

GSA Managed Mobility Program



Managed Mobility Program

Mobile Device & Application Management User Guide

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

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

1	What is the GSA Managed Mobility Program	3
1.1	Why a Program and Not a Vehicle.....	3
1.2	How the Program Will Evolve Over Time.....	3
2	Potential Sources of Supply	4
2.1	Mobility Management Solutions Table.....	4
2.2	MDM/MAM Platforms	5
2.3	Integrators	Error! Bookmark not defined.
2.4	Pricing	5
3	Assessment Methodology	6
3.1	Technical Factors	6
3.2	Compliance Factors.....	6
3.3	Vehicle Factors	6
3.4	Experience / Scalability Factors	7
4	How to Acquire Solutions	8
4.1	Primary Considerations	8
4.1.1	The Need to Go Mobile.....	8
4.1.2	Mobility Decision Balancing.....	8
4.1.3	Adapting Existing RFTC Requirements.....	9
4.1.4	Solution / Marketplace Limitations	11
4.1.5	Should we buy multiple MDM solutions?.....	11
4.2	Availability on Existing Government-Wide Vehicles.....	11
4.2.1	IT Schedule 70.....	12
4.2.2	FSSI Wireless	12
4.2.3	Connections II	13
4.2.4	GWACS	13
4.2.5	Small Business Set-Asides, Directed 8(a) Set-Asides, and Other Government-Wide Procurement Vehicles	15
4.3	Evaluation Considerations	15
4.3.1	FIPS 140-2 Cryptography Claims	15
4.3.2	Use of Validated Modules Such As OpenSSL	16
4.3.3	Cost Evaluation	16
4.4	Award Execution and Monitoring.....	16
4.4.1	FIPS Attestation	16
5	Post-Acquisition Activities	18
5.1	Feedback to the GSA Managed Mobility Program	18
5.2	Program Manager Contact Information	18
6	Acquisition Assistance	19
6.1	When to call for help?	19
6.2	Program Manager Contact Information	19

1 What is the GSA Managed Mobility Program

The GSA Managed Mobility Program assessed comprehensive cross-agency requirements against Mobile Device Management, Mobile Application Management, and Mobility Life-Cycle (MDM/MAM/MLC) solutions that can be procured today via existing government-wide vehicles and through procurement approaches available to every federal agency. The program creates and maintains a list of potential sources of enterprise-class mobile management solutions that meet the greatest governmental needs.

1.1 Why a Program and Not a Vehicle

The Managed Mobility Program is not a new acquisition vehicle. GSA Managed Mobility leverages existing government-wide procurement vehicles and addresses the Digital Government Strategy 5.5 action item for establishment of a government-wide program for Managed Mobility solutions. The MDM and MAM marketplace is undergoing rapid change, and government agency approaches to mobility are evolving. A new Managed Mobility-specific vehicle may quickly become outdated due to market factors (shakeout, M&A, evolving technical requirements), and not be able to respond to changing needs and capabilities. This program provides analysis, best practices, guidance and a central repository of information for government-wide use.

1.2 How the Program Will Evolve Over Time

The GSA Managed Mobility Program will periodically reevaluate government mobility requirements and reassess marketplace solutions with consideration of government-wide acquisition capabilities. This will result in updates to the list of potential sources of supply identified for agency consideration. All updates to the program will be communicated through the web site www.gsa.gov/managedmobility, and updated Requests for Technical Capabilities will be released through FedBizOps at www.fbo.gov.

GSA acknowledges that functional capabilities and requirements will evolve over time. This evolution can be captured through the existing programmatic structure; however we do anticipate revisiting this programmatic methodology in the future.

Certain requirements for mobility solutions will remain consistent: FISMA / NIST SP 800-53 Compliance, FIPS 140-2 Validated Cryptography Modules, availability on existing government-wide procurement vehicles, and demonstrated deployment of the technology.

