TABLE OF CONTENTS

1  Introduction ........................................................................................................................................... 3
  1.1  Background ..................................................................................................................................... 3
  1.2  Objective .......................................................................................................................................... 4
2  Solution Requirements .......................................................................................................................... 5
  2.1  Baseline Telecommunications Expense Management Service (TEMS) Requirements ... 5
    2.1.1  SOLUTION FOUNDATION ................................................................................................. 6
    2.1.2  SUPPORT FOR USER ACTIVITIES ................................................................................... 8
    2.1.3  MANAGEMENT SERVICES ................................................................................................. 14
    2.1.4  COMPLIANCE WITH GOVERNMENT POLICIES ........................................................... 19
  2.2  FedRAMP ......................................................................................................................................... 19
  2.3  Access to Sensitive Information ..................................................................................................... 20
  2.4  Information Security Incidents ....................................................................................................... 20
  2.5  FIPS/FISMA .................................................................................................................................... 21
3  Pricing .................................................................................................................................................. 22
1 Introduction

1.1 Background

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

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

The primary purpose of this document is:

- State the minimum set of requirements across the Federal Government for Telecom Expense Management (TEMS) and Lifecycle Management of mobile devices.

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

This functional technical requirements document includes requirements from the previous Managed Mobility TEMS RFTC solicitation in 2012, requirements obtained from a National Science Foundation Statement of Work (SOW) which had been based on that 2012 TEMS RFTC solicitation, and ongoing inputs from the inter-Agency TEMS MSCT working group.

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

A. Qualified Secure, Scalable Solutions – Technical solutions that address the existing mobile device, application, and content management needs of government mobile technology including minimum level security and policy management. The solutions shall have the ability to scale to the extremely large and evolving nature of federal government cabinet-level agency organizations.
B. Evolutionary and Flexible – The management needs of the Federal Government Mobility are evolving with increased mobile adoption, new mobile applications, enhanced needs for remote access, and emerging policy and security requirements in an increasingly threatening external environment. As a result, the solutions will continue to assess future requirements to ensure the ongoing Federal Government needs of Telecom Expense Management are adequately met. The MSCT intends to re-assess both the TEMS requirements and solution providers on a periodic basis in response to mobility evolution. This will provide government agencies with ongoing, updated qualified solution providers.

C. Shared Mobility Community – The solution providers are expected to monitor and bring forth new industry developments, identify Managed Mobility best practices in both industry and government, and to present these best practices to government. The Managed Mobility space is in a state of rapid change, making it challenging and resource-intensive for agencies to stay properly informed and to adequately maintain and manage mobility within their respective agencies.

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

1.2 Objective

The Federal Government must address agency’s mission needs in a secure, cost-effective manner. This objective is driven by the MSCT as directed by The Office of Management and Budget (OMB). Telecom Expense Management Services (TEMS) is a core capability for effectively scaling the deployment and management of mobile devices, inventory management, reporting functionality, invoicing, and savings. Controlled device deployment, management, tracking, rate plan optimization, and reporting will lead to cost reductions over time.
2 Solution Requirements

2.1 Baseline Telecommunications Expense Management Service (TEMS) Requirements

Figure 1 below summarizes the vendor-provided TEMS capability which may be integrated with existing Agency systems on an as-needed basis, and which shall be compliant with all relevant Agency and Government-wide policies.

The Vendor-provided TEMS solution incorporates the following solution blocks which are outlined in more detail within this functional specification:

- **SOLUTION FOUNDATION**
  - Agency Interface Web Portal
  - As-Needed Integration Services

- **SUPPORT FOR USER ACTIVITIES**
  - Order Management
  - Inventory Management
  - Expense Management
  - Documentation Management

- **MANAGEMENT SERVICES**
  - Program Management
  - Customer Support
  - Training
  - Data Management
  - Audit Capabilities
2.11 SOLUTION FOUNDATION

2.11.1 Agency Interface Web Portal
A web-portal is an access point between the agency and the Mobile Lifecycle & Expense Management provider that allows for management functionality after an initial inventory is conducted. This web-portal must be defined and secure, and be capable of accessing connectivity with the carriers. The portal may be hosted within the Government IT environment, within the Contractor-provided IT environment, within a FedRAMP-approved cloud provider, or a combination at the discretion of the ordering Agency. The Vendor-provided web portal shall be accessible using current industry-standard web browsers (e.g. Explorer, Chrome, Firefox, Safari).

The Vendor shall be responsible for development, testing, reporting, implementation, maintenance, troubleshooting, and hosting of the secure web portal; and ensure that the portal is/remains Section 508 compliant and Federal Information Processing Standards (FIPS) 140-2 certified at the portal and/or Secure Socket Layer (SSL) as required.

