on the mobile device and any transmission of data to or from the mobile device.

Below is a set of detailed MCM requirements, each marked as either Critical (C) – the solution *shall* meet this requirement or Important (I) – the solution *should* meet this requirement or be a future feature of the solution. The detailed requirements are then followed by a series of additional descriptive requirements (indicated as either optional or required), which should also be addressed in the capabilities response.

Table 2.5.3

|  |  |  |
| --- | --- | --- |
|  | **MCM Requirement** | **Priority** |
| 1 | The solution shall provide Document Editing for common file formats (PDF, MS Word, MS Excel, etc.) for managed applications and services. | C |
| 2 | The solution shall provide data loss prevention capabilities | C |
| 3 | The solution shall provide for the restriction of downloading attachments, copying of data to/from removable media, or otherwise create separate spaces or virtual containers for agency data and applications from personal data | TBD |
| 4 | The solution shall send/receive (Encrypt and Sign, decrypt and verify) messages that use PKI or S/MIME encryption, where email functionality is delivered by the solution | TBD |

#### Additional Descriptive MCM Requirements

##### Privacy

Solution providers shall not display advertisements to end users of the Information System as part of its business model (i.e. not an advertising-based model).

Solution providers shall safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)” and in accordance with M-06-16: Protection of Sensitive Agency Information [http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf and M-07-16](http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf%20and%20M-07-16): Safeguarding Against and Responding to the Breach of Personally Identifiable Information <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy. An Ordering Activity may request that PII be kept within U.S. Data Centers.

The solution must disclose privacy-impacting features that cannot be disabled.

##### Continuity of Operations and Disaster Recovery

The solution shall describe how the solution performs Continuity of Operations (COOP) and Disaster Recovery (DR).

##### File Management

The Government seeks solutions that have the capability to secure data, files, and applications (for example PDF files or word docs) on a mobile device. Devices may be Government Furnished (GFE) or BYOD. The solution must demonstrate that the solution is able to hold a set of COTS and/or enterprise applications with respective data/files in a secured space, whether that is within a secured container or secured within the device OS. The solution must also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and file servers.

##### Personal Information Management

The solution shall demonstrate the solution’s ability to support a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities. To ensure that the information is available to other mobile and desktop devices the user may have, as well as for business continuity, backup/restore, and e-discovery purposes, solution providers must be able integrate functionality with a variety of Email, Calendaring and Contact applications, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection. The solution should also demonstrate the solution’s PIM capability to support multiple types of Federal Enterprise Email Systems from different vendors. Please identify which on-premise and cloud-based mail systems are supported, such as Microsoft Exchange, Lotus Notes, Gmail, MS 360, Lotus Domino, MS Exchange or Zimbra.

##### Security Content Automation Protocol (SCAP) Support

SCAP provides the ability to automate security checks and configuration. Solution providers must describe the SCAP support for the server-side components in the solution, including asset management, configuration management, patch management and remediation capabilities.

The requirement is only addressing server SCAP support at this time. SCAP for devices is not currently a requirement.

**2.5.8 Audit and Reporting Requirements**

The solution shall demonstrate the following detailed Audit and Reporting capabilities:

#### Audit and Reporting Detailed Requirements

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Audit and Reporting Requirements** | **Requirement Category** | **Priority** |
| 1 | The solution shall create audit records of security-relevant actions on the device, to include password changes, failed authentication attempts, and connections to enterprise resources. | AUDIT | C |
| 2 | The solution shall create audit records of access to the administrative console and all administrator actions such as policy definition and modification, manual requests to wipe devices, and modifications to device and user information. | AUDIT | C |
| 3 | Audit records shall contain at a minimum the event ID, timestamp, location information, event source, event description, and identity of the device and, if known, the user. | AUDIT | C |
| 4 | To enable event log correlation, the solution shall support synchronizing both the MDM server(s) and managed devices with agency designated Network Time Protocol (NTP) server. | AUDIT | C |
| 5 | The solution shall control access to audit records in order to preserve the confidentiality and integrity of audit data. | AUDIT | C |
| 6 | The solution shall protect logs against unauthorized modification (e.g., through the use of digital signatures). | AUDIT | C |
| 7 | The solution shall protect the confidentiality and integrity of audit records and reporting information transmitted from devices to the MDM server. | AUDIT | C |
| 8 | The solution shall produce hardware and software asset inventory reports for enrolled devices. | REPORTING | C |
| 9 | The solution shall be able to report the installation status of required apps on registered devices. | REPORTING | C |
| 10 | The solution must be able to integrate with the enterprise Security Event and Incident Management (SEIM) systems, including the ability to export audit events in standard formats. | AUDIT | C |
| 11 | The solution shall provide configurable notification alerts to report organization-defined security and non-security events, problems, or issues, and compliance violations to the MDM administrator or DHS management. | REPORTING | C |
| 12 | The solution shall provide configurable reports on alerts, usage, and compliance status. | REPORTING | C |
| 13 | The solution shall capture, track, and retain pertinent device information, including UID, Serial Number, phone number, and Device Group Assignment. | REPORTING | C |
|  | **Audit and Reporting Requirements** | **Requirement Category** | **Priority** |
| 14 | The solution shall support scheduled and ad hoc system performance reports. System performance reports include:  Concurrent Connections,  Number and size of updates,  Peak Time Usage,  Active/inactive user and device counts,  Bandwidth utilization,  Authentication processing times,  Email/Calendar/Contact sync durations,  Connection failure rate to/from device for the MDM system | REPORTING | C |
| 15 | The solution shall provide management dashboards for real-time viewing of organization-defined information on devices, usage, device assignments, location, etc. | REPORTING | C |

