GSA Managed Mobility Program

U.S. General Services Administration

Managed Mobility Program

Request for Technical Capabilities (RFTC)

POC: Jon M. Johnson, Program Manager
Managed Mobility
Integrated Technology Service (ITS) /
Federal Acquisition Service (FAS)
General Services Administration
703.306.6481
jon.johnson@gsa.gov

1 Introduction 4
1.1 Background 4
1.2 Objective 4
1.3 Program Management Office Point-of-Contact (PMO POC) 6
1.4 Preparation Costs 6
1.5 Government Property 6
2 Capabilities Work Statement 7
2.1 High Level Architecture 7
2.1.1 Scope / Scale 7
2.1.2 Multi-Tenancy 7
2.1.3 Solution Security 8
2.1.4 Privacy 12
2.1.5 Service Delivery Model 12
2.2 Mobile Device Management (MDM) 13
2.2.1 Device Enrollment 13
2.2.2 Device Profiles 14
2.2.3 Device Feature Management 15
2.2.4 Data Management 15
2.2.5 Security Content Automation Protocol (SCAP) Support 16
2.2.6 Device Inventory Management 17
2.2.7 Device Inventory Reports 17
2.2.8 System Performance Reports 18
2.2.9 MDM Security / Compliance Reports 18
2.2.10 (Optional) Quality of Service (QoS) 18
2.2.11 (Optional) Classified Data 19
2.2.12 (Optional) PIV / CAC Support 19
2.2.13 (Optional) Biometric Support 19
2.2.14 (Optional) Network Monitoring 19
2.3 Mobile Application Management (MAM) 19
2.3.1 Application Deployment 19
2.3.2 Mobile Application Store (MAS) 20
2.3.3 Application Security 20
2.3.4 (Optional) Third-Party Application Mutual Authentication 21
2.3.1 (Optional) MAM Software Integration Services 21
2.4 Mobility Life Cycle 21
2.4.1 Implementation / Installation 21
2.4.2 Operations Support 22
2.4.3 Demonstration Platform 23
2.4.4 (Optional) Enterprise Configuration 23
2.4.5 (Optional) Integration with FSSI Wireless Portal 23

2.4.6 (Optional) Telecommunications Expense Management System (TEMS) 23
2.4.7 (Optional) Device Replacement / Refresh 24
2.4.8 (Optional) Device Disposal & Reporting 24
3 Pricing 25
4 Instructions 26
4.1 RFTC Questions 26
4.2 Virtual Industry Day ..... **Error! Bookmark not defined.**
4.3 Response Content 27
4.3.1 Executive Summary (2 Page Limit) 27
4.3.2 4.2.2 Table of Contents 28
4.3.3 4.2.3 Technical Section Instructions (75 Page Limit) 28
4.3.4 Acquisition Approach (Required – 1 Page) 35
4.3.5 Pricing Section (No page limit) 35
5 Assessment 36
5.1 Completeness and Correctness of Required Capabilities 37
5.2 Evidence of Enterprise Integration 37
5.3 FIPS/FISMA 37
Appendix A Use Cases 38
Appendix B Glossary and Abbreviations 44

1 Introduction

1.1 Background

The purpose of this solicitation is to identify capable solutions that will meet the federal government's increased needs to manage its mobile devices.

This RFTC has two primary components, Mobile Device Management (MDM) and Mobile Application Management (MAM), and also includes Mobility Life-Cycle (MLC) support. This RFTC also has a set of optional services contained within each.

The primary program components and benefits are:

A. Qualified Secure, Scalable Solutions – Technical solutions that address the existing needs of government mobile technology including security and policy management. The solutions also have the ability to scale to the extremely large and evolving nature of federal government cabinet-level agency organizations.

B. Evolutionary and Flexible – The management needs of the Federal Government Mobility are changing every quarter with increased mobile adoption and emerging policy and security requirements. As a result, this program will continue to assess selected and future solutions to ensure the ongoing and yet to be determined requirements are addresses as the MDM and MAS market continues to develop. The Managed Mobility program intends to re-assess both the program requirements and marketplace in response to this evolution. This provides government agencies with updated qualified solution lists.

C. Shared Mobility Community – Monitoring new industry developments, identification of Managed Mobility best practices, and promotion of these "best practices." The Managed Mobility space is in a state of rapid evolution, making it challenging and resource-intensive for agencies to stay properly informed. By centralizing requirements gathering and solution assessment, the Managed Mobility program reduces the burden on agencies while increasing the quality of their options.

1.2 Objective

The government's mobility management challenge must address the customer agency's mission needs in a secure, cost-effective manner. This objective is driven by the Digital Government Strategy requirement 5.5, which seeks to "Set up a government-wide mobile device management platform" (http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html). Managed Mobility is a core capability for effectively scaling the secure deployment and management of mobile applications, enterprise data on mobile devices, and management of the devices and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to the agencies. The Managed Mobility program defines a 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.

Multiple Solutions Sets

Because of the complexity of the requirements and the rapid evolution of the managed mobility marketplace, respondents may incorporate multiple tools into a proposed solution set.

Though the Mobile Life-Cycle component of this request is required and necessary, we are most interested in the MDM/MAM products and solutions available that can fit the need. We anticipate and welcome responses from all interested parties that can conform to the requirements; however it is anticipated that the MDM and MAM solution sets will address the majority of the requirements listed in this RFTC.

Approach to MDM/MAM Acquisitions

This initiative will identify MDM/MAM platform(s) capable of satisfying the government's mobile device management needs specified by the requirements developed as a result of the Digital Government Strategy (DGS) Item #5.5 Multi-Agency Working Group efforts. **These platforms will be linked through the GSA Managed Mobility website and the GSA Innovation Center website.** User guides for federal agencies will be developed for each acquisition vehicle under which competition can take place in order to procure Managed Mobility solutions, and the user guides will also be accessible on the government-wide platform.

Respondents are required to map their solution sets to offerings available via existing government-wide vehicles. This request will not result in a new contract. Rather, those solution sets that are assessed and found capable of addressing the outlined requirements to satisfy the greatest governmental need will be identified and mapped to existing government-wide acquisition vehicles. Respondents will be required to map their offerings to the specific vehicles where they are currently offered. If the solution set is unavailable on a vehicle identified, then that vehicle cannot be identified as a means to procure the solution. Instructions can be found in Sections 3 & 4.

The content of the responses submitted are considered proprietary and will not be released without the expressed consent of the respondent. Those whom have been assessed and determined capable of meeting the greatest governmental need will be identified on the GSA Managed Mobility web platform. This platform will identify the solutions, government-wide acquisition vehicles, and available price ranges. No other information will be released without consent.

No contractual relationship will exist between the GSA Managed Mobility Program and the solution set providers, as the contractual relation will rest upon the existing government-wide vehicles and any task orders issued thereunder. If a solution set is not identified through this solicitation it will not be restricted or prohibited from competing for any task order competed

against government-wide acquisition vehicles that are conducted in accordance with Federal Acquisition Regulations.

