STATEMENT OF WORK

CONNECTIONS II

Order Identification Number: [######]  
Managed Mobility

Issued by:

[Agency Logo]

[Name of Agency]

[Address of Agency]

DATE: [DD MM YYYY]

**Template Guidance**

**Purpose**

The purpose of this template is to provide Agencies with a baseline document for procurements involving Connections II. This template is based on previous SOWs that were vetted, and thus saves Agencies time and resources during SOW development. The Agency can start with this baseline template to create a SOW and then make alterations to the document to meet their needs. For example, an Agency may want to include a scenario or technology not within the template. In this case the Agency would add text to cover the new scenario or technical requirements.

**Conventions**

Following are the conventions used in the Template.

**Replacement Text**

[Shaded/bracketed] text is replacement text. Replacement text is surrounded by square brackets “[].”

Replacement Text is text the Agency needs to replace with specific information and differs by SOW. For replacement text, the pound sign “#” indicates a number is required. A number within the square brackets [15] indicates from past experience this is the value used by most Agencies, but the value can be adjusted to meet SOW and Agency needs. For example, “[15] days” shows that most Agencies require 15 days for a particular activity. If there are specific differences in the Agency’s required timeframes, such as the inclusion of a holiday or other schedule considerations, then the Agency adjusts the number of days accordingly.

After entering replacement text, delete the square brackets and remove the shading.

**Text Boxes**

Text Boxes contain instructional information to SOW authors which may be retained in or deleted from the document as needed. Text Boxes may also explain options within the SOW or Text Boxes may direct the deletion of instructional pages or text, as is the case with this page.

Table of Contents

[1 Project Description 1](#_Toc408997934)

[1.1 Purpose 1](#_Toc408997935)

[1.2 Background 1](#_Toc408997936)

[1.2.1 Organization and Mission 2](#_Toc408997937)

[1.2.2 Objectives for [Project Name] 2](#_Toc408997938)

[1.3 Scope 2](#_Toc408997939)

[1.3.1 General Description of Requirements 2](#_Toc408997940)

[1.4 Acquisition Type Selected 3](#_Toc408997941)

[1.5 Period of Performance 3](#_Toc408997942)

[1.6 Place of Performance 4](#_Toc408997943)

[1.7 Local Codes, Licensing, and Permit Requirements 4](#_Toc408997944)

[1.8 Security Requirements 4](#_Toc408997945)

[1.9 Government Furnished Equipment 4](#_Toc408997946)

[1.10 Contractor Furnished Equipment 4](#_Toc408997947)

[1.11 Fair Opportunity 4](#_Toc408997948)

[2 Statement of Work 5](#_Toc408997949)

[2.1 Task 1 – Life Cycle Management 5](#_Toc408997950)

[2.1.1 Subtask 1 – Implementation/Installation 6](#_Toc408997951)

[2.1.1.1 Project Management 6](#_Toc408997952)

[2.1.1.2 Deployment/Migration/Transition (If applicable) 6](#_Toc408997953)

[2.1.1.3 Enterprise Systems Integration 7](#_Toc408997954)

[2.1.1.4 Training 7](#_Toc408997955)

[2.1.1.5 Demonstration Platform 7](#_Toc408997956)

[2.1.2 Subtask 2 – Operations Support 7](#_Toc408997957)

[2.1.2.1 Help Desk 7](#_Toc408997958)

[2.1.3 Subtask 3 – Optional Items 8](#_Toc408997959)

[2.1.3.1 Enterprise Configuration (Optional) 8](#_Toc408997960)

[2.1.3.2 Integration with Federal Strategic Sourcing Initiative Wireless Portal   
(Optional) 8](#_Toc408997961)

[2.1.3.3 Pilot (Optional) 8](#_Toc408997962)

[2.2 Task 2 – High Level Architecture 9](#_Toc408997963)

[2.2.1 Scope/Scale 11](#_Toc408997964)

[2.2.2 Multi-Tenancy 11](#_Toc408997965)

[2.2.3 Solution Security 11](#_Toc408997966)

[2.2.3.1 General Security Controls 11](#_Toc408997967)

[2.2.3.2 FISMA or FedRAMP Requirements 13](#_Toc408997968)