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

2 Potential Sources of Supply

Solutions that have been determined to meet the greatest governmental needs against the functional requirements, have been deployed in the federal government, and are verified to be FIPS 140-2 capable are listed alphabetically. We expect that these potential sources of supply should meet the requirements we defined as required and most common across government. Vendor claims should be verified before acquisition. Agencies are free to procure solutions that do not appear below.

2.1 Mobility Management Solutions Table

Mobility Management Solutions (OEMs)	Contact	Demo Site*	Partners/Resellers**	Acquisition Approaches
Afaria (SAP)	Charles Kalajian 874-736-9152 charles.kalajian@sap.com	Demo Page	Accenture Federal, Advantage Solution, CACI, Carahsoft, Delliotte Consulting, EC America, Fultron Inc., ImmixGroup, Karsun Solutions, Klouddata, Oakland Consulting, SAP Government Support and Services, Inc., SAP Public Services, Software Information Resource Corp, Solers, TKC Global Solutions	IT Schedule 70 Alliant GWAC Connections II GWAC GSA 8(a) Stars II SB Set Asides
Airwatch	Mark Williams 703-203-1542 markwilliams@air-watch.com	Demo Page	Sprint, , G4 Government-Solutions, Inc., Ironbow, Shadow-Soft, Unisys, Telecommunication Systems Inc (TCS)	IT Schedule 70 FSSI Wireless BPA Alliant GWAC SB Set Asides
Citrix	Faisal Iqbal (301) 280-0797 faisal.Iqbal@Citrix.com	Demo Page	Global Technology Resources Inc., Accelera Solutions Inc., Convergence Technology Consulting, Force3, DMI, World Wide Technologies, CDW-G, Dell, Immix Group	IT Schedule 70 , Alliant GWAC , Alliant Small Business , 8(a) Stars II , SB Set Asides
Good	Molly Milliken 703-627-1514 Mmilliken@good.com	Demo Page	Accenture, Carahsoft, Computer Science Corp (CSC), AT&T, HP Enterprise Services, SAIC, GDIT, Verizon, T-Mobile, Dell, MicroTech	IT Schedule 70 FSSI Wireless BPA Connections II GWAC Alliant GWAC GSA 8(a) Stars II SB Set Asides
MaaS360 (Fiberlink)	Jeff Ward 434-242-3479 jward@fiberlink.com	Demo Page	Level 3 Communications, The Winvale Group, Patriot Technologies, A&T Systems, ICS Nett, Stratus Dynamics, Cherokee Nation Technologies, Unisys, InfoReliance, Sprint, GDIT	IT Schedule 70 FSSI Wireless BPA Connections II GWAC Alliant GWAC GSA 8(a) Stars II SB Set Asides
MobileIron	Sean Frazier (301) 693-9494 sfrazier@mobileiron.com	Demo Page	AT&T, DMI, Parabal, Triad Technology Partners	IT Schedule 70 , FSSI Wireless , Connections II , Alliant GWAC , SB Set Asides
Symantec	David Hurley (571) 485-0086 David_Hurley@symantec.com	Demo Page	Accenture, Booz Allen, Carasoft, CACI, Computer Science Corp (CSC), Dell, HP Enterprise Services, Lockheed Martin, SAIC, ThunderCat, UnicomGov	IT Schedule 70 , Connections II , Alliant GWAC , 8(a) Stars II , SB Set Asides

* The demo portals are generic demonstrations. We encourage all ordering activities to contact the platform providers for personal demonstrations to determine if they cover all functionality required by the agency or organization.

** This may not be an exhaustive list of partners/resellers. For a more exhaustive list please ensure that you contact the platform provider for details.