#### Additional Descriptive Audit and Reporting Requirements

##### Device Inventory Reports

The solution shall demonstrate the capability to run inventory reports. Device Inventory reports includes all data associated with the device, OS and applications. Device reports will be run and/or exported as needed, and will support the following filters:

1. Device Models
2. Operation System and build level
3. Last Access times (access time not compliance check)
4. Application inventory
5. Last Compliance Check
6. Device Compliance (ability to report on rooted/jailbroken devices, policy, etc.)
7. Carrier
8. Network Card IDs (MAC address)
9. Agency Assignment
10. BYOD or GFE (personal device or government furnished)
11. Security Policy Assignment (policy currently applied to device)

##### System Performance Reports

The solution shall demonstrate the capability to run system performance reports. System performance reports include key performance data to provide insight into the usage of the devices, reliability of the solution, and performance of devices. System performance reports will be run as needed and will support the following filters:

1. Concurrent Connections
2. Peak Time Usage
3. Total active user and device counts
4. Bandwidth utilization trends
5. End-to-End testing results
6. Authentication processing times
7. Email/Calendar/Contact sync durations
8. Connection failure rate to/from device for the MDM system

##### MDM Security / Compliance Reports

The solution shall demonstrate the capability to run security/compliance reports. Security reports include all data relevant to the monitoring and support of the system’s vulnerabilities and defenses, including attempts at fraud. Security status reports will be run as needed and will support the following data:

1. Non-compliant devices
2. Device wipe actions
3. Passcode reset actions
4. User/Devices with failed authentication
5. Aggregate data on failed authentications
6. Devices with blacklisted applications
7. Jailbroken devices
8. Device anti-virus versions
9. Mobile Management Agent

#### (Optional) Quality of Service (QoS)

The solution should support QoS capabilities to prioritize real-time or latency-sensitive application data where appropriate (e.g.: VoIP, video, real-time chat). The solution should be able to enforce and exclude QoS priority by application or protocol to prevent non-real-time applications from inappropriately increasing their traffic priority.

##### (Optional) Classified Data

Some Managed Mobility users may require the ability to access classified data up to the SECRET level via mobile devices. If your solution supports these capabilities, please describe how this is accomplished and indicate the specific impact to pricing for this solution, inclusive of exact dollar amounts.

##### PIV / CAC Support

Solution providers shall offer solutions that support the management of PIV / CAC cards on mobile devices via the MDM.

##### (Optional) Biometric Support

Agencies with strong authentication requirements may need biometric support such as fingerprint or face recognition with their mobile devices. The ability for the MDM to manage this capability may be combined with PIV / CAC support.

##### (Optional) Network Monitoring

Network Monitoring is the monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by enterprise devices).

The solution should include a device application that performs basic diagnostics, such as:

1. Verify network connection and performance
2. Test authentication settings
3. Verify certificates
4. Verify DNS functionality
5. Verify connection to services (mail, MDM, etc.)

### Service Delivery Model

The EMM Solution shall be delivered and (optionally) hosted by the Contractor as a full solution including all hardware, software, hosting, and installation services, using one or more of the following hosting models:

1. Cloud Based - For the purposes of this request a Cloud Only solution is a solution that has all HW/SW components of the solution running in a non-government hosted cloud data center. The solution must show how they provide all required hardware to the network edge of their cloud data center. The solution is responsible for all aspects of system and software performance for solution components within their cloud data center.
2. On Premise - For the purposes of this request an On-Premise solution is a solution that has all HW/SW components running completely within federal Government controlled data centers and network. After installation, the Federal Government will be responsible for operating the infrastructure and devices, application store and container management.
3. Hybrid - For the purposes of this request a Hybrid solution is a solution where the components are distributed across federal Government data centers and the solution’s cloud data center. It is anticipated that the solution will provide all required hardware to the network edge of their cloud data center. The solution will clearly describe all HW/SW components that will be within federal Government data center and those components within the solution’s cloud data center. The solution would be responsible for all aspects of system and software performance for solution components within their cloud data center.

