SIN 517312 Wireless Mobility Solutions Required Checklist

This document is required to be completed by the offeror/contractor in order to add SIN 517312 to any Multiple Award Schedule (MAS) offer submission / contract.

I. Introduction:

This document will assist offerors / contractors when submitting a complete and accurate Add SIN request as required by the IT Category Attachment to the MAS Solicitation. It is required to be filled out by the offer / contractor in order to add SIN 517312 to their offer/contract.

II. Submission Instructions:

The following information is required when requesting to add SIN 517312 to a MAS contract:

TAA Compliant Statement: _____certifies that all proposed products are TAA compliant per The Trade Agreements Act (19 U.S.C. §§2501-2581).

_ Letter of Commitment (Only applicable if offeror is other than the manufacturer/ supplier and adding a new manufacturer - See I-FSS-644 Dealers and Suppliers)

_ Terms of Service (TOS) Agreements (only if applicable)

III. Technical Proposal:

(See SCP-FSS-001, Instructions Applicable to All Offerors- Evaluation Factors for Contract Award)

Relevant Project Experience, as it applies to the new subcategories under the SIN. (see Solicitation-(2) Section II--Technical Proposal")

IV. Subcategory Election:

Please select the desired subcategory under SIN 517312 based on the brief description of the mobility subcategories listed below:

1. __ **Wireless Carrier Services** - Wireless Carrier Services include but are not limited to, Wireless Telecommunications Carriers and Telecommunication Resellers of Wireless Services) provide mobile communications services across CONUS and OCONUS locations.

Requirements:
   A. Voice Service plans and Features that enable mobile voice communications such as Voicemail, Three-way calling, Tethering, etc.
   B. Data Service plans and Features – that provide connectivity and communications for data-capable mobile devices.
   C. Service Enabling End-Points – mobile end-points bundled with voice and data service plans which are included at no cost to the ordering entity.

D. Wireless infrastructure components (which do not include a service plan or features but may include labor) offered under a monthly lease arrangement or recurring charge to ordering entities.

2. __ **Other Mobility End-Point Infrastructure - Mobility infrastructure** - Includes mobile infrastructure equipment for implementing mobile solutions or enhancing wireless communications. Also includes endpoints and miscellaneous hardware included with a mobile solution or service.

3. __ **Mobility-as-a-Service (MaaS)** -A subscription-based, mobile management service   suite enabling mobile endpoints, including service enabling devices to be managed, and utilized as a service. In this context a mobile endpoint is a user interface that requires wireless connectivity to communicate with an enterprise or carrier network. The service provider retains asset ownership of the endpoint(s) and provides service regarding asset issuance, endpoint performance management, service plan management, that mobility management software, and support services into a full solution that minimizes prior device-centric costs and operations.

Requirements
   A. Planning and Management of Agency MaaS Needs and Solutions
   B. Device Provisioning, Kitting, and Delivery
   C. Mobile Device Management and Device Refresh
   D. Ongoing Helpdesk Support
   E. Logistics for end-of-life disposal / recycling

4. __ **Enterprise Mobility Management (EMM)** - A cohesive set of tools, software, and service capabilities for provisioning, management, security, and control of mobile endpoint functionality, its applications, features, and content.

5. __ **Mobile Backend-as-a-Service (MBaaS)** - Mobile application development and delivery service comprised of platform, tools, services, and libraries to develop, integrate, test and publish mobile applications to backend cloud storage and processing resources.

6. __ **Telecom Expense Management Services (TEMS)** - Enterprise solutions that support the lifecycle management of mobility and telecom-related assets.

7. __ **Mobile Application Vetting** - Includes software, processes, and tools required to test, validate, and verify mobile apps against a baseline of security, privacy, and organization-specific requirements and policies.

8. __ **Mobile Threat Protection (MTP)** - Solutions and services that monitor the mobile device in real-time to identify mobile threats that may compromise the mobile

device, mobile applications, or data residing on the device that are not addressed by EMM/MDM or App Vetting.