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

Mobility Management Solutions (Integrators)	Contact	Acquisition Approaches
Accenture	H. Jacob Brody w: (571) 414-2674 c: (571) 215-9676 h.jacob.brody@accenturefederal.com	IT Schedule 70, Alliant GWAC
AT&T	Ryan Love w: (410) 782.2597 c: (571).533.6959 rl496j@att.com	IT Schedule 70, FSSI Wireless, Connections II, Alliant GWAC
CACI	Phil Ardire w: (732) 460-7802 c: (732) 963-5857 pardire@caci.com	IT Schedule 70, Alliant GWAC
CSC	Siva Prakash Yarlagadda (571) 294-4667 Syarlagadda3@csc.com	IT Schedule 70, Alliant GWAC
HP	David Cook w: (404) 648-2002 c: (678) 549-9583 davide@hp.com	IT Schedule 70, Alliant GWAC, Connections II

2.2 MDM/MAM Platforms

Solutions meeting the greatest government needs are mapped to their acquisition vehicles accessible either directly through the platform providers or through their partner/reseller agreements. The partners/resellers were identified by the platform providers themselves, and the ability to procure solutions through a government-wide procurement vehicle will be dependent on not only the partner/reseller but also the terms and conditions of that underlying acquisition vehicle.

2.3 Pricing

MDM/MAM solution price points can vary depending on an agencies need. Typically basic MDM licensing is low cost and can be approximately \$25 per device or user depending on the company’s pricing structure, but this varies when considering the FIPS-140 container elements. Each OEM solution provider above addresses containerization a little differently, and the type of security posture an agency has will impact the robustness of the containerized solution. The prices can bring the total cost of the MDM solutions from the \$50-\$150 per device or user range. We suggest that you contact the vendors to receive more accurate pricing dependent on the functionality that you will require based on the security posture of your users.

3 Assessment Methodology

The GSA Managed Mobility Program developed requirements with a cross-governmental team composed of CIOs, CISOs, and IT Mobility professionals to identify solutions that met the greatest governmental needs, and could be acquired and deployed immediately through existing government wide procurement vehicles.

3.1 Technical Factors

GSA worked with a number of partner agencies (including DHS, DOJ, DOD, DISA, USDA, and others) to identify functional, security and technical requirements that are common across government. The RFTC constituted the 206 functional and security requirements, as well as optional functionality, to which responses were assessed. Each response was assessed for conformance to these stated requirements by representatives of the cross-governmental team, and the assessments were reviewed for consistently applied interpretations of the requirements and responses before being considered valid. These validated assessments were then compared to one another to determine the market-based threshold for technical sufficiency, and to determine the baseline to indicate those solutions meeting the greatest governmental need.

3.2 Compliance Factors

Two compliance factors were assessed separately: FIPS 140-2 Validation and FISMA Authorization to Operate (ATO).

FIPS 140-2 is the (National Institute of Standards and Technology) NIST standard that addresses the use of cryptographic algorithms in IT systems. A solution was assessed as FIPS 140-2 sufficient if it claimed FIPS 140-2 Validated cryptography was in use for all cryptographic operations, AND that claim could be traced to a listed FIPS 140 Validation Certificate (directly or indirectly), or to the NIST FIPS 140 “Modules in Process” list. Solutions not using FIPS 140-2 Validated are less likely to receive an ATO from Agency leadership, and were excluded as a potential source of supply.

The FISMA ATO factor examined the solution for evidence that either the entire solution, or the key technical elements of it, had received an ATO for FISMA Moderate from a government agency in an actual deployment. This can be a time-consuming and costly exercise, so only solutions that provided evidence they had completed this process were included in the potential sources of supply.

3.3 Vehicle Factors

Because the Managed Mobility Program was not creating a new acquisition vehicle, all solutions that met the other factors must be reachable through existing government-wide contract vehicles. The primary vehicles considered were Alliant, Connections II, and GSA IT Schedule 70, though

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

other vehicles were considered where specified by respondents. Solutions that could not meet this requirement were excluded from the potential sources of supply.

Standalone MDM platforms can be purchased via Schedule 70 or Connections II, both of which are GSA IDIQs. MDM, however, is rarely purchased without integration support due to the need to customize security, policy, and operational components. All GSA GWACs identified as potential sources for procuring MDM solutions and solution sets require an integration component.