The Help Desks should be operationally located within the Continental United States (CONUS).

## Support Requirements

#### Project Management

The solution must clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements.

#### Deployment / Migration / Transition

The solution must clearly describe how they provide initial deployment support services. These services are expected for installing, configuring, and certifying the initial deployment of the MDM, MAM and Container solutions, as well as the ability to support specific agency related integrations or customizations. The solution would assist the agency with achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.

The solution must contain a Transition Plan that details how devices previously supported by the solution will transition from existing service in a quick, reliable, and accurate manner to the offered solution. Staffing requirements (contractor and government) for this Transition Plan must also be identified. Solution providers will receive additional consideration if example transition plans from previous MDM deployments are supplied.

The solution must provide an example of a previous successful on-boarding of 10,000 or more devices. The example must include a high-level timeline, staffing required, and a summary walk-through of the process (1 page maximum for summary walk-through).

The Contractor must also provide an example of an exit transition plan that describes how, in case termination for any reason, delivered data conforms to an industry standard format capable of being transported to other systems.

#### Enterprise Systems Integration

The solution must show how they can be responsible for providing steps necessary for deploying and integrating their Mobility Solution into the enterprise-wide environment. This includes such systems as enterprise email, directories, trouble-ticketing, etc. The steps included are expected to vary dependent upon whether the solution is on-premise or a cloud solution.

#### Training

The Government requires that all users of the MDM-MAM system, which includes end users, administrators and developers, be trained to correctly utilize the system. The solution must demonstrate how they can be responsible for developing and updating the MDM-MAM Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan. The online training may be hosted by the government or the contractor, and the contractor must provide the required content.

#### Help Desk

The solution must provide access to help desk support for their solutions. Please indicate the location of the operational help desk. They must satisfy the following criteria:

1. End User Help Desk support must be 24/7 including holidays.
2. Administrative / Management Help Desk must be available 8am-5pm in both EST and PST.
3. Help Desks must utilize a trouble-ticketing system where each request has a unique identifier for tracking purposes.
4. Help Desk interaction must support online requests / resolution, supported with email.
5. Telephone (voice) Help Desk support must be available, but can be limited to business hours.

#### Demonstration Platform

The solution must possess a demonstration platform to educate potential customers on the use, benefits and technical specification of the solution. Solution providers shall provide access to the portal for the purpose of sampling and demonstrations that will be connected to the solution’s site through the OCSIT Innovation Center.

#### (Optional) Enterprise Configuration

This addresses non-core integration, such as Solution connectivity with non-required components (e.g. custom portal, Telecommunications Expense Management System (TEMS) provider system, etc.). Agencies have applications that may be need to be accessed on mobile devices, but that require configuration services to enable. The solution should describe the services they offer of this type. Each configuration service offered must be accompanied by a successful example from industry or government.

#### (Optional) Integration with FSSI Wireless Portal

The FSSI Wireless Business Portal Interface is a secure standard for agencies to interface with cellular carriers to place orders, manage plan/device inventory, and other carrier provided information. The BPI is not a GUI but merely a secure standard for exchanging data between the customer agency and the carrier. Solution providers should indicate their experience and platform's ability with exchanging information with third party providers for the purpose of providing complementary services such as device ordering, logistics, configuration, replacement/refresh, disposal, and disposition reporting

#### (Optional) Telecommunications Expense Management System (TEMS)

TEMS includes a portfolio of purchasing, expense analysis/optimization, invoice payment, reporting (inventory, usage, zero-use identification) and financial functions associated with business communications expense. It also considers nonrecurring services, such as one-time historical audits, and other advisory services relating to enterprises' communications expenditure. The solution may demonstrate how their proposed solution addresses order management, ordering via portal, device provisioning, asset management, device asset tracking, non-device asset tracking, account reports, expense management, service plan management, optimization, and expense tracking/reporting. Further the solution may list additional functions that may be of interested to the Federal Government including the ability to pilot a Mobility Management offering to federal customers.

#### (Optional) Device Replacement / Refresh

Device replacement/refresh refers to complementary logistics services where a Contractor may support Government entities with Device replacement and refresh services based on existing government contracts with device providers, carrier or otherwise. The solution may offer logistical support for device replacement, such as pre-enrolling devices at a depot, etc.