[2.2.3.3 FIPS Requirements 13](#_Toc408997969)

[2.2.3.4 Containerization 13](#_Toc408997970)

[2.2.3.5 IPv6 Support 14](#_Toc408997971)

[2.2.3.6 User Authentication 14](#_Toc408997972)

[2.2.3.7 User Compliance 14](#_Toc408997973)

[2.2.3.8 Alerting 15](#_Toc408997974)

[2.2.3.9 Reporting 15](#_Toc408997975)

[2.2.3.10 Audit Reports 15](#_Toc408997976)

[2.2.3.11 Privacy 16](#_Toc408997977)

[2.2.3.12 Service Delivery Model 16](#_Toc408997978)

[2.3 Task 3 – Mobile Device Management 17](#_Toc408997979)

[2.3.1 Mobile Device Management (MDM) General Requirements 19](#_Toc408997980)

[2.3.2 Device Enrollment 19](#_Toc408997981)

[2.3.3 Device Profiles 20](#_Toc408997982)

[2.3.4 Device Feature Management 21](#_Toc408997983)

[2.3.5 Data Management 22](#_Toc408997984)

[2.3.5.1 Data Collection 22](#_Toc408997985)

[2.3.5.2 Continuity of Operations and Disaster Recovery 22](#_Toc408997986)

[2.3.5.3 File Management 22](#_Toc408997987)

[2.3.5.4 Personal Information Management 23](#_Toc408997988)

[2.3.5.5 Security Content Automation Protocol Support 23](#_Toc408997989)

[2.3.6 Device Inventory Management 23](#_Toc408997990)

[2.3.7 Device Inventory Reports 24](#_Toc408997991)

[2.3.8 System Performance Reports 24](#_Toc408997992)

[2.3.8.1 Mobile Device Management Security/Compliance Reports 25](#_Toc408997993)

[2.3.9 Classified Data (Optional) 25](#_Toc408997994)

[2.3.10 Personal Identity Verification/Common Access Card Support (Optional) 25](#_Toc408997995)

[2.3.11 Biometric Support (Optional) 25](#_Toc408997996)

[2.3.12 Network Monitoring (Optional) 25](#_Toc408997997)

[2.4 Task 4 – Provide Mobile Application Management 26](#_Toc408997998)

[2.4.1 Application Deployment 27](#_Toc408997999)

[2.4.2 Mobile Application Store (MAS) 27](#_Toc408998000)

[2.4.3 Application Security 28](#_Toc408998001)

[2.4.3.1 Mutual Authentication 28](#_Toc408998002)

[2.4.3.2 Application Installation Control 28](#_Toc408998003)

[2.4.3.3 Blacklisting/Whitelisting 28](#_Toc408998004)

[2.4.3.4 Application Environment Requirements 28](#_Toc408998005)

[2.4.3.5 Application Signing 28](#_Toc408998006)

[2.4.4 Third-Party Application Mutual Authentication (Optional) 28](#_Toc408998007)

[3 Labor Types 29](#_Toc408998008)

[3.1 Personnel Requirements 29](#_Toc408998009)

[3.2 Proposed Personnel 30](#_Toc408998010)

[3.3 Special Qualifications and Certifications 30](#_Toc408998011)

[4 Travel and Other Direct Costs (ODC/Un-priced Items) 31](#_Toc408998012)

[4.1 Travel 31](#_Toc408998013)

[4.1.1 Local Travel 31](#_Toc408998014)

[4.1.2 Distance Travel 31](#_Toc408998015)

[4.2 Other Direct Cost (ODC/Un-priced Items) 31](#_Toc408998016)

[5 Invoice Requirements 32](#_Toc408998017)

[5.1 Detailed Billing Requirements 32](#_Toc408998018)

[5.2 Invoice Address, Data Format and Delivery Method 32](#_Toc408998019)

[5.2.1 Invoice Address 32](#_Toc408998020)

[5.2.2 Invoice Submission 33](#_Toc408998021)

[5.2.3 Billing Cycle and Data Elements 33](#_Toc408998022)

[5.2.4 Electronic Funds Transfer (EFT) 34](#_Toc408998023)

[5.3 Billing for Other Direct Costs (ODCs) or Unpriced Item 34](#_Toc408998024)