1.3 Program Management Office Point-of-Contact (PMO POC)

The PMO POC is the individual within a program management function who has overall technical responsibility for efforts. The PMO POC supports the administration of the RFTC by:

- Defining requirements and assessment criteria
- Making final decisions regarding solution qualification
- Providing technical clarification on requirements

The PMO POC responsible for this RFTC is:

Jon Johnson
U.S. General Services Administration
Federal Acquisition Service
10304 Eaton Place
Fairfax, VA 22030
Telephone: 703-306-6481
Email: Jon.Johnson@gsa.gov

1.4 Preparation Costs

The Government will not be responsible for any costs associated with preparing a response to this request.

1.5 Government Property

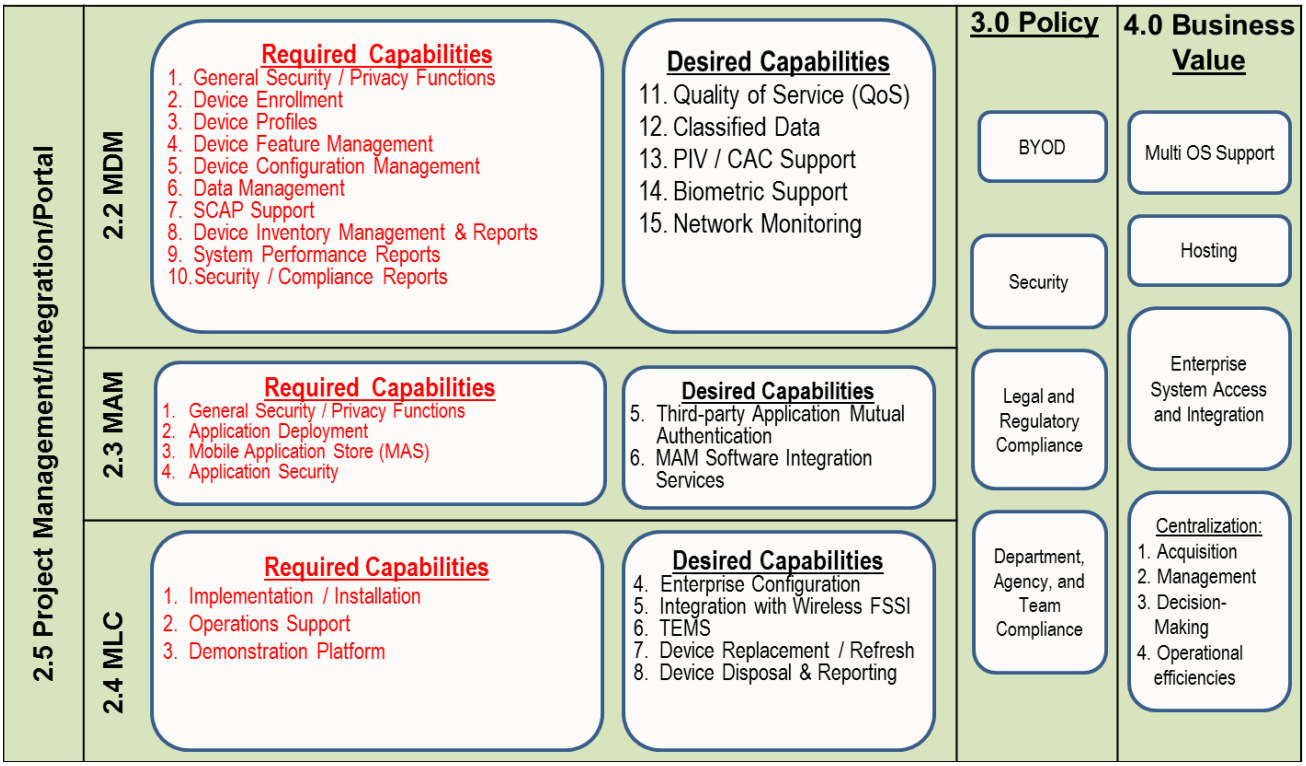
Upon receipt, all responses become government property and will not be returned.

2 Capabilities Work Statement

2.1 High Level Architecture

Managed Mobility is a service portfolio of mobile device management, mobile application management, and mobility lifecycle services. These are shown below and further discussed in the following subsections. Sections in red font are required capabilities, features or attributes. These requirements will be impacted in the future by the release of the Mobile Security Requirements in the Digital Government Strategy 9.2 guidance.

Managed Mobility Framework



2.1.1 Scope / Scale

The respondent's solution should be scalable from 10,000 managed devices and higher.

2.1.2 Multi-Tenancy

The proposed solution must be able to support the Department's / Agency's ("tenants") hierarchical organizational structure within the solution, and support multiple configurations for each of the MDM requirements below. For example, each tenant may have different help desk contact information, policies, and organizational groupings and hierarchy.

2.1.3 Solution Security

Data at rest encryption, data in transit encryption (VPN), and secure applications are included in the short-term requirements for this MDM-MAM solution. These capabilities may be accomplished by separate products which are then integrated into the complete MDM-MAM solution.

The respondent must describe how the solution meets the following general controls / capabilities.

1. Ability to enroll a device before applying any policy (null policy)
2. Ability to create Whitelist / Blacklist for device enrollment to include OS versions and device models
3. Allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or to groups under the MDM
4. Ability to use an existing MDM user attribute repository for enrollment to the new MDM system
5. MDM has native ability with active (device scanning) and passive (on-access scanning) tools to detect, report, and alert on a compromised device (e.g.: jail broken / rooted device, malware) and take action based upon compliance rules
6. Ability to lock the device or to erase (wipe) 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 instruction from MDM (manual)
7. Password policy enforcement:
    - Minimum complexity (length, composition, common words, etc.)
    - Password lifetime limit
    - Password re-use limits
    - Password inactivity timeout (grace period) for device and MDM app
    - Report password failures beyond threshold to MDM
    - Maximum password attempts before lock or wipe
8. Ability to mask passwords when they appear in the Management GUI
9. Ability to determine which administrative user made a configuration change in the MDM administrative environment
10. Ability to determine which device user made a configuration change in the MDM console (self-service logging)
11. 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

12. Ability to read/send (Encrypt and Signed) messages that use PKI or S/MIME encryption, where email functionality is delivered by the solution
13. Ability to restrict 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
14. (Optional) Ability to view the current GPS location of a device or logical grouping of devices on a map

2.1.3.1 FISMA Requirements

The MDM solution must be certifiable at a FISMA Moderate Impact level (NIST SP 800-53 Moderate or DoD 8500.2 MAC II) or higher. The response may include proof of certification, accreditation, or Authorization to Operate (ATO) in a federal environment, or a plan and timeline for achieving certification and/or Authority-To-Operate (ATO).

2.1.3.2 FIPS Requirements

The solution must protect control and management data in transit between the MDM and the device using FIPS 140 certified cryptographic modules.

The respondent must submit with their response 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. The respondent must provide evidence of the solution's 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.