3.4 Experience / Scalability Factors

GSA requires qualifying solutions to manage at least 10,000 devices, and offer additional scalability beyond. While initial agency deployments may be lower, the anticipated demand for mobile device usage will routinely exceed that threshold. GSA recognizes that newer technologies may be naturally excluded by this threshold, but felt that this is a necessary trade-off to support solutions that are immediately deployable. New technologies and solutions will be considered when the Managed Mobility Program periodically re-assesses both marketplace solutions and government requirements.

Solutions that demonstrated deployment experience of 10,000 or more devices in industry or government were included in the potential sources of supply.

4 How to Acquire Solutions

The GSA Managed Mobility Program is intended to assist government agencies acquire mobility management solutions more quickly, at lower cost and with less risk.

4.1 Primary Considerations

The mobile mission and policy management are key considerations in MDM selection: What is the agency trying to achieve with mobile, and how does the agency manage organizational policy to support that objective.

4.1.1 The Need to Go Mobile

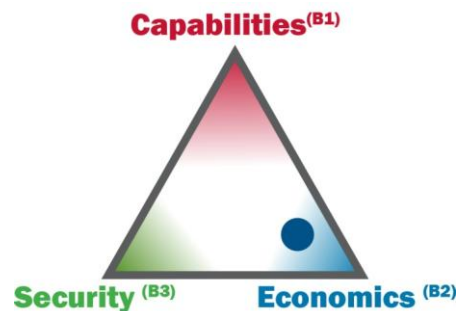
DGS 9.1 includes an excellent guide to determining the extent of mobile device needs vs. desires within an agency. Some of the considerations are:

- How mobility will support the agency mission
- Cost
- Change in security posture
- Productivity impact of increased user mobility
- Agency obligations with increased mobility (contractual compensation requirements when contacting staff off-shift, policy and legal implications of BYOD, etc.)

Please refer to the Mobile Computing Decision Framework in DGS 9.1, available at www.gsa.gov/managedmobility.

4.1.2 Mobility Decision Balancing

Once the mobile capability objective has been defined with respect to the agency mission, the balance of capabilities, economics and security follow. This section of the User Guide offers a cursory overview. For the full process, please refer to the DGS 9.1 Mobile Computing Decision Framework.



The Decision Balance point is represented by the blue dot in the figure above. The closer the Decision Balance point is to a particular factor's vertex, the more critical that factor is to mobile component selection.

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

The three decision balancing factors are defined as follows:

Capabilities: The closer a point is to the Capabilities vertex, the more important the ability to support a wide range of applications and uses becomes. The Capabilities factor reflects the overall flexibility of the device in supporting a wide range of uses. In general, every mobile application that a mission uses requires increased device capability.

Security: The closer a point is to the security vertex, the greater security must be addressed in terms of compliance (policy), threat management, and data integrity. This factor determines the importance of information security to the mission. Some missions, such as those dealing purely with publicly available information, do not require strong security. Other missions, such as those that use Sensitive but Unclassified (SBU) information or Controlled Unclassified Information (CUI) have a strong need for security.

Economics: The closer a point is to the economics vertex, the more important availability, cost, and user familiarity become. Economics includes not only the overall cost of a solution but also training costs and the availability of commoditized components that may be included.

4.1.3 Adapting Existing RFTC Requirements

The GSA RFTC contains 206 functional and security requirements that are ready for agencies to use in their acquisition. These requirements are divided into three areas:

- Mobile Device Management (MDM) – Managing data on devices, and how the devices can use, access and protect that data.
- Mobile Application Management (MAM) – Managing applications running on the device, their installation and removal, and availability through commercial application stores, private enterprise application stores or direct deployment.
- Mobility Life Cycle (MLC) – Requirement necessary to test, deploy and operate a Managed Mobility solution.

Each of these areas has required and desired (optional) capabilities. The required capabilities are those that every surveyed agency indicated was needed to field or operate a managed mobility solution in their enterprise. Desired (optional) capabilities are those that were either advanced capabilities not common in the marketplace, or those that were required by a minority of agency users.