[5.3.1 Invoice for Travel Expenses 34](#_Toc408998025)

[6 Section 508 35](#_Toc408998026)

[7 Proposal Instruction to Offerors 35](#_Toc408998027)

[7.1 General Instructions 36](#_Toc408998028)

[7.1.1 Materials Submitted 36](#_Toc408998029)

[7.1.2 Format 36](#_Toc408998030)

[7.1.3 Proprietary Data 37](#_Toc408998031)

[7.2 Preparation of Technical Proposal 37](#_Toc408998032)

[7.2.1 Executive Summary 38](#_Toc408998033)

[7.2.2 Technical Approach 38](#_Toc408998034)

[7.2.3 Management Approach 38](#_Toc408998035)

[7.2.4 Proposed Personnel Qualifications and Certifications 39](#_Toc408998036)

[7.2.5 Past Performance 39](#_Toc408998037)

[7.3 Preparation of Price Proposal 40](#_Toc408998038)

[8 Evaluation Factors and Basis for Award 40](#_Toc408998039)

[8.1 Evaluation Methodology and Basis for Award 40](#_Toc408998040)

[8.2 Evaluation Approach – Trade Off or Lowest Price Technically Acceptable 41](#_Toc408998041)

[8.3 Technical Evaluation Criteria 42](#_Toc408998042)

[8.4 Price Evaluation Criteria 44](#_Toc408998043)

[9 Task Order Award 45](#_Toc408998044)

[10 Organizational Conflicts of Interest 45](#_Toc408998045)

[11 List of Acronyms 46](#_Toc408998046)

[12 Attachments 48](#_Toc408998047)

[12.1 Attachment A – Project Management Plan 48](#_Toc408998048)

[12.2 Attachment B – Support Locations 48](#_Toc408998049)

[12.3 Attachment C – Pricing Requirements 48](#_Toc408998050)

[12.4 Attachment D – Pricing Template 48](#_Toc408998051)

[12.5 Attachment E – Past Performance Worksheet 49](#_Toc408998052)

[12.6 Attachment F – Task Order Deliverables 49](#_Toc408998053)

List of Tables

[Table 1. Date of Task Order Award 4](#_Toc408804760)

[Table 2. Number of each Type of Proposal Volume 36](#_Toc408804761)

[Table 3. Offerors’ Proposal Factors and Sub-factors 42](#_Toc408804762)

List of Figures

[Figure 1. Managed Mobility Framework 9](#_Toc408804957)

# Project Description

**[Project Name]**

Note: Text boxes contain informational material that should be deleted by the Agency when finalizing this document. Please delete the box and use this space to give a short overview of the Project named above.

The Connections II Managed Mobility Project Statement of Work (SOW) Template is provided by the General Services Administration (GSA) to help customer Agencies contract for Managed Mobility support. It is recognized that agencies have a very wide spectrum of Managed Mobility tasks that can be performed by a Connections II offeror. This SOW Template is designed as an example SOW that must be tailored to meet an Agency’s specific needs.

Note also that although the SOW Template implementation tasks are generally ordered in the sequence they will be executed, they may overlap in some cases and be performed in parallel (see *Section 2 ‑ Statement of Work*).

The SOW Template is intended to accommodate Agency customers with Managed Mobility services. All task-specific sections are offered as examples of what sort of information should be entered by the agency. It is assumed that client agencies will have their own specific Managed Mobility tasks with varying levels of detail and therefore parts of the SOW Template may be tailored, replaced or omitted entirely, depending on the requirements of the Agency.

## Purpose

This Statement of Work (SOW) supports the selection of a “value-added” mobile service manager to set up a Managed Mobile Service Delivery Platform under the GSA Connections II contract. This platform will be used to manage mobile government services, leveraging mobile technologies to increase quality and improve overall efficiency and security in [Agency Name] mobile communications processes. This task order does not cover obtaining wireless service plans for mobile devices.

The government’s need for secure, cost-efficient mobility management is driven by the Digital Government Strategy requirement 5.5, which seeks to “Set up a government-wide mobile device management platform” (http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html). Managed mobility is a core capability for effectively scaling the secure deployment and management of mobile applications, enterprise data on mobile devices, and management of the devices and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to the agencies.