2.1.3.3 Containerization

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. If the solution provider uses containers, respondents must describe how the proposed solution 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

2.1.3.4 IPv6 Support

IPv6 compliance is a goal for this request. On-premise portions of the MDM solution must 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 respondent must provide a description of the IP based components of their solution and the status (compliant or non-compliant) of the proposed solution. If the proposed solution is not compliant at time of response submission, the respondent shall provide an estimated timeline to achieve IPv6 compliance.

2.1.3.5 User Authentication

The proposed solution for the device must support PIN or password authentication for the managed applications. Policy should also be able to enforce a device PIN.

The respondent must include a web management portal as part of their proposed solution, and the web management portal must be capable of PIV / CAC 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. Respondents 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 – Something the user knows, like a 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, iris or facial image

2.1.3.6 User Compliance

The respondent must demonstrate the following capabilities. The proposed solutions are required to enable the:

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 specify application info for an application compliance rule
4. Ability to 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

2.1.3.7 Alerting

The following alert capabilities are required to notify agency operations staff about devices under their management. The solution must demonstrate the following capabilities:

1. Ability to set up custom alerts to users and management based upon various parameters
2. Ability to send custom alerts to one or more user roles including administrators
3. Ability to specify a creation policy for custom alerts to include having various alert severity levels
4. Ability to have automated alerts for security issues such as compromised devices
5. Ability to create alerts based upon device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.
6. Ability to view alerts pending acknowledgement
7. Ability to acknowledge alerts and track acknowledgement
8. Ability to search and run reports on alerts

2.1.3.8 Reporting

The solution must demonstrate the following capabilities:

1. Ability to run reports by device, profile, provision details, or compliance status
2. Ability to subscribe to a Report (automatic generation and delivery on a schedule)
3. Ability to schedule a Report (Monthly, weekly, daily, etc.)
4. Ability to print a Report using a printer
5. Ability to print a Report to a file
6. Ability to report on devices that haven't communicated with the MDM in a period of time
7. Ability to report all policy compliance status details of devices under MDM management
8. Ability to view reports in HTML5 dashboards from tablets or mobile devices.

The solution must be able produce the following types of reports:

2.1.3.8.1 Audit reports

Audit reports provide data necessary to monitor, reconcile, and audit system processing and reconciliation activities. Audit reports will be run as needed, exportable and will support the following filters:

1. Administrator activity (admin actions performed, time stamps, etc.)
2. User access times and enrollments
3. Participating Agencies (number of devices by Agency and across all Agencies)
4. Devices (number of devices, type, OS version, etc.)
5. Console logins and functions (connections to the management console, actions performed, etc.)
6. Policy changes and versions (policy revision control and historical changes)

2.1.4 Privacy

The proposed solution must not display advertisements to end users of the Information System as part of its business model (i.e. not an advertising-based model).

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

2.1.5 Service Delivery Model

The MDM Solution must 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 will running in the a non-government hosted cloud data center. The respondent must show how they provide all required hardware to the network edge of their cloud data center. The respondent 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 respondent's cloud data center. It is anticipated that the respondent will provide all required hardware to the network edge of their cloud data center. The respondent will clearly describe all HW/SW components that will be within federal Government data center and those components within the respondent's cloud data center. The respondent 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).

2.2 Mobile Device Management (MDM)

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. Products that support MDM are evolving rapidly at this time.

The respondent is asked to describe how the proposed solution meets the following general requirements:

1. Ability to enforce enterprise rules while allowing Agency/Bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities
2. Ability to take the following action upon a group of devices from a search: Reassign to Group (any type of logical grouping). User or device groupings are an example.
3. Ability to assign Profile to one or many Groups (any type of logical grouping). User or device groupings are an example.
4. Ability to view required applications from the Mobile Application Store (MAS)
5. Ability to view and run reports on user and device information for all Smartphones including usage and cost
6. Ability to run reports by groups of users to include location
7. Ability for the solution to support a Software Development Kit (SDK) or Application Programming Interface (API) Framework to integrate with existing or future Enterprise Applications
8. Ability for the MDM solution to be able to be monitored from industry standard tools (e.g. HP OpenView, SCOM, etc.)
9. Ability for the MDM solution to integrate certificates from the solution's internal PKI system to mobile devices as well as third party public PKI providers such as VeriSign
10. Ability for the 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).

2.2.1 Device Enrollment

Enrollment adds a device to the MDM management domain. The respondent must demonstrate that the proposed solution meets the following required capabilities:

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 to specify minimum OS version for profile provisioning
4. Ability for Target Device Ownership (GFE, Personal etc.) to be used for profile provisioning
5. Ability to edit any field for a "live" or "active" profile
6. Ability for a user with appropriate authorization to self-enroll an agency or BYOD device
7. Ability to centrally manage multiple devices for a single user (user device view)

8. Ability to have different policies or grouping for multiple devices under one user (i.e.: tablet policy, phone policy)
9. Ability to apply multiple policies to devices simultaneously (user is member of group policy X, with device policy Y) – when multiple controls conflict, the most restrictive control takes precedence
10. Ability to use external directory service repository for enrollment
11. Ability for system to require users have read policy and signed agreement for enrollment
12. Ability to set support email and phone information for registration messages
13. Ability to set a URL to redirect user to upon successful enrollment
14. Ability to edit an enrollment activation notification message to the user (email and/or SMS)
15. Ability to set a default Device Ownership type upon enrollment for different groups
16. Ability to use internal user list for enrollment for different groups
17. Ability to set support email and phone information for registration messages for different groups
18. Ability to edit an enrollment activation notification message to the user or group of users (email and/or SMS)
19. Ability to send a user or group an activation enrollment message (email or SMS)

2.2.2 Device Profiles

The solution must support the creation of per-user and per-group device profiles. Features and capabilities to be controlled appear in the next section.

The solution must demonstrate the following profile capabilities:

1. Ability to create a profile template
2. Ability to copy profiles
3. Ability to edit a "live" or "active" profile
4. Ability to set Profile Removal Permission (who can remove a profile from a device or user)
5. Ability to set Profile Start Date (when the profile starts applying to associated devices)
6. Ability to set Profile End Date (when the profile stops applying to associated devices)
7. Ability for an edited profile to automatically update devices that currently have the profile
8. Ability to push a profile to any individual device
9. Ability to automatically remove profiles from devices whose state changes from qualifying to not qualifying. This may happen as a result of changing a profile to be more exclusive.
10. Ability to support multiple profiles being applied to a single device (most restrictive rules apply)
11. Ability to delete a profile from the MDM system
12. Ability to set a description for a profile
13. Ability to manage the following via a profile:
    a) Allow installing applications
    b) Control use of camera

   c) Control use of installed applications, including default applications
14. Allow multiple Wi-Fi configurations for multiple profile's
15. Ability to manage device Wi-Fi settings via a policy via a MDM policy
16. For a profile: Control Wi-Fi Security Type: None, WEP, WPA/WPA2, Enterprise (any)
17. For a profile: Ability to support multiple VPN configurations for a profile.
18. For a profile: Support VPN Connection (or Policy) Type: IPSec (Cisco), Juniper SSL, FS SSL, and Custom SSL, etc.
19. For a profile: Ability to support a VPN connection Proxy for a VPN configuration
20. Ability to support multiple email/calendar/contact configurations per profile
21. Allow multiple Web Clip / Web Shortcut configurations per profile