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

2.5 Project Management/Integration/Portal	2.2 MDM	<p style="text-align: center;">Required Capabilities</p> <ol style="list-style-type: none"> 1. General Security / Privacy Functions 2. Device Enrollment 3. Device Profiles 4. Device Feature Management 5. Device Configuration Management 6. Data Management 7. SCAP Support 8. Device Inventory Management & Reports 9. System Performance Reports 10. Security / Compliance Reports 	<p style="text-align: center;">Desired Capabilities</p> <ol style="list-style-type: none"> 11. Quality of Service (QoS) 12. Classified Data 13. PIV / CAC Support 14. Biometric Support 15. Network Monitoring 	3.0 Policy	4.0 Business Value
	2.3 MAM	<p style="text-align: center;">Required Capabilities</p> <ol style="list-style-type: none"> 1. General Security / Privacy Functions 2. Application Deployment 3. Mobile Application Store (MAS) 4. Application Security 	<p style="text-align: center;">Desired Capabilities</p> <ol style="list-style-type: none"> 5. Third-party Application Mutual Authentication 6. MAM Software Integration Services 	BYOD	Multi OS Support
	2.4 MLC	<p style="text-align: center;">Required Capabilities</p> <ol style="list-style-type: none"> 1. Implementation / Installation 2. Operations Support 3. Demonstration Platform 	<p style="text-align: center;">Desired Capabilities</p> <ol style="list-style-type: none"> 4. Enterprise Configuration 5. Integration with Wireless FSSI 6. TEMS 7. Device Replacement / Refresh 8. Device Disposal & Reporting 	Security	Hosting
				Legal and Regulatory Compliance	Enterprise System Access and Integration
				Department, Agency, and Team Compliance	<p style="text-align: center;"><u>Centralization:</u></p> <ol style="list-style-type: none"> 1. Acquisition 2. Management 3. Decision-Making 4. Operational efficiencies

Having determined the need for mobility, agencies next determine what type of mobile functionality the mission requires. Several broad categories are:

- Personal Information Management (PIM) – This is access to enterprise email, contacts and calendaring
- Virtual Desktop Interface (VDI) – This presents a traditional enterprise desktop on the mobile device
- Mobile access to intranet web sites – Be careful that those sites render correctly on mobile browsers, popups are particularly challenging in that environment

4.1.3.1 What can you remove?

While some requirements will always need to appear in an MDM (FISMA compliance, FIPS 140, audit, access control), others may be optional depending on the agency mission and use case. The majority of requirements in the RFTC support security, auditing and compliance. Some of the “extra” functional requirements that could be removed are listed below:

- Display of device location on a map.
- Multi-tenant support – The ability to have more than one enterprise managed within an MDM environment. Many cloud-based MDM solutions natively support this.
- Software Development Kit (SDK) – The ability to develop or wrap new applications within the MDM/MAM controlled environment.

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

- Geofencing – Enabling or disabling features based on the location of the device (or when device location is not known).
- PIV / CAC Support on Devices – This option can be costly and should be removed if not required by the agency. Note that this is separate from PIV / CAC support at the MDM server / management interface, which is required to support strong audit trails and HSPD-12 compliance.

4.1.3.2 What should you add?

Any unique agency-specific requirement should be included in the agency RFP, however remember that the proposed sources of supply may not be able to accommodate functionality that falls too far beyond what has been defined. Requirements that are extremely specific, such as management of land/mobile radio systems, may not be available from one of the proposed sources of supply. Agencies are free to procure solutions that are not listed, and are encouraged to use the Managed Mobility materials and Program Office to advance that process.

4.1.4 Solution / Marketplace Limitations

Some MDM features may not be available on all platforms. Vendors may respond positively to a feature request when it is not supported or possible (because of manufacturer API limitations) on every platform an agency needs. Agencies should require the vendor to be specific about which platform supports each feature.

4.1.5 Should we buy multiple MDM solutions?

Generally the increased costs of integrating multiple MDMs will outweigh any gain in functionality. Obvious exceptions are critical agency requirements.