The Vendor’s IT WTEMS system and secure web-portal shall undergo an initial and periodic IT Security Review(s); and the Vendor shall document and address any defects, deficiencies, or vulnerabilities identified by the Government, or when known or discovered by the Vendor; and ensure the system meets all Federal requirements (e.g., FIPS 140-2 certified encryption where encryption is used). The Vendor’s web-portal shall remain secure, accurate, available, and accessible to designated Government and Vendor personnel, in real-time, to:

- Access Agency TEMS user data, as necessary, and to monitor and manage the Agency’s wireless enterprise. Access will be supported from multiple types of devices, including desktop / laptop PC’s, and miscellaneous mobile devices (e.g. tablets, and cell phones)
- Define, assign, and view user roles on the system
- Verify and manage functionality after the initial inventory of TEMS data
- Serve as the master inventory data base
- Provide consolidated-centrally managed access to all Agency TEMS data
- Serve as the single/comprehensive ordering and reporting portal for use by Agency customers
- Provide current, detailed instructions and allow all wireless transactions to be executed within the portal environment including (but not limited to) device and service requests, look-up provider plan(s) and devices, order creation, tracking and cancellations, account requests and management approvals
- Provide current, detailed instructions on and allow the initiation of moves, additions, changes, and disconnects (MACD) associated with agency wireless assets
- Provide current, detailed instructions and allow designated users to modify, configure, and customize data to meet agency requirements; ensures governance / policy compliance
of approved devices and plans. Maintains both role segmentation and agency maintained security policies, device assignments, and specifications.

- Allow for the assignment of permissions that enable authorized staff to receive requests for devices, services and accessories, make approvals and forward approved request to vendor for appropriate action.
- Provide tools and processes to deliver spend/savings analysis and optimizations beyond what is provided by the wireless carriers, and optimizes cost savings across carriers.
- Provide reports on actions taken by the TEMS vendor to deliver cost savings to the Government, and recommendations provided to the Government for additional actions to obtain savings and service optimizations.
- Permit the Government to assign and manage tiered accounts (e.g. administrator accounts with all privileges or user accounts with different access (read/write) to various portions of the TEMS functionality).

Federal Agencies are encouraged to have the Vendor provide the following to ensure that the Vendor-provided portal meets Agency needs:

- A description of how the Vendor will provide a consolidated, centrally managed web portal with access to all data, and use of this portal by federal customers.
- A description of how the portal will allow all wireless transactions to be executed within the portal environment including device and service requests, provider plan and device look-up, order tracking, account requests and management approvals.
- A description of how the portal will allow for any moves, additions, changes, and disconnects (MACD) associated with both wireless assets, how it can be modified, configured and customized to meet agency requirements, and how access will be allowed based on system user roles.
- Ease of configurability to meet day-to-day user needs, including:
  - How the solution’s application interface can be configured to meet the requirements of different users in the organization
  - How the solution can restrict user access to system data and functions
  - How reporting capabilities can be configured to meet user requirements
  - How the application can be configured to support fixed and mobile procurement policies
  - How the solution can support configurable mobility management workflows
  - How other business process workflows (e.g. Human Resources, Finance) can be configured to meet user requirements if needed to support Agency business processes
  - How the web-based portal addresses workflow to allow assignment of permissions that enable authorized staff to receive requests for devices, services and accessories, make approvals and forward approved request to vendor for appropriate action.

The portal shall be Section 508 compliant and Federal Information Processing Standards (FIPS) 140-2 certified. FIPS 140-2 compliance may not be required for the portal itself, but the Secure Socket Layer (SSL) will require FIPS 140-2 certification.
2.1.1.2 As-Needed Integration Services

As determined by each Agency to meet unique requirements, the Vendor will integrate the Vendor-provided web portal with all necessary Agency IT systems in order to provide effective and comprehensive TEMS service. As part of the integration services, the Vendor must address:

- How the Vendor’s web portal shall be capable of being a system of record for the Agency’s telecommunication service, device and license inventory, with integrated ordering and inventory modules.
- How the Vendor master inventory and asset database will integrate with all Agency databases.
- How the Vendor management, ordering and billing/financial portals will integrate with relevant Agency databases.
- How Agency data will be kept consistent with Vendor databases through automated processes.
- How the Vendor TEMS service will be integrated with other mobility management services (e.g. MDM, wireline voice, wireline data).

Some examples of the types of data flow are:

- New completed orders will create inventory and needs to flow to the asset management system.
- Charges and payments need to be updated in both the asset management and financial systems.
- Budgeting and purchase order information needs to be set up in the financial system, provided to the TEMS capability to be used in ordering and spend reporting.
- Real time notifications need to flow to users of both systems.

Agencies may also require that the TEMS solution be integrated with Mobile Device Management (MDM) solutions & Mobile Application Stores (MAS). When MDM/MAS integration is needed by Agencies, the Vendor must show how the system will meet all business rationale for each level of integration and the resulting high level definition of the data to be exchanged between systems, provide the ability to use the portal as a means to exchange data with MDM and MAS systems, and set the standard and utilize this same specification across MDM and MAS systems.

- The portal shall ensure that move, add, change and disconnect information is entered once into the web portal and the information is forwarded to the MDM and MAS systems.
- The Vendor’s web portal shall maintain both role segmentation and agency maintained security policies, device assignments, and specifications.
- The Vendor’s system shall demonstrate web portal’s role-based ordering ensures governance / policy compliance of approved devices, plans, and MDM/MAS environments.

2.1.2 SUPPORT FOR USER ACTIVITIES

2.1.2.1 Order Management

The solution shall provide ordering and procurement services through its portal solution. Ordering and procurement services shall include the ability to provide order status, order and change request tracking, and ensure adequate controls exist to prevent fraud waste and abuse.
The solution shall provide:

- An ordering process that uses workflow management with multiple approval hierarchies for multiple functional or business units. Individual component level requirements will be specified by the ordering agency.
- An ordering interface that ensures that only government approved devices and accessories can be ordered through the portal.
- Ability to reconfigure the portal/systems to accommodate different standard equipment sets as they change and as they are approved by the government COR over time.
- Ability to control device type by Special Designation, Cost Center, System Role, or other Agency-defined category.