2.2.3 Device Feature Management

The solution must be able to control the following features / capabilities at a minimum:

1. Multi-OS Support – Manage multiple operating system devices such as RIM's BlackBerry, Apple's iOS, Google's Android, Microsoft's Windows Phone, etc.
2. Device passcode enforcement (complexity, length, presence)
3. Installation of applications (See Mobile Application Management (MAM))
4. Camera (enable / disable)
5. Control all radios / communications:
   - Wi-Fi (enable / disable)
   - Bluetooth (enable / disable)
   - Near Field Communication (NFC) (enable / disable)
6. Ability to enable or disable specific hardware component and uses: Enable blue tooth headphone, disable Bluetooth keyboard
7. GPS (enable / disable)
8. Store enterprise data to removable media (disable)
9. (Optional) Roaming (enable / disable)
10. (Optional) – Microphone (enable / disable)
11. (Optional) – Geofencing for device features; enable or disable features based on device location

2.2.4 Data Management

Data Management is the ability to read, write, transmit and receive data on mobile devices as well as with backend systems/repositories.

2.2.4.1 Data Collection

The solution must 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

2.2.4.2 Continuity of Operations and Disaster Recovery

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

2.2.4.3 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 respondent 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 respondent must also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and file servers.

2.2.4.4 Personal Information Management

The respondent must 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 respondent 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.

2.2.5 Security Content Automation Protocol (SCAP) Support

SCAP provides the ability to automate security checks and configuration. Respondents must describe the SCAP support for the server-side components in your solution, including asset management, configuration management, patch management and remediation capabilities. The request is only considering server SCAP support at this time. SCAP for devices is not currently a requirement.

2.2.6 Device 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

Please identify which of the above elements can be automatically populated with the MDM solution.

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

2.2.7 Device Inventory Reports

The solution must 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)

2.2.8 System Performance Reports

The solution must 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

2.2.9 MDM Security / Compliance Reports

The solution must 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

2.2.10 (Optional) Quality of Service (QoS)

The solution may 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.

2.2.11 (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.

2.2.12 (Optional) PIV / CAC Support

Respondents may optionally offer solutions that support the management of PIV / CAC cards on mobile devices via the MDM.

2.2.13 (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.

2.2.14 (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 may 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.)

2.3 Mobile Application Management (MAM)

2.3.1 Application Deployment

The solution must 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)

2.3.2 Mobile Application Store (MAS)

The solution must 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.)

2.3.3 Application Security

2.3.3.1 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.

2.3.3.2 Application Installation Control

The respondent must 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.

2.3.3.3 Blacklisting / Whitelisting

The solution must 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.

2.3.3.4 Application Environment Requirements

The solution must 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")

2.3.3.5 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.

2.3.4 (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.

2.3.1 (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.

2.4 Mobility Life Cycle

2.4.1 Implementation / Installation

2.4.1.1 Project Management

The respondent 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.

2.4.1.2 Deployment / Migration / Transition

The respondent 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 respondent 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 respondent must submit a Transition Plan that details how devices previously supported by the respondent 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. The proposed solution will receive additional consideration if example transition plans from previous MDM deployments are supplied.

The respondent 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.

2.4.1.3 Enterprise Systems Integration

The respondent 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.

2.4.1.4 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 respondent 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.

2.4.2 Operations Support

2.4.2.1 Help Desk

The respondent 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.

2.4.3 Demonstration Platform

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

2.4.4 (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 respondent should describe the services they offer of this type. Each configuration service offered must be accompanied by a successful example from industry or government.

2.4.5 (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. Respondents 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

2.4.6 (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 respondent 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 respondent 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.

2.4.7 (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 respondent may offer logistical support for device replacement, such as pre-enrolling devices at a depot, etc.

2.4.8 (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. Response should indicate experience, willingness, resources, and ability to provide these services.

3 Pricing

Although pricing submission is not required for this particular request, as it is simply a Request for Technical Capabilities, pricing that is available through any publicly accessed source may be submitted as part of this overall Managed Mobility effort. Publicly available pricing includes releasable information found, for example, in GSA Advantage, GSA eLibrary, FPDS-NG.

We encourage respondents to indicate for us the range at which their product is sold to their federal customers, inclusive of the discounted rate that you offer your best federal customer. We recognize that not every federal customer purchases solutions identically, and often pricing is dependent specific agency needs and requirements. The intent here is to indicate the range of potential pricing, subject to the particular requirements that fall beyond the specifications of this RFTC. Please submit a pricing table which reflects the price structure and currently listed prices for your solutions on Federal contracts/task orders.

For those respondent's 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 respondent's IT Schedule 70 contract, the solution must currently reside on that contract vehicle to be considered. If the solution cannot be identified on the respondent's IT 70 contract it will not be considered for assessment at this time.

4 Instructions

The purpose of this Request for Technical Capabilities (RFTC) is to identify solutions from providers that address the common federal requirements listed above. This process will result in the identification of one or more qualified solution providers for service offerings related to Managed Mobility and other related services as outlined in Section 2, and identify the means for ordering activities to reach these solution providers through existing government-wide contract vehicles. GSA may facilitate orders and solicitations issued under existing acquisition vehicles (such as IT Schedule 70, Connections II, or FSSI Wireless) either directly or through a virtual storefront.

Only solution providers who map offerings to their existing government-wide acquisition vehicles will be considered.

The Close Date for responses is 11:00 PM (EST), March 8 2013. Responses shall be submitted to GSA PMO POC Jon Johnson (jon.johnson@gsa.gov) and Contracting Specialist John Malloy (john.malloy@gsa.gov). Late responses will not be accepted or assessed. The electronic time stamp on response submitted via email shall determine timeliness of response.

This RFTC does not obligate the Government to pay any costs incurred in the submission of any response or in making necessary studies for the preparation thereof, nor does it obligate the Government to procure or contract for said services.

4.1 Virtual Industry Day

GSA will hold a **virtual industry day at 9:30 am EST on Wednesday February 6, 2013** to address the questions submitted. The Industry Day will occur virtually via WebEx. You must submit an expression of interest to Jon Johnson (jon.johnson@gsa.gov) who will then send information by close of business on Tuesday February 5, 2013. The objective of the industry day will be to give a better understanding of its purpose of this effort, walk through the requirements, and to provide context for questions potential respondents may have.

4.2 RFTC Questions

Submit all questions concerning this RFTC in writing by 11:59 PM (ET), February 8, 2013 to the PMO POC at the following email address: jon.johnson@gsa.gov. The Government will publish questions and answers (without attribution to the company submitting the question) on fedbizopps within a reasonable timeframe giving particular consideration to the response submission due date and time.

In posing questions, respondents must cite the relevant section, paragraph, and page number. Questions should be written in a way that enables clear understanding of the respondent's issues or concerns. Statements expressing opinions, sentiments, or conjectures are not considered valid inquiries and will not receive a response. Further, hypothetical questions aimed at receiving a potential "assessment decision" will not be entertained.