## Background

Use this space to describe the purpose for this task and the environment in which it will be performed.

In order to provide background information relevant to this SOW, this section should include at a minimum the following subsections.

### Organization and Mission

[Add summary Agency-specific information here].

### Objectives for [Project Name]

[This is where the Agency provides justification for and lists the benefits of implementing this project, such as “This task order for [Agency/Site], [Project Name], will provide valuable benefits by improving operational efficiencies and improving the quality, efficiency and security of agency communications, etc.”]

## Scope

Managed Mobility is a service portfolio that includes mobile device management, mobile application management, and mobility lifecycle services.

Scope information for this SOW should include the following subsections at a minimum. Please consider such details as number and types of devices and organizational structure, e.g.: The offeror’s solution should be scalable to 10,000 managed devices and higher. The proposed solution must be able to support the Agency’s hierarchical organizational structure within the solution, and support multiple configurations for each of the Mobile Device Management (MDM) requirements below.

### General Description of Requirements

Managed Mobility is a core capability for effectively scaling the secure deployment and management of mobile applications, enterprise data on mobile devices, and management of the devices and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to the agencies. The Managed Mobility program defines a functional framework, and Government agencies should be able to work with all components of the framework seamlessly in an easy to use, secure, integrated solution.

The bulleted items below should be viewed as example text. In filling out this section, please describe what is needed to complete the project and how it should be accomplished. For example, how many devices and what type of devices are required? What networks will accommodate them? Does there need to be configuration management based on network connection? What are the security requirements?

The offeror shall provide a solution with the following characteristics:

* Ability to enforce enterprise rules while allowing Agency/Bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities
* Ability to take the following action upon a group of devices from a search: Reassign to Group (any type of logical grouping). User or device groupings are an example.
* Ability to assign Profile to one or many Groups (any type of logical grouping). User or device groupings are an example.
* Ability to view required applications from the Mobile Application Store (MAS)
* Ability to view and run reports on user and device information for all Smartphones including usage and cost
* Ability to run reports by groups of users to include location
* Ability for the solution to support a Software Development Kit (SDK) or Application Programming Interface (API) Framework to integrate with existing or future Enterprise Applications
* Ability for the MDM solution to be able to be monitored from industry standard tools -e.g. HP OpenView, System Center Operations Manager (SCOM), etc.
* Ability for the MDM solution to integrate certificates from the solution’s internal Public Key Infrastructure (PKI) system to mobile devices as well as third party public PKI providers such as VeriSign
* Ability for the MDM to perform its functions from within a secure Virtual Private Network (VPN) used to transport all enterprise data (i.e., no MDM control data transported unencrypted across the open internet).

Suggested examples of project tasks are listed below. Agency may remove or modify the narratives as needed. This section is intended only as a high level overview.

## Acquisition Type Selected

The agency will need to determine which contract type to use (either Firm Fixed Price [FFP] or Time and Material [T&M]).

[Agency] has selected the Connections II Contract for the [Project Name] Project. Connections II allows FFP or T&M task orders. This requirement will be for a [Add Agency selected contract type here] task order.

This solicitation includes requirements for all labor and equipment necessary to support [task name].

The offeror shall adhere to the terms and conditions of the Connections II Contract, and shall meet and comply with the Agency-specific requirements described in this SOW.

## Period of Performance

The Tasks agreed upon by [Agency] and the offeror will remain in effect for the life of the Connections II Task Order. The offeror shall provide technical support, and shall procure and install [or recommend] equipment for these Tasks. The term of the order will be from the date of award through a base period (for example, one year) plus [n] option periods. The overall period of performance is specified in the following table.