2.1.2.1.1 Catalog

The solution shall demonstrate the ability to perform an initial contract optimization analysis of existing wireless service agreements to identify immediate savings. This includes the ability to perform and report follow-on comprehensive assessments of all existing wireless service contracts and agreements to identify improvements and cost savings opportunities. These capabilities include:

- Asset Acquisition
- Service Plan Acquisition
- Service Plan Management

The vendor catalog solution shall also automatically update as new data is received to continually identify new improvements and cost savings opportunities.

2.1.2.2 Inventory Management

The TEMS solution shall be capable of establishing an accurate inventory database.

- The desired goal is 100% accuracy of all Agency user assets
- Initial inventory to be delivered (Agency to define timeline based on number of assets, physical location of assets, ability of Agency personnel to provide data when desired)
- Vendor to deliver results to the COR for agency verification and acceptance
- Ongoing inventory management to be provided by the Vendor over the life of the contract consistent with the inventory validation cycle and deliverable that has been preapproved by the Government.
- Tracking of phones, devices, and accessories procured by Agency personnel for emergency or temporary-use situations.

Inventory Management also includes maintenance and continual database updates as needed or required. The solution’s Inventory Management System shall:

- Describe whether, when, and how designated Agency representatives can access the inventory
- Include the ability and instructions for designated Agency representatives to search, filter, and sort information by type
- Provide the ability for designated Vendor and Government representatives to link (or map) an inventory item to multiple supplier billing accounts
• Describe the manual entry and automated components of inventory updating
• Provide Service Level Agreements associated with the inventory management system
• Ensure all warranty components for all equipment is properly identified, documented, catalogued, registered, and utilized according to the Original Equipment Manufacturers (OEMs) requirements
• Leverage warranty replacements for devices and peripherals such as cellular device holders or cases as to optimize savings for the Agency when replacements are required

The vendor solution shall provide provisions for the following:

- Device/Asset Tracking
- Non-Device Tracking (e.g. accessories, miscellaneous hardware, software, licenses)
- Real-Time Inventory
- Account Reports
- Device Disposal (e.g. disposal of devices on behalf of the Government and tracking inventory change, or simply tracking disposal of devices that the Government returns to the carrier as dictated by Agency workflow processes)
- Reporting ENERGY STAR compliance
- Reporting Electronic Product Environmental Assessment Tool (EPEAT) assessment

### 2.1.2.3 Expense Management

The respondents must demonstrate how they are capable of providing a reduction of telecommunication costs through dispute recovery, rate plan optimization, contract optimization and elimination or reduction of zero use devices. The respondent’s expense management processes shall be compliant with Agency-specific policies and workflows.

#### 2.1.2.3.1 Invoice Consolidation

The solution shall provide invoice consolidation capabilities tailored to the specific Agency business processes, which shall include the following activities at a minimum:

- Collect, process, and validate paper and electronic invoices received from multiple carriers in multiple billing formats against agency information, ordering records, and telecom contract and service agreement terms
- Allocate cost information from the carrier invoices across agency’s organizational units and financial accounts to provide increased visibility and accuracy for agency’s cost and spend management functions
- Prepare monthly reports identifying billing and invoicing errors for agency claim and dispute submittal
- Integrate invoice data with procurement and inventory management data records to enable and support spend, inventory and usage analysis by the Vendor and Agency telecommunications managers
- Prepare monthly standardized management reports detailing spending levels and trends by carrier, regions, business units, accounts, service lines and service types
- Provide the capability to generate custom-designed and ad hoc spending reports at both a summary and various organizational or financial account levels
• Prepare management reports on budget spend, including projections for current and future fiscal years
• Prepare and provide necessary electronic reports or formatted data feeds to the Agency’s bill payment system (or the Vendor’s internal payment system if the task order includes the Bill Payment Services option).
• Provide recommendations to the Agency on areas for improvement and savings regarding agency’s invoice process (e.g. where invoice consolidation with major carriers would benefit the Government).
• Provide recommendations to the Agency for alternative invoicing options that may benefit the Government (e.g. prepayment of invoices by the vendor with follow-up verification by the Government.
• Provide help desk support as listed in Section 2.1.3.2, Customer Support, to answer billing and invoicing questions from agency financial and telecommunications account managers and to provide and implement recommendations

2.1.2.3.2 Contract Optimization
The solution shall perform an initial contract optimization analysis and rate-plan and usage optimization analysis of existing wireless service agreements to identify immediate savings. This includes the ability to perform and report follow-on comprehensive assessments of all existing wireless service contracts and agreements to identify improvements and cost savings opportunities. The vendor shall periodically perform these contract and rate optimizations on a regular basis, no less frequently than annually. Contract optimization activities shall include:

• Benchmarking the agency’s existing pricing, service terms and conditions with those of other federal and commercial customers and accepted “Best Practices” to identify recommended changes.
• Making specific recommendations for rationalization of rate-plan types, migration of service lines between specific wireless service providers, changing the number of total wireless service providers, changes in contract terms and conditions, and other opportunities that would lower total cost while maintaining or improving the quality of wireless service provided to the agency’s users. Provide all necessary metrics (e.g. minutes/capacity purchased, minutes/capacity used, average minutes/capacity used for the specific user/line, internal Agency cost center, and overall Agency.
• Submitting changes for agency approval and assist with the implementation of contract optimization recommendations, changes, and sourcing/competitive bidding among Wireless service providers to lower overall costs.
• Tracking and reporting savings derived from the requisite contract and rate-plan optimization efforts.
• Identifying and reporting on zero use devices.