4.3 Response Content

The solution provider shall respond to all requirements specified in the RFTC. By submitting a response you are representing that your firm has performed all the requirements and therefore it is not necessary or desirable that this be repeated in your response. Do not merely reiterate the objectives or reformulate the requirements specified in the RFTC. A response that only restates the requirements or statements from this request, or just simply states that it is compliant with the request without providing a description of the approaches, techniques, or solutions may be considered unsatisfactory.

A complete response shall consist of the following sections:

1) Executive Summary
2) Table of Contents
3) Technical Section

Please submit Technical Sections in the following order.

1: Security Requirements
2: Common Technical Requirements (MDM)
3: Common Technical Requirements (MAM)
4: Past Experience Requirements

Those requirements identified as optional requirements will be considered only after the mandatory requirements appear to have been met.

4) Approach to MDM/MAM Acquisitions
5) Price Section

Response Format - The response shall be legible, single-spaced, 1" margins, and in a Times New Roman, 11-point type size font, printable to 8 ½ x 11 inch paper. The pages of the response shall be separately numbered. The footer of each page submitted in response shall include the company name of respondent. Diagrams must be with a minimum 8-point font size text. If a response exceeds the page limitations, only the pages within that limit will be assessed. Respondents are encouraged to directly reference other segments of their response where appropriate.

4.3.1 Executive Summary (2 Page Limit)

Submit a concise executive summary of the entire response and a highlight of any key or unique features. Any summary material presented here shall not be considered as meeting the requirements for any other part or section of the response.

The executive summary shall identify whether the respondent is a small business, small-disadvantaged business, Section 8(a) business, woman-owned small business, HUBZone small business, veteran-owned small business, service-disabled veteran owned small business, as well as federally recognized Native American tribes or tribal organizations. Further, the executive summary shall identify all the government-wide contractual vehicles under which the solutions can be procured. The executive summary must include your Federal Tax Identification Number (TIN) and Data Universal Numbering System (DUNS) number. Provide the name, title, telephone number, fax number, and E-mail address for the individual authorized/designated to represent the firm.

4.3.2 4.2.2 Table of Contents

The response shall contain a master table of contents that contains topics and page numbers only.

4.3.3 4.2.3 Technical Section Instructions (75 Page Limit)

Each respondent shall propose solutions to the mandatory requirements. Further, the response must identify how the solution meets the requirements in each of the use cases listed in the appendix.

If the Technical Section exceeds the page limitation set forth, the excess text may not be assessed.

4.2.3.1 Technical Requirements Reference

The Technical Section shall address the specific requirements listed in the RFTC**. The Technical material should be provided in the order contained in the tables on the following pages:**

Table 1

General Managed Mobility Requirements & Past Experience (Common for All Respondents) These characteristics represent core capabilities that must be present in order to provide Managed Mobility services to Federal Customers based on the common requirements developed by the inter-agency working group. All questions in this section require a Yes answer in order for the assessment to proceed further. Respondents should answer the questions, affirming their capability to meet the

requirements, and provide a short description of how they have done so.			
High Level Architecture Requirements & Respondent Capabilities/Experience	**Required or Optional**	**RFTC Section 2 or other Reference**	**Use Case Reference**
1. Scope/Scale: Is the respondent's solution scalable from 10,000 managed devices and higher? (Y/N)	Required	2.1.1 Scope / Scale	6
2. Multi-Tenancy: Does the proposed solution support the Department's / Agency's ("tenants") hierarchical organizational structure within the solution, and support multiple configurations for each of the MDM requirements? (Y/N)	Required	2.1.2 Multi-Tenancy	
3. Solution Security: Does the proposed solution describe how they meet the 14 identified general controls/capabilities of solution security? (Y/N)	Required	2.1.3 Solution Security	
4. FISMA: Does the respondent provide evidence that the proposed solution is capable of being certified at the FISMA moderate impact level? (Y/N)	Required	2.1.3.1 FISMA Requirements	
5. FIPS Requirements: Does the respondent provide evidence that their solution uses FIPS 140 certified cryptographic modules and continued validation? (Y/N)	Required	2.1.3.2 FIPS Requirements	
6. Containerization: If applicable, does the respondent describe how the proposed solution meets FIPS 140-2, controlled wipe capabilities, and platform-by-platform container protection as it related to BYOD scenarios? (Y/N)	Required	2.1.3.3 Containerization	2,3
7. IPv6 Support: Does the respondent provide evidence of either IPv6 compliance or intention to comply? (Y/N)	Required	2.1.3.4 IPv6 Support	
8. User Authentication: For cloud-based systems, does the respondent provide evidence of being capable of meeting authentication standards related to the portal and device, as well as 2 multifactor authentication methods? (Y/N)	Required	2.1.3.5 User Authentication	2,3,10
9. User Compliance: Does the proposed solution demonstrate the 4 items related to user compliance enablement? (Y/N)	Required	2.1.3.6 User Compliance	1,2,4,5,6,7
10. Alerting: Does the proposed solution demonstrate the 8 alert capabilities required to notify agency operations staff about devices under their management? (Y/N)	Required	2.1.3.7 Alerting	2,6
11. Security Reporting Capabilities: Does the proposed solution demonstrate the 8 reporting capabilities, as well as the stated support functions	Required	2.1.3.8 Reporting & 2.1.3.8.1 Audit reports	3,5,6,8

applicable to Audit Reports? (Y/N)			
12. Privacy: Does the proposed solution disclose privacy-impacting features that cannot be disabled? (Y/N)	Required	2.1.4 Privacy	3
13. Service Delivery Model: Is the proposed solution delivered and (optionally) hosted by the provider as a full solution including all hardware, software, hosting, and installation services, using one or more of the following hosting models: (on premise, Cloud, Hybrid)? (Y/N)	Required	2.1.5 Service Delivery Model	

Table 2

MDM Requirements & Respondent Capabilities/Experience	Required or Optional	RFTC Section 2 or other Reference	Use Case Reference
1. General MDM Capabilities: Does the proposed solution address/describe how their solution meets all 10 of the mandatory general MDM requirements? (Y/N)	Required	2.2 Mobile Device Management (MDM)	
2. Device Enrollment: Does the proposed solution demonstrate the 19 capabilities identified regarding the ability to add a device to an MDM management domain? (Y/N)	Required	2.2.1 Device Enrollment	1,2,3
3. Device Profiles: Does the provider support the 21 items related to the creation of per-user and per-group device profiles? (Y/N)	Required	2.2.2 Device Profiles	1,2
4. Device Feature Management: Does the proposed solution demonstrate the 7 required features and capabilities identified regarding device feature management? (Y/N)	Required	2.2.3 Device Feature Management	
5. Data Management: Does the proposed solution demonstrate the ability to read, write transmit and receive data on mobile devices as well as with backend systems/repositories? (Y/N)	Required	2.2.4 Data Management	
6. Data Collection: Does the proposed solution demonstrate the ability to collect and report on the 6 data points identified? (Y/N)	Required	2.2.4.1 Data Collection	
7. Continuity of Operations and Disaster Recovery: Does the proposed solution describe how it performs Continuity of Operations (COOP) and Disaster Recovery (DR)? (Y/N)	Required	2.2.4.2 Continuity of Operations and Disaster Recovery	
8. File Management: Does the proposed solution demonstrate that the solution is able to hold a set of COTS and/or enterprise applications with respective data/files in a single secured space? Does the proposed solution also demonstrate how the solution is able to share files between applications, between	Required	2.2.4.3 File Management	