Table 1. Date of Task Order Award

|  | **Start Date** | **End Date** |
| --- | --- | --- |
| **Base Year** | <Performance\_Start\_Date> | <Performance\_End\_Date\_Base\_Period> |
| **Option Period 1** | <Performance\_Start\_Date\_Option\_Period\_1> | <Performance\_End\_Date\_Option\_Period\_1> |
| **Option Period 2** | <Performance\_Start\_Date\_Option\_Period\_2> | <Performance\_End\_Date\_Option\_Period\_2> |
| **Option Period 3** | <Performance\_Start\_Date\_Option\_Period\_3> | <Performance\_End\_Date\_Option\_Period\_3> |
| **Option Period n** | <Performance\_Start\_Date\_Option\_Period\_n> | <Performance\_End\_Date\_Option\_Period\_n> |

***[Note: This table is for illustration purposes only. Connections II ends January 2021. An order placed before January 19, 2021 can remain active up to January 2026, if so planned. The Agency has the option to add or remove years in order to complete the [Project Name].]***

## Place of Performance

The offeror shall comply with the geographic requirements specified in this solicitation to provide support. The Place of Performance will be specified in *Attachment B – Support Locations*.

## Local Codes, Licensing, and Permit Requirements

In the performance of this task order, the offeror agrees to abide by all laws, codes, rules and regulations set forth with regard to the equipment by municipal or State authorities having jurisdiction in effect on the date of this task order. The offeror shall be responsible for obtaining all local licenses and permits. This section applies to all tasks associated with this task order.

## Security Requirements

Please specify if this project is “Classified” or “Unclassified.” If “Classified,” specify to what level. If contractor personnel will need to hold or obtain some form of clearance, or meet some other security-related condition (e.g., American citizenship), please specify.

All documentation (i.e., DD 254) required for security certification will be the responsibility of the offeror and the client organization.

## Government Furnished Equipment

Upon the award and placement of the task order, Government Furnished Equipment (GFE) may be made available by the Agency for use by the offeror to support the tasks. The offeror shall use GFE to provide support services as mutually agreed upon by the offeror and Agency. The offeror shall evaluate all equipment as the Agency directs.

## Contractor Furnished Equipment

The contractor shall furnish all necessary tools, equipment and materials required for performing all work associated with the completion of this requirement, which also includes testing and installation.

## Fair Opportunity

This SOW will be released for Fair Opportunity under Federal Acquisition Regulation (FAR) 16.505.

# Statement of Work

The offeror shall perform the following tasks under the Task Order.

* Task 1 – Life Cycle Management
* Task 2 –High Level Architecture
* Task 3 –Mobile Device Management
* Task 4 –Mobile Application Management

This section describes the full range of offeror support services, equipment, and equipment services that must be provided under this task order.

## Task 1 – Life Cycle Management

A Telecommunications Life Cycle Management (TLM) system is needed to manage the Agency’s devices, applications and services. It shall be able to perform the following functions (elaborated in the table below):

* Project Management
* Implementation
* Training
* Support

The offeror shall describe its compliance with the requirements in the table below.

| **Mobility Life Cycle Management** | **Required or Optional** | **Section** | **Description** |
| --- | --- | --- | --- |
| 1. **Project Management**. The proposed solution shall clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements. | Required | 2.1.1.1 |  |
| 1. **Professional Services**. The offeror shall clearly describe how they provide initial deployment support services including installation, configuration, and the certification of initial solutions, as well as for additional professional services to support specific agency related integrations or customizations. | Required | 2.1.1.2 |  |
| 1. **Enterprise System Integration**. The offeror shall demonstrate experience in providing the steps necessary for deploying, integrating, and securing a mobility solution into an enterprise-wide environment. | Required | 2.1.1.3 |  |
| 1. **Training**. The offeror shall demonstrate how they can be responsible for developing and updating the Mobile Device Management-Mobile Application Store (MDM-MAS) Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan. | Required | 2.1.1.4 |  |
| 1. **Operations Support**. The offeror/solution shall provide access to help desk support that meets the identified criteria. The offeror shall indicate the location of their help desk support. | Required | 2.1.2 |  |
| 1. **Demonstration Platform**. The proposed solution shall possess a fully functional and secure demonstration platform with associated mobile devices to educate potential customers on the use, benefits and technical specification of the solution, and provide access to the portal for the purpose of sampling and demonstrations that will be connected to the offeror’s site through a federal website. | Required | 2.1.1.5 |  |
| 1. **Enterprise Configuration**. The offeror shall demonstrate the non-core integration services as indicated. | Optional | 2.1.3.1 |  |
| 1. **Integration with Federal Strategic Sourcing Initiative (FSSI) Wireless Portal**. The offeror shall demonstrate how to integrate their proposed solution with the FSSI Wireless portal to automatically retrieve asset and plan data, and return relevant data to the FSSI portal. | Optional | 2.1.3.2 |  |
| 1. **Pilot**. The proposed solution shall be delivered within the pre-production pilot timelines and installation dates identified in this RFP and agreed to in the SOW. | Optional | 2.1.3.3 |  |

### Subtask 1 – Implementation/Installation

#### Project Management

The offeror shall clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements.