2.1.2.3.3 Dispute Resolution
The vendor solution shall collect and prepare information necessary to resolve billing and accounting errors with the wireless service providers and maintain this information in the portal. The vendor shall also manage and track all claims through final resolution. Dispute resolution capabilities include:
• Collect and prepare support material necessary to file and defend claims submitted to the carriers for billing and account corrections.

• Research, review, dispute, and track all potential billing errors and represent the agency as an authorized agent with all carriers and telecommunications suppliers.

• Submit written claims to telecom carriers and suppliers, including reasonable and necessary support documentation, to identify and recover any audit savings for the agency. These are not contract claims as defined in FAR Part 33, which will be handled by a warranted Contracting Officer.

• When errors are found and credits are due to the government, apply those credits to the service line level to ensure they are correctly applied to the component, individual, and/or project chargeback codes. Additionally, credits may also reference a telecom carrier invoice and line item number.

• Collect, prepare, and submit any information necessary to identify and recover any audit savings from the wireless service providers.

• Manage and track all disputes through final resolution. These are not contract claims as defined in FAR Part 33, which will be handled by a warranted Contracting Officer.

• Prepare and provide the agency with monthly reports detailing the status of claims filed with the carriers, billing accuracy rates for individual carriers, and the amount of any savings (or additional cost) recovered as a result of the audit and dispute recovery efforts.

• Apply recovered funds to the specific wireless service being credited.

2.1.2.3.4 Expense Analysis

The vendor solution shall support allocation of fixed and mobile costs to specific codes, enabling reporting of costs by department, location, employee, and other relevant scenarios. The vendor shall ensure that automated cost allocations can be overridden on a single-case basis, provide appropriate level of detail for cost allocation/chargeback, and accommodate varying allocation and chargeback rules based on the billing media (EDI, FTP, paper, etc...), and whether these rules include fixed percentages from some expenses and allocations based on consumption. The vendor shall support EDI 810/820 standards for invoice payment/cost allocation and payment advice files.

2.1.2.3.5 Expense Reporting

The vendor solution shall be capable of reporting on all aspects of the TEMS capabilities to support multiple goals, including cost reduction for carrier-provided service plans, elimination of wasteful spending trends, detecting fraud by any party, and any other aspect of full lifecycle management.

The reporting capability will allow the Government to categorize and track lifecycle issues, including:

• Identification of actual usage patterns by carrier, device type, program office, and end user

• Identification of usage patterns and classification into regular usage, minimal usage, zero usage and mis-aligned usage (where actual usage does not match the plan, or international roaming)

• Identification of alternate carriers or contracts to obtain optimized pricing

• Identification of cost savings to date, and strategies for continued spend optimization
• Identification of contract restructuring to obtain additional volume-based discounts

Mission-critical metrics should be available to the entire enterprise – on demand – to allow the Government to make informed decisions from real time reports such as analysis of usage patterns, spend trending, and inventory expense by location. Reporting capabilities shall include configurable summary dashboards and detailed reports, ad-hoc reports, the ability to drill down into every level and aspect of data, and comprehensive data analytics and visualization tools.

2.1.2.3.6 Rate Optimizer

- The vendor shall perform an initial rate plan analysis of existing wireless service agreements to identify immediate savings. Subsequent to the initial review, the vendor shall conduct follow-on reviews to ensure cost savings and price reductions for products and services pursuant to the contract.
- The vendor shall provide recommendations to rationalize rate plan types, the number of service lines with each wireless service provider, the total number of wireless service providers, and other opportunities that might lower total cost while maintaining or improving the quality of wireless service provided to Agency users.
- The vendor shall calculate costs to the Agency based on actual monthly usage patterns of users and determine where individual account and rate plan changes should be made to lower future costs. The analysis shall be based on a three-month usage period. This applies primarily to voice and data usage. All other featured usage shall be monitored and addressed on current month usage. This information shall be contained in the monthly Performance Status Report.
- The vendor shall provide optimization recommendations to the Agency designated representatives, and upon approval, implement the optimization recommendations and changes as specified by the Government. Where permitted by Agency-specific policies and workflows, the vendor will immediately implement optimizations, and then notify the Government of changes and make further changes as directed.
- Standard service optimizations of each vendor’s priced offerings shall be performed on a regular basis, no less frequently than quarterly. Contract optimization (e.g. optimizing across multiple vendors) shall be also be performed on a regular basis, no less frequently than annually, to assist the Government with implementing major contract changes.