mobile devices, and/or between devices and hosted file servers? (Y/N)			
9. **Personal Information Management:** Does the proposed solution demonstrate the solution's ability to provide/enable a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection? (Y/N)	Required	2.2.4.4 Personal Information Management	
10. **Security Content Automation Protocol (SCAP) Support:** Does the proposed solution demonstrate the ability to support server-side components, including asset management, configuration management, patch management and remediation capabilities? (Y/N)	Required	2.2.5 Security Content Automation Protocol (SCAP) Support	
11. **Device Inventory Management:** Does the proposed solution demonstrate the ability to 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? Does it record, track and manage the 16 pieces of information identified in inventory management? (Y/N)	Required	2.2.6 Device Inventory Management	1,2,3,6,7,8
12. **Device Inventory Reports:** Does the proposed solution demonstrate the ability use the identified filters to run or export device inventory reports associated with the device, OS, and applications? (Y/N)	Required	2.2.7 Device Inventory Reports	6
13. **System Performance Reports:** Does the proposed solution demonstrate the ability to run system performance reports using the identified filters? (Y/N)	Required	2.2.8 System Performance Reports	
14. **MDM Security/Compliance Reports:** Does the proposed solution demonstrate the ability to run MDM security/compliance reports using the identified filters? (Y/N)	Required	2.2.9 MDM Security / Compliance Reports	6
15. **Quality of Service (QoS):** Does the proposed solution demonstrate the ability to support QoS capabilities to prioritize real-time or latency-sensitive application data where appropriate (e.g.: VoIP, video, real-time chat)? Does the proposed solution also enforce and exclude QoS priority by application or protocol to prevent non-real-time applications from inappropriately increasing their traffic priority? (Y/N)	Optional	2.2.10 (Optional) Quality of Service (QoS)	
16. **Classified Data:** Does the respondent describe the ability of the proposed solution to access classified data up to the SECRET level via a mobile device? (Y/N)	Optional	2.2.11 (Optional) Classified Data	

17. PIV/CAC Support: Does the respondent adequately describe how the proposed solution is capable of supporting the use of PIV/CAC cards to support digital signatures, encryption, or access to enterprise resources? (Y/N)	Optional	2.2.12 (Optional) PIV / CAC Support	10
18. Biometric Support: Does the respondent demonstrate the ability for the proposed solution to offer biometric support such as fingerprint or face recognition? (Y/N)	Optional	2.2.13 (Optional) Biometric Support	
19. Network Monitoring: Does the respondent demonstrate the basic diagnostic functions related to monitoring device network quality and performance?	Optional	2.2.14 (Optional) Network Monitoring	

Table 3

MAM Requirements & Respondent Capabilities/Experience	All Required	RFTC Section 2 or other Reference	Use Case Reference
1. Application Deployment: Does the proposed solution demonstrate the ability to support the 5 controls and capabilities identified for application deployment? (Y/N)	Required	2.3.1 Application Deployment	1,2,4,6,7
2. Mobile Application Store: Does the proposed solution include a Mobile Application Store that allows users to select private enterprise applications for installation on managed devices, integrated into the Managed Mobility MDM portal, which allows application provisioning by group policy and mandatory application deployment? (Y/N)	Required	2.3.2 Mobile Application Store (MAS)	2
3. Mutual Authentication: Does the proposed solution demonstrate the ability for applications to mutually authenticate to ensure the communications channel is not intercepted? (Y/N)	Required	2.3.3.1 Mutual Authentication	
4. Application Installation Control: Does the proposed solution demonstrate the solution's process to support relevant authorizations and approvals (including change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance, including the ability to monitor application usage? (Y/N)	Required	2.3.3.2 Application Installation Control	1.2.6,7
5. Blacklisting/Whitelisting: Does the proposed solution demonstrate the capability, managed through user and group policies, to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting)? (Y/N)	Required	2.3.3.3 Blacklisting / Whitelisting	2,5
6. Application Environment Requirements: Does the proposed solution demonstrate the capability to detect and enforce device environment conditions such as those listed? (Y/N)	Required	2.3.3.4 Application Environment Requirements	2

7. Application Signing: Does the proposed solution support requiring digital signatures for application installation? (Y/N)	Optional	2.3.3.5 Application Signing	
8. Third-Party Application mutual Authentication: Does the proposed solution offer the ability to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc…? (Y/N)	Optional	2.3.4 (Optional) Third-Party Application Mutual Authentication	
9. MAM Software Integration: Does the solution demonstrate the ability to deliver new or existing applications to mobile devices? (Y/N)	Optional	2.3.1 (Optional) MAM Software Integration Services	

Table 4

Mobility Life Cycle Management	All Required	RFTC Section 2 or other Reference	Use Case Reference
1. Project Management: Does the proposed solution 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? (Y/N)	Required	2.4.1.1 Project Management	
2. Professional Services: Does the respondent clearly describe how they provide initial deployment support services including installation, configuration, and the certification of initial solutions, as well as for additional professional services to support specific agency related integrations or customizations? (Y/N)	Required	2.4.1.2 Deployment / Migration / Transition	
3. Enterprise System Integration: Does the respondent demonstrate experience in providing the steps necessary for deploying and integrating a mobility solution into an enterprise-wide environment? (Y/N)	Required	2.4.1.3 Enterprise Systems Integration	
4. Training: Does the respondent demonstrate how they can be responsible for developing and updating the MDM-MAS Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan? (Y/N)	Required	2.4.1.4 Training	
5. Operations Support: Does the respondent/solution provide access to help desk support that meets the identified criteria? (Y/N) Does the respondent indicate the location of their help desk support? (Y/N)	Required	2.4.2 Operations Support	
6. Demonstration Platform: Does the proposed solution possess a demonstration platform to educate potential customers on the use, benefits and technical specification of the solution, and will it provide access to the portal for the purpose of sampling and demonstrations that will be connected to the respondent's site through a federal website? (Y/N)	Required	2.4.3 Demonstration Platform	

7. Enterprise Configuration: Does the respondent demonstrate the non-core integration services as indicated? (Y/N)	Optional	2.4.4 (Optional) Enterprise Configuration	
8. Integration with FSSI Wireless Portal: Does the respondent demonstrate how to integrate their proposed solution with the FSSI Wireless portal to automatically retrieve asset and plan data, and return relevant data to the FSSI portal?	Optional	2.4.5 (Optional) Integration with FSSI Wireless Portal	
9. Telecommunication Expense Management System (TEMS): Does the respondent demonstrate how their proposed solution addresses the identified TEMS functions? (Y/N)	Optional	2.4.6 (Optional) Telecommunications Expense Management System (TEMS)	
10. Device Replacement/Refresh: Does the respondent offer logistical support for device replacement as indicated? (Y/N)	Optional	2.4.7 (Optional) Device Replacement / Refresh	
11. Device Disposal & Reporting: Does the respondent indicate experience, willingness, resources, and ability to provide these services as indicated? (Y/N)	Optional	2.4.8 (Optional) Device Disposal & Reporting	

4.3.4 Approach to MDM/MAM (Required – 1 Page)

Each respondent must submit an acquisition architecture that indicated all government-wide acquisition vehicles under which their proposed solution may be procured. Map the particular offerings to how they are identified under each vehicle. Examples of government-wide vehicles include IT Schedule 70 Contracts and GWACs.