#### Deployment/Migration/Transition (If applicable)

The offeror shall clearly describe how they provide initial deployment support services. These services are expected for installing, configuring, and certifying the initial deployment of the Mobile Device Management (MDM), Mobile Application Management (MAM) and/or Container solutions, as well as the ability to support specific agency related integrations or customizations. The offeror shall assist the agency with achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.

The offeror shall submit a Transition Plan that details how devices currently in use will transition from existing service in a quick, reliable, and accurate manner to the offered solution. Staffing requirements (offeror 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 offeror shall provide an example of a previous successful on-boarding of 10,000 or more devices. The example shall include a high-level timeline, staffing required, and a summary walk-through of the process (one (1) page maximum for summary walk-through).

The offeror shall also provide an example of an exit transition plan that describes how, in case of termination for any reason, delivered data conforms to an industry standard format capable of being transported to other systems.

#### Enterprise Systems Integration

The offeror shall show how they can provide steps necessary for deploying, integrating, and securing their Mobility Solution into the enterprise-wide environment. This includes such systems as enterprise Telecom Expense management (TEM), Mobile Device/Application Management (MDM/ MAM), email, directories, trouble-ticketing, etc. The steps included are expected to vary depending upon whether the solution is on premise or a cloud solution.

#### Training

All users of the Mobile Device Management –Mobile Application-Management (MDM-MAM) system, which includes end users, administrators and developers, shall be trained to correctly utilize the system. The offeror shall demonstrate how it will develop and update the MDM-MAM Training Material content (Enterprise, User, Administration levels), as well as how it will provide prepackaged online training, training classes, and associated materials described in the Training Plan. The online training may be hosted by the government or the offeror, and the offeror shall provide the required content.

#### Demonstration Platform

The offeror shall possess a demonstration platform to educate potential customers on the use, benefits and technical specification of the solution. The demonstration platform shall be fully functional and secure for use with associated mobile devices to educate potential customers on the use, benefits and technical specification of the solution. Offerors shall provide access to the portal for the purpose of sampling and demonstrations that will be connected to the offeror’s site through a federal website.

### Subtask 2 – Operations Support

#### Help Desk

The offeror shall provide access to help desk support for their solutions. The offeror shall indicate the location of the operational help desk. The proposed solution must satisfy the following criteria:

1. Help desk shall be integrated so end user(s) can report problems within the TLM system, or the agency’s HD system can integrate either tightly or loosely with TLM system
2. End User Help Desk support shall be provided 24 hours per day/7 days per week, including holidays
3. Administrative/Management Help Desk shall be available 8am-5pm in both Eastern Standard Time (EST) and Pacific Standard Time (PST)
4. Help Desks shall utilize a trouble-ticketing system where each request has a unique identifier for tracking purposes
5. Help Desk interaction shall support online requests/resolution, supported with email
6. Telephone (voice) Help Desk support shall be available during business hours [Specify business hours here]
7. The MDM shall support Help Desk remote access to the device for troubleshooting purposes (Optional)

### Subtask 3 – Optional Items

#### Enterprise Configuration (Optional)

This requirement addresses non-core integration, such as Solution connectivity with non-required components (e.g., custom portal, Telecommunications Expense Management System (TEMS) provider system, etc.). [Agency name] has applications that may need to be accessed on mobile devices, but that require configuration services to enable. The offeror shall describe the services they offer of this type. Each configuration service offered shall be accompanied by a successful example from industry or government.