2.1.2.3.7 Bill Payment

- As needed by Agency-specific policies and workflows, the vendor shall accept, pay out, manage, and report on bills from carriers utilizing the web portal, backend analytics and integration services as is appropriate for the Agency.
- The vendor shall provide an effective workflow process from invoice receipt through payment, incorporating details such as average times from receipt, to approval, to payment.
- The vendor shall provide a consolidated invoice capability incorporating multiple carriers. Service shall support funding streams that consolidates wireless service, equipment, miscellaneous managed services and fees.
- Service shall include payment for shipping, equipment and accessories provided by carriers, and miscellaneous equipment and accessories needed for wireless packages that are not provided by the wireless carriers meeting FAR-51.
2.1.2.4 Documentation Management

The vendor’s TEMS solution will include a document repository which allows the Government to store, update, and perform configuration on a variety of documents to include policy documents, carrier contract info, and user guides. The content, and structure of the repository, shall be fully under the control of the Government.

Access to this repository will be provided using role-based access, and multiple types of roles shall be supported.

2.1.3 MANAGEMENT SERVICES

2.1.3.1 Program Management

A Program/Project Manager with responsibilities for managing contract, schedule, costs and deliverables is required. The respondent must identify their PM POC for all customer interface, and who clearly demonstrates past experience in developing and implementing a Project Management Plan directly related to wireless TEMS, and how this example of project management tracked the quality and timeliness of the delivery of the required elements.

The Vendor shall designate a Project Manager as a Key Personnel representative and the Lead for this effort.

This individual will be primarily responsible for managing all areas of contract performance, deliverables, and reporting; including but not limited to: staffing; managing, tracking, and reporting contract performance, deliverables, and training, quality control, schedule (planning and managing), costs, customer service, identifying risk and risk mitigation, communicate and interface with the COR and Government leads.

Guidelines for Agency requirements include:

- Have at least 24 months recent project management experience successfully leading at least two (2) IT customer focused projects directly relating to wireless TEMS using Project Management Institute (PMI) project management standards; or at least 12 months project management experience successfully completing at least one major IT customer project relating to wireless TEMS that is same or similar in size, scope, and complexity for this effort using PMI project management standards.
- Be knowledgeable, and demonstrate the ability to remain current, on all aspects regarding wireless TEMS services, carrier plans, and offerings available to the Government through existing contract vehicles.
- Provide the ability to work effectively with the Government and wireless TEMS carrier representatives.
- Serve as the primary interface with the Contracting Officer’s Representative and Government technical leads.
- Anticipate appropriate Government customer and account needs and provide reliable customer relations to a diverse set of customers with a wide array of different wireless cellular service needs.
- Successfully manage time and resources.
• Be thoroughly knowledgeable and be able to discuss or explain all aspects of the Vendor’s wireless TEMS services and related customer operations
• Ensure deliverables are provided on-time with minimal need for revisions or corrections
• Effectively lead or participate in oral and written communications with the COR and Government leads
• Effectively investigate, mitigate, and resolve contract performance issues or concerns.

The Project Manager shall also ensure that the Program Management Plan that has been reviewed and accepted by the Government is properly implemented, executed, and remains current to ensure consistent, quality service delivery through standardized performance metrics and reporting.

As part of the overall duties for the Program Manager, the Vendor shall create and maintain a Program Management Plan to ensure consistent, quality service delivery through standardized performance metrics and reporting. The plan shall include at a minimum:

• Documented standard processes and procedures
• Defined controls and metrics
• Processes to ensure standardized reporting on all service delivery performance
• Staffing Plan
• Training Plan

Once accepted by the Government, revisions to the Vendor’s Program Management Plan must be reviewed and preapproved by the COR in writing.

Contract Transition-In: The Vendor shall provide a Transition Plan that details how devices previously supported by the government will transition from existing service in a quick, reliable, and accurate manner to the offered solution. This action begins at contract award and includes downloading relevant service contracts, user profiles, device data and usage into database or solution systems, and the performance of initial optimization for the agency. Staffing requirements (vendor 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 Vendor’s transition-in plan shall be based on lessons-learned from successful on-boarding of hundreds to many thousands of devices. The example must include a high-level timeline, staffing required, and a summary walk-through of the process.

The program management plan shall clearly describe how initial deployment support and integration services will be provided. These services are expected for installing, configuring, and certifying the initial deployment of the TEMS solution, as well as the ability to support specific agency related integrations or customizations. The program management plan shall also detail all activities associated with assisting the Agency with quickly and efficiently achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.
**Contract Transition-Out:** The Vendor shall provide a transition-out plan that describes how all data associated with this TEMS solution shall be delivered to the Government, and the contract close-out processes that the Vendor will follow.

### 2.1.3.2 Customer Support

The Vendor shall provide a high degree of professional customer services to various Agency users that collectively have a wide array of different wireless cellular service and reporting needs. For example, Agency staff that regularly travel domestically and abroad require access to wireless data in-route to, from, and while at their temporary duty stations. In these instances the Agency relies heavily on its TEMS provider to ensure that the needs of its traveling staff during travel are managed effectively and cost-efficiently.

**Note to Agency Representatives:** Help Desk / Customer Service desk support is anticipated to be one of the key cost drivers for TEMS service support. The help desk / service desk support requirements were obtained from other agencies, but your specific Agency needs will likely differ. Please assess Agency-specific needs to ensure minimal head count is provided by the TEMS provider but will meet your needs.

In addition, the customer support desk shall include:

- A trouble-ticketing system where each request has a unique identifier for tracking purposes
- Help Desk interaction that supports online requests / resolution, supported with email
- Telephone (voice) Help Desk support must be available, but can be limited to business hours
- Ability to generate and receive automated customer surveys, process and report the results to Agency management, and incorporate lessons-learned into ongoing service improvement.