4.3.5 Pricing Section (No page limit)

Please submit pricing in accordance with the guidelines set forth in Section 3.

5 Assessment

Responses will be assessed according to the following criteria:

1. Completeness and Correctness of Required Capabilities
    - Capabilities are met, with evidence of existing deployment of the technical components
2. Evidence of Enterprise Integration and Past Experience
    - The response provides examples and evidence of previous integration of the solution into large-scale enterprises (non-Government examples permitted for integration)
3. FIPS/FISMA Components
    - Examples are provided where each of the technical components have received an FIPS Certification and/or a FISMA Authorization.

Additional consideration will be given to the requested optional capabilities.

Solutions that meet the required criteria above will be found capable of fulfilling the outlined requirements to satisfy the greatest governmental need as determined against the common set of GSA Managed Mobility Program requirements found in this document (Section 2). The list of capable solutions, the devices and versions they apply to, the acquisition vehicles available to procure these solutions, and vendor and contract information will be made available to agencies seeking Managed Mobility services via the GSA Managed Mobility website and the GSA Innovation Center Website.

<u>Assessment Appeal</u>

If a solution set has been assessed and is not found capable the respondent will be notified and have an option to appeal the finding of the assessment team. No additional information will be permitted to be submitted, but an independent member of the GSA Mobility Team or Federal Mobility Working Group who had not reviewed the respondent's submission will review the materials and make a decision as to whether the respondent can be found capable of fulfilling the outlined requirements to satisfy the greatest governmental need against the common set of requirements. No further appeals will be allowable.

GSA anticipates releasing follow-on requests for capabilities periodically, and plans to update specific requirements with each release. In the event that submissions are not assessed as complete and correct, or not found capable against the requirements as written, the respondent may submit again when GSA releases the next request for capabilities. Follow-on requests will be determined by changes in the commercial market and with redeveloped common federal requirements.

5.1 Completeness and Correctness of Required Capabilities

GSA will solely determine capability based on the evidence provided in the submission and may ask vendors for clarification at its discretion. To assist GSA with assessment, responses should highlight the specified technical criteria met before detailing additional capabilities. The solution must describe how and with what components the criteria are met; it is not sufficient to merely state "we meet this criteria".

5.2 Evidence of Enterprise Integration

The enterprise integration examples must detail how technical tools (such as an MDM solution) are integrated into each of:

1. The enterprise IT systems (mail, etc.)
2. Each other (MDM with inventory management, etc.)
3. The enterprise mobile device management process (process, policy, procedure)

5.3 FIPS/FISMA

In regards to FIPS certification, the government will assess whether the solutions include a FIPS 140-2 certificate number or appears on the NIST "Modules in Process" list.

In regards to FISMA, the government will assess whether the respondent offers evidence of FISMA authorization or has a plan and timeline for achieving an Authorization-to-Operate at the Moderate impact level.

Appendix A Use Cases

The following Use Cases are intended to assist the respondent with architecting a solution that will address the operational requirements of Government Agencies. They are written in a scenario format, with specific requirements highlighted.

Use Case #1 – New Hire

Required capabilities:

1. Multiple group policies per device
2. Automatic application deployment
3. Enterprise Application Management (MAM)
4. Enterprise Application Store (MAS)
5. Enterprise email integration
6. Device data monitoring, location monitoring

A new IRS field agent is hired and issued an agency device. The device is enrolled by the MDM system, and the device is added to the "Field Agents" policy group. This policy automatically pushes a set of required applications to the device, including an MDM agent, email client, agency secure intranet web browser, and enterprise application store, each installed in the secure managed container the MDM agent has set up on the device.

The MDM agent also prompts the user to define required device and container PINs. The new field agent's manager emails her a list of suggested applications to install from the enterprise application store, and recommends a free navigation application from the vendor application store. In a few weeks the new field agent has completed training, and their device is added to a new policy group that pushes the case history application to her device and enables use of the camera to capture document images.

Use Case #2 – Bring Your Own Device (BYOD)

Required Capabilities:

1. Black / Whitelisting
2. Automatic policy control implementation (in this case, location privacy)
3. Role-based access to applications
4. Application utilization, version
5. CAC / PIV authentication to management site
6. Separation of Personal and Business Data

An agency staffer is using a personally-owned device, an Android, to access enterprise data (BYOD). Their manager has approved them in the MDM portal, and assigned them a default device profile. The MDM portal sends an email to the staffer with a link to the portal. The staffer logs in to the portal with their agency PIV card, and is instructed to install the MDM application from the public Google Play application store. After registering their device through the MDM application, the application blocks further connection to the enterprise because the

staffer's device is not at the minimum Android OS version required. After the device is updated to the current OS available from their carrier, the MDM application enables connection to email, contacts and calendar. Since the device is identified as "BYOD" in the MDM management portal, continuous location tracking of the device through the MDM application is automatically disabled. It is still available on-demand if the device becomes lost or stolen.

A few days later the staffer learns of an enterprise application they think may help their work. The staffer attempts to install the application from the enterprise application store, but is denied. They contact their manager, and are told that the application is licensed, so distribution is limited to minimize costs. The manager authorizes the user for the application by adding them to that application's "permit" policy, and the user installs the application. 45 days later the staffer receives an automated email from the MDM that they haven't used the application in 30 days, and if they don't plan to use it to uninstall it as it's a per-user license application. Three months later, the manager receives a notification from the MDM system that their staffer hasn't used this application in over a month.

After discussing with the staffer, the manager discovers the application isn't as helpful as the staffer thought it would be, and they agree to remove it and release the license for the application. The manager removes the staffer from the application "permit" policy, and the application is automatically removed from their device.

Use Case #3 – Lost / Stolen Device (Unrecovered)

Required Capabilities:

1. Remote container wipe
2. Remote device wipe
3. Device location tracking
4. Device status reporting
5. User self-enrollment
6. BYOD provisioning

A GSA employee requests email, calendaring and contacts (Personal Information Management, or PIM) access on his personally-owned device. After management approval, the GSA help desk sends him an enrollment text message to his device. He enrolls his device into the MDM system and downloads the PIM application. The MDM solution requires he lock the device with a strong PIN. One morning he discovers his vehicle has been broken into and his device stolen. He calls the enterprise help-desk to report the loss, and since this is a personally-owned device he is asked for permission to turn on location tracking. The help desk locates the device across town in a location not familiar to the employee, and confirms the device has been locked since the night before. He asks the help-desk to remotely wipe the entire device. The employee reports the device stolen to law enforcement and his carrier, who issues him a new device after he pays a deductible. He contacts the help desk again to have the new device provisioned.

