Managed Mobility Program Frequently Asked Questions (FAQs)

1. What is the Managed Mobility Program?
   A. The Managed Mobility Program offers agencies the information and resources they need to identify and procure centralized management solutions for mobile devices. Mobile Device and Application Management (MDM/MAM) and Mobile Lifecycle & Expense Management (ML&EM) solutions are the focus of this program to date.

2. Why was the Managed Mobility Program created?
   A. GSA was assigned the Managed Mobility Program by OMB as a result of its core strengths in IT and networking, along with its leadership contributions to the mobility components of the Federal CIO's Digital Government Strategy. Item # 5.5 calls on GSA to "develop a government-wide mobile device management program" to support agency acquisition of Managed Mobility solutions. After initially addressing MDM/MAM, the Managed Mobility Program attention is focused on addressing Mobile Lifecycle & Expense Management (ML&EM), adding that component to our program.

3. Is this a new acquisition vehicle?
   A. No, the Managed Mobility Program does not create new acquisition vehicles. This program instead identifies and evaluates solutions that are currently on existing vehicles and can be procured today. The program creates and maintains a list of enterprise-class mobile management solutions that meet the greatest number of government-wide requirements.

4. How will this list change over time?
   A. GSA will periodically re-evaluate both government needs/requirements and the marketplace's ability to address those needs. Some Agencies that are participating in the requirements and assessment selection are: ATF, CMS, DISA, DHS, DoD, DoJ, FBI, NIST, NOAA, USDA, USMC, and GSA.

5. Can I buy a solution not on the list?
   A. Yes! And you can use the Managed Mobility program's central repository, information, and staff to help you buy the solution that best meets your requirements.

6. How do I use the list?
   A. See the Managed Mobility User Guides for details.

7. What solutions are not part of the Management Mobility Program?
   A. IT (non-mobile) equipment and services and IT (non-mobile) focused management solutions are not part of this program. No-charge or purchased mobile devices and associated service plans are part of the FSSI Wireless program, available at www.gsa.gov/wirelessfssi.

8. What were the key factors used to evaluate and select the Managed Mobility solutions?
   A. The program utilized four key factors/areas to evaluate the solutions. These included Technical, Compliance, Acquisition Vehicle, and Experience/Scalability factors. Additional information and details about these factors are provided in the User Guides.

9. Were only solutions from OEM vendors assessed against GSA's Request for Technical Capabilities for MDM/MAM?
   A. No. Solutions from OEM vendors and integrators were assessed. It is expected that as the market and specific solutions evolve, additional solutions would be assessed in the future.

10. How many vendors and integrators were selected and where can I get their names?
    A. The list of selected vendors and integrators is available at www.gsa.gov/managedmobility

11. Are agencies required to procure solutions only on the potential solutions list?
    A. No. The solutions on the list have been carefully evaluated and would provide benefits and lower acquisition, implementation and management costs and risks. However, agencies are free to procure solutions not on this list. If agencies have requirements that are not reflected in this program, they are encouraged to forward those requirements to the Managed Mobility program office to better understand and share future requirements/needs with other agencies. In addition to the solutions listed below, other MDM/MAM and ML&EM partner solutions may also be able to meet an agency's specific needs. No solution can be precluded from competition in compliance with the Federal Acquisition Regulations (FAR). Refer to the User Guide for more information about potential sources of supply and acquisition vehicles.

12. What types of information and tools are available on the Managed Mobility central repository?
    A. The repository can be found at www.gsa.gov/managedmobility and it contains all the information an agency needs in terms of what to consider when procuring an MDM/MAM or ML&EM solution, and potential pathways to procure them. It includes a User Guide, Potential Sources of Supply, FAQs, Fact Sheet, Government-Wide Requirements, White Paper, Success Story, and contact information for Program Expert and Staff.

13. Which federal policies and administrative priorities does this program adhere to?
    A. The program adheres to several, including the following:
    - White House Digital Government Strategy (DGS), dated May 23, 2012
    - Executive Order 13576--Delivering an Efficient, Effective and Accountable Government
    - FISMA, as implemented through NIST SP 800-53 and DoDD 8500.1M

- FIPS 140-2 to protect, control and manage data in transit between the MDM and the device using FIPS 140 certified cryptographic modules

14. Should I buy and integrate multiple MDMs?
    A. You should first consider that generally integration costs are likely to outweigh any functional increase. See the User Guide for details.

15. What key features/capabilities are included in MDM/MAM solutions?
    A. The below table provides information about key features/capabilities.

Mobile Device Management (MDM)	Mobile Application Management (MAM)	MDM Integration
• Device enrollment • Profile provisioning • Profile management • Multi-profiles per device • Feature management • Multi-OS support • Device remote control: track/control, camera/microphone/Wi-Fi, Bluetooth, GPS, roaming, geofencing • Data collection • Secure data files, applications • Multi-account e-mail support • Automated security checks • Provision, control, track devices • Device reporting • COOP and disaster recovery • Wipe data/apps	• Controlled application deployment • Enable/disable commercial app stores • Installed app reporting • Blocking app purchases • App whitelisting/blacklisting • Enterprise mobile app store (MAS) • Mutual authentication • Detect/enforce device environment conditions • Require app digital signatures • Third-party app mutual authentication • Software integration services	• Support for implementation and installation, including deployment, transition, system integration, and training • Operations support such as a help desk, a demonstration platform, and enterprise configuration

16. What are the key features associated with ML&EM?

    Key Features include:

- Bill Payment
- Cost Allocation
- Device Disposition
- Device and Expense Audit Capabilities
- Dispute Resolution
- Expense Management
- Inventory Management
- Invoice Consolidation & Processing
- MDM Integration
- Order Management
- Project Management and Planning
- Service and Device Acquisition

17. Who is the primary contact to get more information about this Program?
    A. 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

18. What FISMA levels do the solutions address?
    A: The assessed solutions are expected to meet FISMA Moderate, according to the specific guidance in the Mobile Device Security Baseline, DGS #9.1.

19. What security capabilities are covered by these solutions?
    A: The security requirements are listed in the MDM/MAM requirements document and the ML&EM requirements document. For further information, please contact the Program Office.