9. __ **Mobile Identity Management** - Mobile Identity Management is a set of complementary products and solutions that issue and maintain certificates, which may include Derived PIV Credential usage.

Requirements
    A. Wifi authentication
    B. Virtual Private Networking
    C. User authentication to COTS, SaaS, and GOTS applications and services
    D. HTTPS/TLS Data in Transit
    E. Data Encryption
    F. Signing of individual documents and records

10. __ **Internet of Things (IoT)** - The design, development, operation or maintenance of an infrastructure of networked components comprised of computing resources, digital sensors, actuators, and human interfaces that are combined into systems to achieve specific goals.

11. __ **Other/Mobile Services-** wireless communication services not commonly used across agency enterprises due to unique usage, features, niche application or legacy technology requirements. Examples include paging, short term rental/disposable endpoint component, and satellite-only communications providers. Vendors under 517312 prior to SIN rewrite, who DO NOT fall under the subcategories, 1-10, will be placed under subcategory 11, (Other/Mobile Services).

V. Submitting the Modification Request:
You may submit your modifications electronically (only) to the following:

a.) Submit via www.eoffer.gsa.gov

NOTE: Prior to the submission of your modification, please call your current MAS Schedule Information Technology Category (ITC) Contracting Officer (CO) to indicate your company is submitting a modification to add 517312.

517312 --- Wireless Mobility Solutions - SUBJECT TO COOPERATIVE PURCHASING
The MAS Information Technology SIN for Wireless Mobility Solutions includes a variety of services that address the mobility needs of government agencies. The sub-categories associated with the Wireless & Mobile Services SIN 517312 are listed below beginning on page 4 of this document.

Vendor Submission Requirements

Vendor submissions shall use this document for describing their offering for each subcategory they wish to be considered under. If a vendor requires additional space to describe their offering, or if a vendor desires to provide additional documents, please check the box next to "Additional Documentation Attached". Attachments may be submitted using Adobe, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and/or Microsoft Visio. The preferred document type is Adobe. Additionally, any attachments shall be named based on the subcategory or subcategories that they are supporting. The subcategory or subcategories that an attachment is supporting should also be listed at the TOP of at least the title page of each document. These submissions should describe how the vendor plans on providing each subcategory they wish to be considered under, not simply case studies of past awards. Case studies are an additional submission requirement, to be used as a reference and/or to show positive past performance.

Subcategories

1.   Wireless Carrier Services
(including, but not limited to, Wireless Telecommunications Carriers and Telecommunication Resellers of Wireless Services) which support mobile communications in CONUS and OCONUS locations
   A. Voice Service plans and Features that enable mobile voice communications such as Voicemail, Three-way calling, etc.
   B. Data Service plans and Features – that provide connectivity and communications for data-capable mobile devices.
   C. Service Enabling Devices (SEDs) – mobile devices bundled with voice and data service plans which are included at no cost to the ordering entity.
   D. Wireless infrastructure components (which do not include a service plan or features but may include labor) offered under a monthly lease arrangement or recurring charge to ordering entities.

Vendor Submission:
Additional Documentation attached

2.   Other Mobility End-Point Infrastructure - Mobility infrastructure
Includes mobile infrastructure equipment for implementing mobile solutions or enhancing wireless communications. Also includes user interfaces and miscellaneous hardware included with a mobile solution(s) or service.