**Customer Service Plan:** The Vendor shall develop and implement a Customer Service Plan, for Government review and acceptance, which describes in detail how they will provide High-Touch and Low-Touch Customer Services. The Vendor’s Customer Service Plan shall include a combination of High-Touch and Low-Touch Services – depending on the required service, customer experience, and customer preference.

1. **High-Touch Customer Service:** High-Touch Customer Support shall include a high degree of customer service and interaction to resolve customer issues in a timely, proactive manner; i.e. understand and anticipate each unique customer situation and take appropriate actions to respond and resolve customer issues as they occur/in real-time. Depending on the customer location and situation support shall be provided in by telephone (human interaction) and/or face-to-face interaction. High-Touch Customer Service shall be available 24x7x365/6 (including all federal holidays).

2. **Low-Touch Customer Service:** Support will be provided by automated telephone systems and online, self-service web-based portals to process business transactions. Low-Touch Customer Service shall be available 24x7x365/6 (including all federal holidays).
**Mitigate Charges:** The Vendor shall monitor, report, and with written COR preapproval take actions to temporarily (or permanently) mitigate charges for users with unusually high international or local voice and data usage that may negatively impact service to other users or costs to the agency.

**Help Desk Support and Customer Service Management Plan.** The Vendor’s Customer Service Plan shall also include how they will provide Help Desk Support Services for approved TEMS solutions, and identify Vendor personnel (by position title) and any required Agency support that will be included in the Agency customer service chain and Administrative Help Desk Services as described below.

Customer Help Desk Support team shall be available to coordinate and assist the Agency IT Help Desk in identifying, documenting, and tracking all customer help desk requests until satisfactorily resolved.

Customer help desk interactions and functions shall also:

- Utilize a trouble-ticketing system where each call/request has a time-stamp and unique identifier for tracking purposes
- Include telephone (voice) support available during the CORE contract business hours
- Support online requests and resolution supported by email
- Record, archive, and be retrievable upon written request from the COR
- Include automated tracking and verification of each customer contact until resolved and archived
- Track the duration of each call, similar calls from the same or multiple users
- Track dropped, abandoned, and disconnected calls
- Optionally, integrate support with other mobile managed services (e.g. MDM deployment, kitting, etc.)
- Optionally, integrate support with pre-existing Agency Help Desk Support personnel and systems
- Facilitate routine customer satisfaction surveys and matrix upon CORs request
- Administrative Help Desk Support includes, but is not limited to, invoicing, billing, or other account related services, and must be available from Monday through Friday, 8:30 AM to 5:30 PM EST, excluding federal holidays where the Government (or Agency Headquarters) is officially closed for business.

### 2.1.3.3 Training

The Government requires that all users of the TEMS system, which includes end users, administrators and developers, be trained to correctly utilize the system. The Vendor shall be responsible for developing and updating the TEMS Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan. Online training shall be hosted by the vendor, and the vendor must provide the required content.

### 2.1.3.4 TEMS Data Management

**Transition-In (Use Case #1 – from prior TEMS provider):** The Vendor shall ingest current and historical data from the prior TEMS support vendor, and/or Government databases as necessary in order to implement service. The Vendor will initiate ongoing data ingest from the carriers on
behalf of the Agency, and notify the Agency of any discrepancies to allow the Government to address with the carriers. The Vendor shall provide any necessary data cleanup to implement service.

**Transition-In (Use Case #2 – without prior TEMS provider, without historical analysis):** The Vendor shall initiate regular data ingest from the Government databases and wireless carriers as necessary in order to implement service. The Vendor shall provide any necessary data cleanup to implement service. The vendor will notify the Agency of any discrepancies to assist the Government to address with the carriers. Historical tracking, data cleanup, and analysis will be performed on carrier data dated as of or later than the date of contract award.

**Transition-In (Use Case #3 – without prior TEMS provider, with historical analysis):** The Vendor shall initiate regular data ingest from the Government databases and wireless carriers as necessary in order to implement service. The Vendor shall provide any necessary data cleanup to implement service. The vendor will notify the Agency of any discrepancies to assist the Government to address with the carriers. Historical tracking, data cleanup, and analysis will be performed on carrier data dated as of [TBD – Agency to specify].

**Transition-Out:** The Vendor shall export all managed TEMS data to the next TEMS support vendor and/or Government databases using commercially standard format(s) as requested by the Government to effect smooth transition of services.

### 2.1.3.5 Audit Capabilities

The Vendor shall be capable of applying risk mitigation strategies and implementing cost controls to assist the Agency to comply with with OMB Circular A-123 and Presidential Executive Order 13589.

The vendor shall provide all necessary audit support to the Agency. At a minimum, auditing should include:

- Validation of account ownership and service existence
- Verification of rates, charges, and discounts
- Verification of correct account numbers and phone numbers associated with accounts
- Identification and Recovery of missing carrier invoices
- Analysis of invoices for abuse, misuse and fraud

### 2.1.3.6 Management Reporting

The Vendor shall provide a robust menu of standard, preconfigured reports facilitated by a web-based “download and save” capability through the portal. The respondent shall provide sample reports that are available as standard reports and shall indicate the degree of customization of these reports that is possible. The Vendor shall provide data analytics capabilities and display techniques that represent data in graphical or tabular format(s) that foster clear understanding by Agencies.