#### (Optional) Device Disposal & Reporting

Device Disposal and Reporting refers to the compliant device wiping, destruction, recycling and reporting of mobile devices per government standards (NIST, R2, others) as required per individual agency requirements. The solution provider should indicate experience, willingness, resources, and ability to provide these services.

# Pricing

When request or evaluate pricing of the solution providers, pricing should be presented on a per device basis – it can be presented in the context of price ranges, pricing tiers based upon volume, pricing based upon pre-defined product configurations or some other scenario or set of scenarios. However, to keep with the purpose of this document and to scale across government, it is strongly suggested that pricing submissions be kept to fairly simple structures so that a cost per device can be easily determined and understood in the context of services delivered.

Pricing may either be customized or may be submitted based upon availability through publicly accessed source. Pricing should be submitted as an integral part of the providers’ solution.

Agencies should request that solution providers indicate the range at which their product is sold to their federal customers, inclusive of the discounted rate that is offered to their best federal customer. It is recognized that not every federal customer purchases solutions identically, and often pricing is dependent specific agency needs and requirements. The intent is to indicate the range of potential pricing, subject to the particular requirements that fall beyond the specifications. Additionally, agencies should request a pricing table, which reflects the price structure and currently listed prices for the solutions on Federal contracts/task orders.

For those solution providers offering their solution under IT Schedule 70 the solutions must be on the vehicle and the pricing must correspond to what is found on the schedule. If the solution is offered via a solution’s IT Schedule 70 contracts, the solution must currently reside on that contract vehicle to be considered. If the solution cannot be identified on the solution’s IT 70 contract it will not be considered for assessment at this time. For pricing related to other government-wide acquisition vehicles the rules would be consistent with those of that particular vehicle necessary to reach the solution’s solution set.

# 

***Glossary and Abbreviations***

|  |  |
| --- | --- |
| **Term** | **Description** |
| Agency | “Department” or other administrative unit of the federal government, such as the General Services Administration (GSA), which is using this contract vehicle. This also includes quasi-government entities, such as the United States Postal Service. |
| API | Application Programming Interface |
| Blacklist | Application or software not deemed acceptable and have been denied approval. This may vary between agencies. |
| Bureau | A sub-Agency Bureau level organization, which is using this contract vehicle, as defined by OMB ([www.whitehouse.gov/sites/default/files/omb/circulars/a11/current\_year/s79.pdf](http://www.whitehouse.gov/sites/default/files/omb/circulars/a11/current_year/s79.pdf)). |
| BYOD | Bring Your Own Device; Staff brings their personally-owned devices and the Enterprise installs capabilities such as email on them. May also refer to bringing devices from other agencies. |
| CAC | Common Access Card; a 2-factor electronic identity card used by the Department of Defense to identify individuals. The civilian equivalent is the Personal Identity Verification (PIV) card. |
| Capability | A technical service requirement that is a component of the base service. |
| CBP | Customs and Border Protection |
| CIO | Chief Information Officer |
| COTS | Commercial Off-The-Shelf; solutions that can be purchased in a complete form from existing commercial vendors. |
| DANIEL | DHS Advanced Network Integration and Experimentation Lab |
| Data Plan | Includes web browsing, send and receive email, download attachments, downloading applications, and application data usage. |
| Device | Also called handheld wireless devices, these include handheld devices that are capable of wireless voice or data communications. The devices support cellular or paging technologies augmented by technologies such as WLAN and satellite. |
| Feature | An enhancement beyond base service that is to be selected at the option of the user. Features are normally separately priced, although some features have been defined to be not separately priced (NSP). Each feature must be ordered separately even if not separately priced. |
| FAS | Federal Acquisition Service. |
| FICAM | Federal Identity, Credential, and Access Management mainly addresses user certificate authentication although it does touch on passwords. FICAM is the guidance document, ICAM is the body that created it. |
| FIPS | Federal Information Processing Standards. |
| FSSI | Federal Strategic Sourcing Initiative; FSSI Wireless provides wireless service and device ordering capabilities to Government agencies. |
| GB | Gigabyte or 1000 MB of data. |
| GFE | Government Furnished Equipment. |