#### Integration with Federal Strategic Sourcing Initiative Wireless Portal (Optional)

[The Federal Strategic Sourcing Initiative (FSSI) Wireless Business Portal Interface (BPI)](http://www.gsa.gov/portal/category/100931) is a secure standard for agencies to interface with cellular carriers to place orders, manage plan/device inventory, and other carrier provided information. The BPI is not a Graphical User Interface (GUI) but merely a secure standard for exchanging data between the customer agency and the carrier. Offerors shall indicate their experience with this standard and their platform's ability to exchange information with third party providers for the purpose of providing complementary services such as device ordering, logistics, configuration, replacement/refresh, disposal, and disposition reporting.

#### Pilot (Optional)

*[Agency to add pilot requirements if applicable]*

Potential free 90-day pilot program for the limited number of telecom assets.

The proposed solution shall be delivered within the pre-production pilot timelines and installation dates identified in this RFP and agreed to in the SOW.

## Task 2 – High Level Architecture

Managed Mobility is a service portfolio that includes mobile device management, mobile application management, and mobility lifecycle services. These are shown below and further discussed in the following subsections. Sections in red font are required capabilities, features or attributes. These requirements will be impacted in the future by the release of the Mobile Security Requirements in the Digital Government Strategy 9.1 guidance.

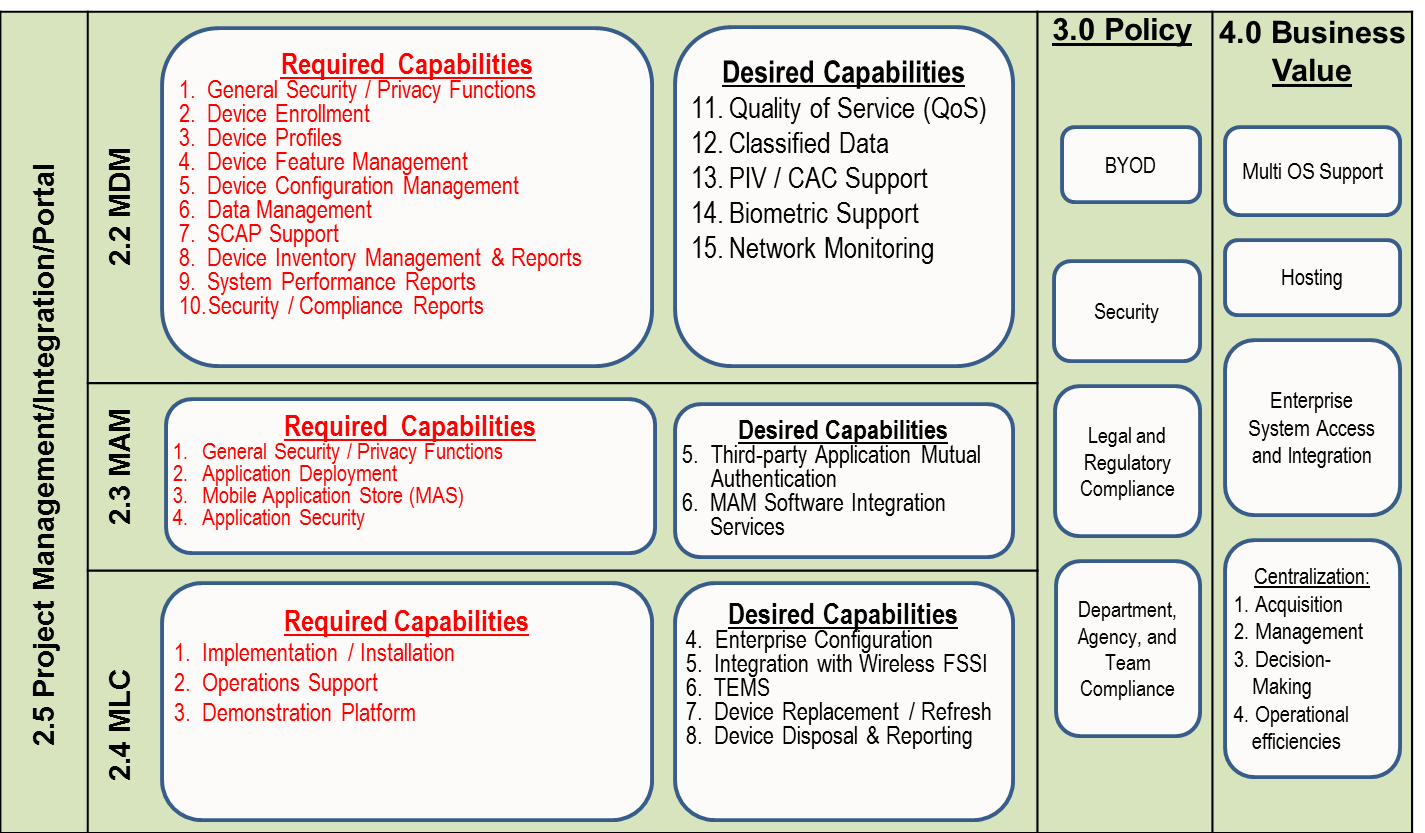


Figure 1. Managed Mobility Framework

The General Managed Mobility Requirements and Past Experience (common for all offerors) have characteristics that represent core capabilities that must be present in order to provide Managed Mobility services to Federal Customers based on the common requirements developed by the inter-agency working group. All questions in this section require a Yes answer in order for the evaluation to proceed further; a No answer in response to any question may result in the offeror being eliminated from consideration for an award. Offerors shall answer the questions, affirming their capability to meet the requirements, and provide a short description of how they have done so.

| **High Level Architecture Requirements  and Offeror Capabilities/Experience** | **Required  or Optional** | **Y/N** | **Section** | **Description** |
| --- | --- | --- | --- | --- |
| 1. **Scope/Scale**. Is the offeror’s solution scalable from an initial requirement of X users to the maximum requirement of Y users? (Y/N) | Required |  | 2.2.1 |  |