For example, there may be instances where two products can do both MDM and MAM, where one is selected for MDM and the other for MAM. That type of solution should be carefully evaluated for increased costs and complexity.

4.2 Availability on Existing Government-Wide Vehicles

The ability to procure MDM solutions currently exist via multiple government-wide procurement vehicles. Each vehicle's applicability will be dependent on the ordering activity's requirements, needs, and acquisition strategy. Below is a short description of the particular procurement approach, vehicle applicability, and considerations one needs to make when procuring MDM from each.

4.2.1 [IT Schedule 70](#)

IT Schedule 70 is the largest, most widely used acquisition vehicle in the federal government.



Schedule 70 is an indefinite delivery/indefinite quantity (IDIQ) multiple award schedule, providing direct access to MDM/MAM/MLC solutions and services.

When procuring MDM solutions from IT Schedule 70 an agency is able to either procure stand-alone solutions, or solutions along with integration support through [Contractor Teaming Arrangements](#). These are arrangements whereby vendors can team together to compliment each others' abilities while addressing an agency's need, and allowable and encouraged under IT Schedule 70.

IT Schedule 70 allows for the greatest flexibility when reaching the solutions, either direct or through their partner/reseller arrangements. Often solution providers have only a few resellers, but many partners that market or integrate their products. Contact the solution providers directly and they can provide the most current information on how to access their particular products. Agencies need to be cognizant of the rules that apply to ordering from federal supply schedules found in FAR 8.405 "[Ordering Procedures for Federal Supply Schedules](#)." The Agency CO is required to "provide the RFQ to as many schedule contractors as practicable" and ensure that a minimum of 3 bids are received in order for competition requirements to be met for all orders above the Simplified Acquisition Threshold (FAR 8.405-1(d)(3)(i)). If less than 3 bids are received, the CO will have to make a determination "explaining that no additional contractors capable of fulfilling the requirement could be identified despite reasonable efforts to do so." Posting requirements on eBuy is also a way to satisfy competition rules and fair opportunity, and by posting your requirements on eBuy an award can be made without a determination even if 3 bids are not received.

4.2.2 [FSSI Wireless](#)

The FSSI Wireless BPAs is an *ideal* vehicle under which to procure MDM solutions. The FSSI Wireless BPAs were established for agencies to procure and manage wireless services across government. Agencies are able to implement cellular service plans and devices more efficiently and effectively through:



GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

- Unified acquisition – consolidates the number and variety of disperse wireless contracts to reduce life-cycle management costs and drive better volume discounts.
- Improved information management – simplifies service plan management and enables centralized access to standardized usage data to easily identify opportunities for cost savings.
- Center of excellence – leverages best practices and collaboration across agencies and the entire community of stakeholders to optimize performance and increase value.

MDM/MAM and wireless service and devices plans are a natural fit to procure all under one contractual umbrella. MDM/MAM, as well as Telecommunication Expense Management (TEMS), is all within scope of the FSSI Wireless contract and sensible means to address comprehensive end-to-end mobility needs for any federal agency.

4.2.3 [Connections II](#)

Connections II is another GSA IDIQ within the ITS Network Services portfolio under which an agency can procure MDM solutions through their relationship with identified integrators and resellers.



Connections II meets federal agencies' telecom equipment, labor, building, and campus infrastructure solution needs, including:

- Infrastructure design, installation, and implementation
- Professional services to support existing networks
- Transition planning and integration services
- Customized client-specific systems

When procuring MDM solutions from the Connections II IDIQ an agency is able to procure solutions along with integration support through one of the Connections II partners.

4.2.4 [GWACS](#)

Government-wide Acquisition Contracts (GWACs) enable federal agencies to buy cost-effective, innovative solutions for information technology (IT) requirements. GWACs provide access to IT solutions



GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

such as systems design, software engineering, information assurance, and enterprise architecture solutions.