Use Case #4 – New Application Deployment

Required Capabilities:

1. Application selection and approval by either whitelist or blacklist approach
2. Application deployment via Over the Air (OTA)
3. Application deployment via role-based, organization, level, and/or other application policy parameters
4. Application selection and management as a function of enterprise or personal application status

Agency employees may select and download mobile applications based on their agency or organization's specific policy which may represent whitelist (approved application meeting a certain criteria) or blacklist (any application except those specified). Additional mobile application accessibility and mobile application management functionality may also reflect other agency policies including role/function (defined by OPM position # or agency), organization (agency, sub-agency, location, region, etc.), device ownership status (government, employee, other) and employee level (e.g. rank, pay scale, etc.).

The agency may also dictate application release management and application access to data as a function of the agency application policy.

Use Case #5 – Blocking of Inappropriate Website

1. Site blacklisting
2. Application blacklisting
3. Reporting possible erroneous filtering / blocking

A user receives an email from a colleague with several URLs taken from a web forum posting that address an area of interest to the user. The user selects each URL in turn on her device to view the content. The first link is uninteresting, but when she selects the second link her device informs her access is prohibited as it is listed as a gambling site. She observes that the link is a misspelling of a common web site, and successfully tries manually entering a corrected link. The third link produces a message that the requested site is blocked for containing malware. Noting the URL is a .EDU website at a major university and suspecting this is an error, she selects the option to have the URL manually reviewed.

Use Case #6 – Security Problem Identified on Device

1. Ability to perform application installation in stages
2. Ability to control application installation via cellular or WiFi
3. Deployment policy for applications and device policies
4. Ability to report application presence on devices

5. Ability to define a policy for specific device types, operating system versions, or combinations of device configurations or settings

A new SMS attack on Android devices is announced, and the Agency has more than 10,000 devices that are on the list of vulnerable targets. The Agency identifies and tests an on-device SMS-filtering solution and decides on immediate deployment, notifying users via email about the new application. The MDM Administrator loads the approved application into the MDM private application store, associates it as a required application with the group policy governing the affected users, and sets the required OS version. She then has the MDM solution select 10% of the devices and deploy the application with a deployment policy that automatically installs the application if WiFi connectivity is present. After a few hours the MDM Administrator observes several hundred successful installs with no associated help-desk tickets, and instructs the MDM solution to deploy the update via WiFi to all users. After 48 hours 80% of the devices have received the application. The SMS-filtering application is beginning to report actual SMS attacks attempted against devices (an application feature not required of the MDM), and the Agency governance decides that the application should be deployed to remaining users, regardless of the availability of WiFi. The MDM Administrator updates the deployment policy for the application, marking it as required, immediate installation, no connectivity restrictions. Within an hour 97% of the devices are running the new application. The MDM Administrator generates a list of user emails for devices that do not yet have the application installed. The Agency sends an email to the affected users requesting them to facilitate the update immediately, warns them of the threat, and lets them know that SMS will be disabled for their device in two days if the update is not installed. They are advised to contact the help desk for assistance. After two days, the MDM Administrator generates a list of remaining devices without the application and passes it to the service account management team. After receiving approval the account management team disables SMS service on those devices, and informs the MDM Administrator. She sends a notification email to the affected users about the change to their device plans, and directs them to the Help Desk for assistance.

Use Case #7 – Application Update

1. Automatic application updating
2. Custom user notifications and actions for policy events
3. Monitoring and reporting of application versions
4. Specify device state requirements for policy enforcement

A new version of application is available to two users, Fred and Ginger. They both receive messages on their device when they next run the application. They are told the application must be updated before a certain date and are asked they want to install the update now, be reminded later, or not be interrupted with the update message. Ginger chooses to be reminded later, and later that day installs the application update. The MDM application version monitoring system reflects Ginger's updated application in its statistics.

Fred has time-critical tasks to complete, and chooses to not be reminded any more about the update. The device informs him the update will happen automatically after the deadline. He forgets about the update after a few days, and the time limit for installing the update passes. The

application deployment policy will enforce the update automatically, but only when connectivity is over WiFi, to not consume data from the device airtime plan. The MDM agent watches each start of the application, and when it is started while the device has WiFi connectivity, informs Fred that the application will now be updated. The application is updated, the MDM monitoring records the successful update, and Fred's device is now compliant.

Use Case #8 – Lost Device (Recovered)

Required Capabilities:

1. Device Location Tracking
2. User Self-Service

One day a user realizes she doesn't have her Government-Furnished device. In the user self-service portal to the MDM system she looks up her device based on the mobile number and name, and requests the device report its location and status. Since she has been authenticated with her PIV card, the system identifies her as authorized. In a few minutes the device reports its location through the MDM portal. It is at a local library, and there have been no PIN failures (attempted accesses). She notes the address, and instructs the device to display a "lost phone" message with a callback number and sound a tone. The user heads to the library and is able to recover the device.

Use Case #9 – Mobile Law Enforcement or Inspection Worker with Tablet and Custom Application

Required Capabilities:

1. Device Location Tracking
2. Containerized application with ability to synchronize data with enterprise database remotely via secure, encrypted connectivity.
3. Commercial-off-the-shelf tablet computer with cellular service plan and agency-specific application

An agency has an organization of remote and mobile employees that use a tablet computer to record data for both law enforcement and on-site inspection activities. The data is immediately transported via the cellular network to the agency enterprise database where it is recorded and processed for analysis and transactions. Data may occasionally be sensitive but unclassified. Reliable, secure, and compliant communication is required. The agency may periodically push related application updates via Over-the-air as the employees may have limited access to agency buildings and on-site infrastructure.

Use Case #10 – Agency users want to access enterprise applications using their mobile device and/or tablet.

Required Capabilities:

1. PIV card authorizes MDM to create derived credential
2. New logical credential stored in mobile device
3. Maximize reuse of PIV data model

An agency as an organization of remote and mobile employees that use a mobile device and/or tablet computer to access the agency resources must be able to authenticate using their PIV cards. In most cases the mobile device and/or tablet computer may not support a card reader and it may not be practical for the agency user to have to carry around a card reader. The mobile platform must allow an agency to authenticate to agency applications at the appropriate level of assurance for that application.

Appendix B 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.
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).
BYOD	Bring Your Own Device; Staff bring 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.
COTS	Commercial Off-The-Shelf; solutions that can be purchased in a complete form from existing commercial vendors.
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.
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.
Ordering Entity	Any Agency, sub-Agency, state or local government that is using this contract vehicle.
Ordering Agency Portal	The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency. 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.
Subsystem	A subsystem is a set of elements, which is a system itself, and a 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	The receipt of invoices from parties other than the Contractor for services within or outside the

Direct Billing	scope of this agreement.
Trade Agreements Act (TAA)	The TAA of 1979 is an Act of Congress that governs trade agreements negotiated between the U.S. and other countries under the 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.