|  |  |
| --- | --- |
| **Term** | **Description** |
| GPS | Global Positioning System; A network of orbiting satellites that enable receivers on the ground to report their position, velocity and time. Mobile devices often use Assisted GPS (AGPS) which leverages cell towers to speed reporting time. |
| Government | All government entities that use or administer this contract vehicle, including state, local and education. |
| Government Web Store | Concept of web-based acquisition interface and management platform where government stakeholders (employees, citizens, partners) may initiate purchases, manage previous purchases, and manage contractor relationships. Concept is based on enterprise version of a commercial web storefront. |
| HSPD-12 | Homeland Security Presidential Directive 12, which (among other things) directs agencies to deploy 2-factor authentication for information systems. |
| M2M | Machine to machine technologies that allow both wireless and wired systems to communicate with other devices of the same ability. |
| MAS/MAM | Mobile Application Services/Mobile Applications Management. |
| MB | Megabyte, a common term used to describe the amount of data being sent over a wireless network. |
| Mbps | Megabits per second, a common term used to describe wireless transmission speeds. |
| Mobile Device | Characteristics include 1) a small form factor, 2) at least one wireless network interface for Internet access or voice communications, 3) built-in (non-removable) data storage, 4) an operating system that is not a full-fledged desktop or laptop operating system, 5) built-in features for synchronizing local data with a remote location (desktop, laptop, organizational servers, etc.) if data capable, 6) generally operates using battery power in a non-fixed location. |
| Mobile Device Management (MDM) | MDM – Mobile Device Management. MDM is a widely used term describing device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application support (application performance, version control, distribution, etc.), mobile data management (on device), and some mobile network monitoring. The definition of MDM varies and reflects its growth (pre-maturity) status. |
| NIST | National Institute of Standards and Technology |
| Ordering Entity | Any Agency, sub-Agency, state or local government that is using this contract vehicle. |
| Ordering Agency | The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency. |
| PIV | Personal Identification Verification |
| Portal | A software (or web) solution that enables instant and effortless exchange of business information (Electronic Data Interchange – EDI) over the Internet. This is accomplished by the use of a common operating framework for accessing data and information from different systems. A typical TEMS portal will pull information from carrier electronic billing systems, which is uploaded into their platform (portal). This allows the administrator/user a single view that provides multiple carrier information in a seamless manner, offering efficiency. |
| Secure Communications | Communication services that includes security components such as encryption to ensure the privacy and integrity of the communications. |
| Smartphone | Electronic handheld wireless device that integrates the functionality of a mobile cellular phone, personal digital assistant (PDA) or other information appliance. |
| **Term** | **Description** |
| Subsystem | A subsystem is a set of elements, which is a system itself, and a [component](http://en.wikipedia.org/wiki/Component) of a larger system (Wikipedia). For instance, a subsystem could include both the encryption software and the related software on the server. |
| TEMS | Telecommunications Expense Management Services, delivered by third parties, relating to processes for the sourcing, procurement and auditing functions connected with business communications expenses. It also considers nonrecurring services, such as one-time historical audits, and other advisory services relating to enterprises' communications expenditure [Gartner]. |
| Text Messaging or SMS | Text Messaging or Short Message Service (SMS) is the exchange of brief written messages between cellular phones, smartphones, and data devices over cellular networks. |
| Third-Party Direct Billing | The receipt of invoices from parties other than the Contractor for services within or outside the scope of this agreement. |
| Trade Agreements Act (TAA) | The TAA of 1979 is an [Act of Congress](http://en.wikipedia.org/wiki/Act_of_Congress) that governs trade agreements negotiated between the U.S. and other countries under the [Trade Act of 1974](http://en.wikipedia.org/wiki/Trade_Act_of_1974). Its stated purpose is to:   1. Approve and implement the trade agreements negotiated under the Trade Act of 1974 [19 U.S.C. 2101 et seq.]; 2. Foster the growth and maintenance of an open world trading system; 3. Expand opportunities for the commerce of the United States in international trade; and 4. Improve the rules of international trade and to provide for the enforcement of such rules, and for other purposes.   The TAA designated countries are listed in the following web site:  <http://gsa.federalschedules.com/Resource-Center/Resources/TAA-Designated-Countries.aspx> |
| Trouble Ticket | Also called a trouble report, this is the documentation of a service or device failure that impacts the service. The ticket enables an organization to track the detection, reporting, and resolution of some type of problem. |
| WLAN Calling | Wireless Local Area Network: Enables a wireless handset to make and receive calls via an internet-connected WLAN (e.g., Wi-Fi network) instead of the cellular network. |
| White List | Whitelist: Application or software considered safe to run, and is preapproved. |
| Wireless Systems and Subsystems | Wireless infrastructure, servers, and software that enable an enterprise to enhance its cellular coverage, increase cellular capacity, and enable enterprise solutions (e.g., BlackBerry Enterprise Server) using services offered by the wireless industry. |
| 24/7 phone support | Technical support and user assistance is provided by telephone and Internet 24 hours a day, 365 days (or 366 during leap years) per year. |