An ordering activity would not be able to directly procure MDM solutions from GWACs alone, but all solutions are accessible via the GSA GWACs if there is an integration component to the requirements. Further it should be noted that it is very easy for MDM solution providers to establish partnerships and can do so with any and all providers found on any of the GSA GWACs. We have listed the pre-identified partnerships that the MDM solution providers have provided to us, but the ability of them to form partnerships with GWAC holders, and thereby compete under the various GWACs

Each GWAC listed below can had different strengths and attributes. The information below provides a brief description of the particular GWAC, as well as identifies the Mobility Solutions and partners found in each.

4.2.4.1 Alliant GWAC



Alliant, GSA’s premier enterprise GWAC, provides flexible access to customized IT solutions from a large, diverse pool of industry partners. With a \$50 billion program ceiling and a five-year base period with one five-year option, Alliant allows for long-term planning of large-scale program requirements.

4.2.4.2 8(a) Stars II GWAC

8(a) STARS II, a small business set-aside GWAC, provides flexible access to customized IT solutions from a large, diverse pool of 8(a) industry partners. With a \$10 billion program ceiling and a five-year base period with one five-year option, 8(a) STARS II allows for long-term planning of large-scale program requirements while strengthening opportunities for 8(a) small businesses.



4.2.5 **Small Business Set-Asides, Directed 8(a) Set-Asides, and Other Government-Wide Procurement Vehicles**

4.2.5.1 **NASA SEWP**

Solutions for Enterprise-Wide Procurement (SEWP, pronounced 'soup'), is a multi-award Government-Wide Acquisition Contract (GWAC) vehicle focused on IT products and product based services. The 38 pre-competed Contract Holders offer a wide range of advanced technology including MDM. Product based services such as installation, training, maintenance and warranty are also available through SEWP. As an OMB authorized GWAC, the SEWP contracts are utilized by all Federal Agencies.



4.2.5.2 **Small Business Contracting and Set-Asides**



There are multiple ways to reach the Mobility Management Solutions through small businesses. Agencies are able to contract directly with 8(a) companies through the GSA 8(a) Stars GWAC, or are able to conduct small business set-asides through either IT Schedule 70 or Alliant Small Business GWAC. Each of the potential sources for mobility management solutions have relationships with small businesses, and we encourage agencies to contact the solution providers directly to learn more about their small business partnerships.

4.3 **Evaluation Considerations**

Managed Mobility solutions have many features and capabilities, some of which will be critical to your agency and other that are desirable or optional. This section will cover how to evaluate required capabilities such as compliance, and offer guidance on evaluating other capabilities.

4.3.1 **FIPS 140-2 Cryptography Claims**

Vendor claims of “FIPS 140” encryption or cryptography must be traceable to a certificate on the [NIST FIPS 140 Validated Modules](#) list. The validation certificate does not need to reference the vendor or solution directly, but if it doesn't, the vendor must explain how they're using a third-party module, which one, and include a FIPS Attestation letter with the proposal and contract materials on award (see Award Execution below).

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

Cryptographic modules that are in the process of evaluation are generally accepted as compliant. They must appear on the [NIST Modules In Process](#) list.

Solutions may rely on the underlying operating system for cryptographic functions. In this case they must assert they are using the OS-provided cryptographic module and that module must appear on the NIST FIPS Validated Modules or Modules In Process list.

4.3.2 Use of Validated Modules Such As OpenSSL

Government recommends use of existing validated modules where possible. This generally reduces time and cost to produce a solution. A popularly re-used module is the OpenSSL module (Certificate #1747). All module usage claims must include assertions that the modules are operating unmodified in FIPS-enabled mode and are be accessed and used in accordance with the module's Security Policy (see Award Execution below for example text).

4.3.3 Cost Evaluation

Most Managed Mobility solutions have a per-user or per-device cost, typically priced annually on either a license or subscription basis. Solutions often have tiered costs linked to various levels of support, as well as additional services required for the solution to be operational within an agency infrastructure. Agencies must analyze the costs/benefits of providing some level of support internally (and diverting resources from their mission) versus outsourcing that support at additional cost.