Vendor Submission:
Additional Documentation attached

3.   Mobility-as-a-Service (MaaS)
A subscription-based, mobile management service suite enabling mobile endpoints, including SEDs to be managed, and utilized as a service. In this context a mobile endpoint is a user interface that requires wireless connectivity to communicate with an enterprise or carrier network. The service provider retains asset ownership of the endpoint(s) and provides service regarding asset issuance, endpoint performance management, service plan management, that mobility management software, and support services into a full solution that minimizes prior device-centric costs and operations. MaaS includes end-to-end management with respect to:
   A. Planning and Management of Agency MaaS Needs and Solutions
   B. Provisioning, Kitting, and Delivery
   C. Enterprise Mobility Management and SED Refresh
   D. Ongoing Helpdesk Support
   E. Logistics for end-of-life disposal /recycling

Vendor Submission:

Additional Documentation attached

4.   Enterprise Mobility Management (EMM)

Is a collective set of tools, software, and service capabilities required for the provision, management, security, and control of mobile device functionality, its applications, features and content that are delivered to government (or contractor) owned or employee owned (BYOD) mobile devices. The three main EMM areas include mobile device management (MDM), mobile application management (MAM), and mobility content management (MCM).

Vendor Submission:
Additional Documentation attached

5.   Mobile Backend-as-a-Service (MBaaS)

Represents mobile application delivery solutions that provide mobile application developers with a platform, tools, and libraries to develop, integrate, test and publish their applications to backend cloud storage and processing resources while also providing common features such as user management, push notifications, social networking integration, and other features demanded by mobile users.

Vendor Submission:
Additional Documentation attached

6.   Telecom Expense Management Services (TEMS)

Enterprise solutions which support the full lifecycle management of mobility and telecommunications assets. TEMs functions include cataloging, ordering, deployment, workflow management, inventory control, invoicing, disposition, and reporting of an enterprise's mobility resources. TEMS providers may offer standalone solutions and other support services, such as data and system integration services, to implement and maintain their solution.

Vendor Submission:
Additional Documentation attached

7.   Mobile Application Vetting

Application Vetting or "app" vetting (also referred to as "app threat intelligence" or "threat protection services") refers to software, processes, and tools required to test, validate, and verify mobile apps against a baseline of security, privacy, and organization-specific requirements and policies. Vendors may provide on premise, cloud-based, or outsourced app vetting solutions that run static and/or dynamic analysis tests and reporting on apps to detect security vulnerabilities and malicious or privacy violating behaviors.

Vendor Submission:
Additional Documentation attached

8.   Mobile Threat Protection (MTP)

MTP is a component of a layered Mobile Endpoint Protection Strategy that covers the major areas not addressed by EMM/MDM or App Vetting. MTP solutions monitor the mobile device in real-time to identify mobile threats that may compromise the device, mobile applications, or data residing on the device. MTP integrates with an EMM system deployed on devices resulting in remediation or quarantining of the threat. The MTP solution evaluates an application threat and compliance against a set of pre-defined agency policies based upon acceptable risks, it validates operating system (OS) integrity against any compromise, it detects network threats such as MITM (Man-in-the-Middle) attacks and will detect device configuration risks.

Vendor Submission:
Additional Documentation attached

9.   Mobile Identity Management (MIM)

MIM is the secure integration of the attributes that unerringly identify a person in the physical and online environments, within the mobile device. MIM is a set of complementary products and solutions that issue and maintain certificates, which may include Derived PIV Credential (DPC) usage. A valid PIV card is required to issue a DPC. Once issued, credentials on a mobile device will support:
   A. WIFI authentication
   B. Virtual Private Networking
   C. User authentication to Commercial off the Shelf (COTS), Software-as-a-Service (SaaS), and other applications and services
   D. Data in Transit
   E. Data Encryption
   F. Signing of individual documents and records

Vendor Submission:
Additional Documentation attached

10. Internet of Things (IoT)

Internet of Things (IoT) service providers engage with those who design, develop, operate, or maintain an infrastructure of networked components comprising computing resources, digital sensors, actuators, and human interfaces that are combined into systems to achieve specific goal(s).

Vendor Submission:
Additional Documentation attached

11. Other/Mobile Services

Wireless communication services not commonly used across agency enterprises due to unique usage, features, niche application or legacy technology requirements. Examples include paging, short term rental/disposable endpoint component, and satellite-only communications providers.

Vendor Submission:
Additional Documentation attached