All reporting shall provide the capability for authorized users to generate new reports and ad hoc reports at both a summary level as well as down to organizational and financial account levels. Reports shall be provided in 508 compliant electronic formats with read/write capability using applications that are compatible with agency programs (such as Microsoft Office).
For vendors to participate in this program, GSA requires that they submit a semi-annual report that can capture programmatic traction and savings that agencies benefit from by using a TEMS provider. This semi-annual report will be due after, and reflect activities through Q2 (after March 31st) and Q4 (after September 30th) of the federal FY (October-September).

Information that will be requested is only that information that can be publically releasable. At minimum the Government will require the agency, task order number, total amount of the award, and attributable savings to date. Respondents must indicate that they are willing and able to provide the publicly available information to the GSA Managed Mobility PMO in the following format:

<table>
<thead>
<tr>
<th>Agency</th>
<th>Task Order #</th>
<th>Total Award Amount</th>
<th>Attributable Savings to Date</th>
</tr>
</thead>
</table>

This report will be available in both Excel format and in formats suitable for processing with mobile devices. This report is not for distribution for anyone other than the PMO and is meant to track programmatic impact as well as attributable savings. It is protectable under FOIA Exemption #4 and cannot and will not be distributed, internally within GSA or externally with other parties, without the expressed written and documented consent of the TEMS provider.

2.1.4 COMPLIANCE WITH GOVERNMENT POLICIES

2.1.4.1 Security
The TEMS 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).

2.1.4.2 IPv4/IPv6
IPv6 compliance is a goal for this request. On-premise portions of the solution must support IPv6 for network communications. Controls on network communications must apply to both IPv4 and IPv6 communications. 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 as applicable. If the proposed solution is not compliant at time of response submission, the respondent shall provide an estimated timeline to achieve IPv6 compliance.

2.2 FedRAMP
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Therefore:

- If the approved solution is cloud based, the Agency requires a FedRAMP compliant solution listed on www.fedramp.gov under “FedRAMP Ready Cloud Systems” or evidence that the Vendor is actively pursuing FedRAMP compliance or provide evidence acceptable to the Agency that the security controls are equivalent to FedRAMP requirements
- If the approved solution is not cloud based, as a minimum, the vendor shall provide a system security plan and privacy threshold analysis/privacy impact analysis, incident
response and contingency plans, and an independent assessment of the security control effectiveness.

2.3 **Access to Sensitive Information**

In conjunction with contract performance Vendor personnel may require access to Sensitive Agency Information. Sensitive Agency Information includes Personally Identifiable Information (PII). Sensitive Agency information, including systems or records, is protected under the Privacy Act. Sensitive Agency Information may also exist in other types of records, such as databases, log files, e-mail, and correspondence files. Therefore, all Vendor personnel are responsible for recognizing Sensitive Information, avoiding inappropriate or accidental access, use, or disclosure in accordance with Agency IT policies, and proper procedures for incident reporting.

In addition, written preapproval from the COR, or the Chief Information Officer (CIO) or delegate, is required prior to the use or storage of Sensitive Information or sharing of Sensitive Information by the Vendor with any subvendor, person, or entity. The Vendor shall not remove, copy or transfer Sensitive Information from approved location(s), electronic device(s), or other container(s), without prior approval of the CIO, or designate.

2.4 **Information Security Incidents**

An information security incident is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure or acquisition, or unauthorized access of any Vendor or Government systems or information.

*Information Security Incident Reporting Requirements.* All Information Security Incidents shall be reported in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant. The Agency will determine when an Incident requires additional focus and attention:

- Vendor personnel shall report all Information Security Incidents to the COR and IT Security, orally and in writing, not later than 30 minutes, after becoming aware of a potential or actual Incident, regardless of day or time
- When notifying the COR and IT Security via email copy the Contracting Officer if possible; when reporting the incident by phone or face-to-face, or if the Contracting Officer’s email is not immediately available; contact the Contracting Officer immediately after reporting the incident to the COR
- When reporting SI incidents in writing (i.e. emails or written incident reports) the Vendor shall not forward, include, or repeat Sensitive Information in the subject or body
- As required and preapproved by the Government Vendor personnel shall transmit Sensitive Information (or attachments containing SI) in accordance with (IAW) FIPS 140-2 compliant encryption methods. Passwords shall not be communicated in the same email as attachments
- As required Vendor shall also provide supplementary information or reports related to a previously reported incident directly to the COR and IT Security using the following email subject line: “Supplementary Information/Report related to previously reported incident ## [insert number].”
Information Security Incident Response Requirements. All determinations related to Information Security Incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by authorized Agency officials at the Agency’s discretion;

- The Vendor shall provide full access and cooperation for all activities determined by the Agency to be required to ensure an effective Sensitive Information or Incident Response, including but not limited to, all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents
- The Vendor shall also cooperate and assist the Agency in Incident Response activities, including but not limited to, inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Incident and/or liability for any additional Response activities
- The Vendor shall cooperate and assist the Agency with responding to and supporting other Federal agencies and/or third parties to aid in Incident Response activities
- The Vendor shall be responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by the Agency, whether incurred by the Agency, agents under contract or on assignment to the Agency, or by third party firms.

The Vendor shall provide and maintain a detailed summary document demonstrating how their SECURE WEB ACCESS POINT (WEB PORTAL) meets each of the above SOW requirements for this section.