4.4 Award Execution and Monitoring

4.4.1 FIPS Attestation

All FISMA-compliant solutions must use FIPS 140-2 Validated modules for cryptography and key management. These modules must also be used in the validated configuration to be compliant. Verifying this is often difficult or impossible, so the accepted approach is to ask the vendor to provide a letter stating they are using a FIPS-approved module, and it is implemented and accessed in accordance with the documented Security Policy for the module located on the [NIST FIPS 140 web site](#).

The Contracting Officer must ensure such a letter of attestation is signed by the vendor contract representative and included in the contract package. This gives the Government recourse should the FIPS implementation be found lacking or absent in subsequent audits.

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

Sample wording for the letter appears below.

To <Contracting Officer>,

<Vendor> confirms that FIPS 140-2 Validated Module <Module name> with certificate number <module certificate #> is used unmodified in the following product(s): <product list with version numbers>, and provides all cryptographic services for the listed product(s).

<Vendor> confirms that all instances of the above FIPS 140-2 Validated Modules are implemented in accordance with the Security Policy associated with the certificate.

<Vendor> agrees to maintain the FIPS 140-2 Validated configuration in the listed product(s), and to correct any implementation defects when detected.

Signed,

<Vendor Contract Representative>

5 Post-Acquisition Activities

5.1 Feedback to the GSA Managed Mobility Program

GSA keeps the Managed Mobility program useful to Agencies by receiving Agency feedback. Please contact the Managed Mobility Program Manager to share what did and didn't work well for you when acquiring your mobile device services, even if you performed the acquisition outside of the Managed Mobility Program.

5.2 Program Manager Contact Information

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

6 Acquisition Assistance

The GSA Managed Mobility program is committed to assisting agencies in procuring Mobility Solutions. We can leverage our knowledge of the commercial sector, federal security requirements, and acquisition approaches to provide in depth analysis to better inform agency customers. We can assist with acquisition strategies, provide scope reviews for proposed acquisition approaches, and validate agency assumptions concerning the market and solution capabilities regardless of whether they have been identified as potential sources of supply or not. Further, if there is a need for assisted acquisitions we can facilitate that internally within GSA's Assisted Acquisition Service.

6.1 When to call for help?

Agencies are encouraged to use and adapt the materials provided for their procurement purposes. If there are any questions related to the materials provided agencies are encouraged to contact Jon Johnson, Program Manager.

6.2 Program Manager Contact Information

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

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

Appendix A Appendix 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

**GSA Managed Mobility Program
Mobile Device & Application Management Users Guide**

	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.
MLC	Mobility Life Cycle services which may involve managed or one-time/professional services to evaluate/design/implement support MDM and systems integrating with MDM
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	The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency.
Portal	A software (or web) solution that enables instant and effortless exchange of business information (Electronic Data Interchange – EDI) over the Internet. This is accomplished by the use of a common operating framework for accessing data and information from different systems. A typical TEMS portal will pull information from carrier electronic billing systems, which is uploaded into their platform (portal). This allows the administrator/user a single view that provides multiple carrier information in a seamless manner, offering efficiency.
Secure Communications	Communication services that includes security components such as encryption to ensure the privacy and integrity of the communications.
Smartphone	Electronic handheld wireless device that integrates the functionality of a mobile cellular phone, personal digital assistant (PDA) or other information appliance.
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	Text Messaging or Short Message Service (SMS) is the exchange of brief written messages

GSA Managed Mobility Program
Mobile Device & Application Management Users Guide

or SMS	between cellular phones, smartphones, and data devices over cellular networks.
Third-Party Direct Billing	The receipt of invoices from parties other than the Contractor for services within or outside the scope of this agreement.
Trade Agreements Act (TAA)	<p>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:</p> <ol style="list-style-type: none"> 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. <p>The TAA designated countries are listed in the following web site: http://gsa.federalschedules.com/Resource-Center/Resources/TAA-Designated-Countries.aspx</p>
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.