2.5 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. If a respondent’s system does not have a FIPS certification, they must provide evidence that their system has been assessed as FIPS compliant through a deployment at a federal agency. This evidence must include the name, agency, and contact information for the authorizing official.

In regards to FISMA, the government will assess whether the respondent offers evidence of FISMA authorization at the Moderate impact level. The respondent will provide evidence of an ATO, contact information for the authorizing official, or provide evidence that their system is currently undergoing a authorization review.
3 Pricing

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

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

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

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency</td>
<td>“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.</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>Blacklist</td>
<td>Application or software not deemed acceptable and have been denied approval. This may vary between agencies.</td>
</tr>
<tr>
<td>Bureau</td>
<td>A sub-Agency Bureau level organization, which is using this contract vehicle, as defined by OMB (<a href="http://www.whitehouse.gov/sites/default/files/omb/circulars/a11/current_year/s79.pdf">www.whitehouse.gov/sites/default/files/omb/circulars/a11/current_year/s79.pdf</a>).</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device; Staff brings their personally-owned devices and the Enterprise installs capabilities such as email on them. May also refer to bringing devices from other agencies.</td>
</tr>
<tr>
<td>CAC</td>
<td>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.</td>
</tr>
<tr>
<td>Capability</td>
<td>A technical service requirement that is a component of the base service.</td>
</tr>
<tr>
<td>CBP</td>
<td>Customs and Border Protection</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf; solutions that can be purchased in a complete form from existing commercial vendors.</td>
</tr>
<tr>
<td>DANIEL</td>
<td>DHS Advanced Network Integration and Experimentation Lab</td>
</tr>
<tr>
<td>Data Plan</td>
<td>Includes web browsing, send and receive email, download attachments, downloading applications, and application data usage.</td>
</tr>
<tr>
<td>Device</td>
<td>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.</td>
</tr>
<tr>
<td>Feature</td>
<td>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.</td>
</tr>
<tr>
<td>FAS</td>
<td>Federal Acquisition Service.</td>
</tr>
<tr>
<td>FICAM</td>
<td>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.</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards.</td>
</tr>
<tr>
<td>FSSI</td>
<td>Federal Strategic Sourcing Initiative; FSSI Wireless provides wireless service and device ordering capabilities to Government agencies.</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte or 1000 MB of data.</td>
</tr>
<tr>
<td>GFE</td>
<td>Government Furnished Equipment.</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System; A network of orbiting satellites that enable receivers on the ground.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>Government</td>
<td>All government entities that use or administer this contract vehicle, including state, local and education.</td>
</tr>
<tr>
<td>Government Web Store</td>
<td>Concept of web-based acquisition interface and management platform where government stakeholders (employees, citizens, partners) may initiate purchases, manage previous purchases, and manage vendor relationships. Concept is based on enterprise version of a commercial web storefront.</td>
</tr>
<tr>
<td>HSPD-12</td>
<td>Homeland Security Presidential Directive 12, which (among other things) directs agencies to deploy 2-factor authentication for information systems.</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine to machine technologies that allow both wireless and wired systems to communicate with other devices of the same ability.</td>
</tr>
<tr>
<td>MAS/MAM</td>
<td>Mobile Application Services/Mobile Applications Management.</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte, a common term used to describe the amount of data being sent over a wireless network.</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second, a common term used to describe wireless transmission speeds.</td>
</tr>
<tr>
<td>Mobile Device</td>
<td>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.</td>
</tr>
<tr>
<td>Mobile Device Management (MDM)</td>
<td>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.</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Ordering Entity</td>
<td>Any Agency, sub-Agency, state or local government that is using this contract vehicle.</td>
</tr>
<tr>
<td>Ordering Agency</td>
<td>The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency.</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identification Verification</td>
</tr>
<tr>
<td>Portal</td>
<td>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.</td>
</tr>
<tr>
<td>Secure Communications</td>
<td>Communication services that includes security components such as encryption to ensure the privacy and integrity of the communications.</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Electronic handheld wireless device that integrates the functionality of a mobile cellular phone, personal digital assistant (PDA) or other information appliance.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subsystem</td>
<td>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.</td>
</tr>
<tr>
<td>TEMS</td>
<td>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].</td>
</tr>
<tr>
<td>Text Messaging or SMS</td>
<td>Text Messaging or Short Message Service (SMS) is the exchange of brief written messages between cellular phones, smartphones, and data devices over cellular networks.</td>
</tr>
<tr>
<td>Third-Party Direct Billing</td>
<td>The receipt of invoices from parties other than the Vendor for services within or outside the scope of this agreement.</td>
</tr>
<tr>
<td>Trade Agreements Act (TAA)</td>
<td>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.</td>
</tr>
<tr>
<td>Trouble Ticket</td>
<td>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.</td>
</tr>
<tr>
<td>WLAN Calling</td>
<td>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.</td>
</tr>
<tr>
<td>White List</td>
<td>Whitelist: Application or software considered safe to run, and is preapproved.</td>
</tr>
<tr>
<td>Wireless Systems and Subsystems</td>
<td>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.</td>
</tr>
<tr>
<td>24/7 phone support</td>
<td>Technical support and user assistance is provided by telephone and Internet 24 hours a day, 365 days (or 366 during leap years) per year.</td>
</tr>
</tbody>
</table>