| 1. **Multi-Tenancy**. Does the proposed solution support the Department’s/ Agency’s (“tenants”) hierarchical organizational structure within the solution, and support multiple configurations for each of the MDM requirements? | Required |  | 2.2.2 |  |
| 1. **Solution Security**. Does the proposed solution describe how it meets the 14 identified general controls/capabilities of solution security found in the Digital Government Strategy 9.1 guidance? | Required |  | 2.2.3 |  |
| 1. **Federal Information Security Management Act of 2002**. Does the offeror provide evidence that the proposed solution is capable of being certified at the **Federal Information Security Management Act of 2002** (FISMA) moderate impact level? | Required |  | 2.2.3.2 |  |
| 1. **Federal Information Processing Standards Requirements**. Does the offeror provide evidence that their solution uses Federal Information Processing Standards (FIPS) 140 certified cryptographic modules and continued validation? | Required |  | 2.2.3.3 |  |
| 1. **Containerization**. If applicable, does the offeror describe how the proposed solution meets FIPS 140-2, controlled wipe capabilities, and platform-by-platform container protection as it related to BYOD scenarios? | Required |  | 2.2.3.4 |  |
| 1. **IPv6 Support**. Does the offeror provide evidence of either IPv6 compliance or intention to comply? | Required |  | 2.2.3.5 |  |
| 1. **User Authentication**. For cloud-based systems, does the offeror provide evidence of being capable of meeting authentication standards related to the portal and device, as well as 2 multifactor authentication methods? | Required |  | 2.2.3.6 |  |
| 1. **User Compliance**. Does the proposed solution demonstrate the 4 items related to user compliance enablement? | Required |  | 2.2.3.7 |  |
| 1. **Alerting**. Does the proposed solution demonstrate the eight (8) alert capabilities required to notify agency operations staff about devices under their management? | Required |  | 2.2.3.8 |  |
| 1. **Security Reporting Capabilities**. Does the proposed solution demonstrate the eight (8) reporting capabilities, as well as the stated support functions applicable to Audit Reports? | Required |  | 2.2.3.9/.10 |  |
| 1. **Privacy**. Does the proposed solution disclose privacy-impacting features that cannot be disabled? (Y/N) | Required |  | 2.2.3.11 |  |
| 1. **Service Delivery Model**. Is the proposed solution delivered and (optionally) hosted by the provider as a full solution including all hardware, software, hosting, and installation services, using one or more of the following hosting models (on premise, cloud, hybrid)? | Required |  | 2.2.3.12 |  |

### Scope/Scale

This SOW is for procurement of enterprise class MDM/MAM solution scalable to 10000 devices and higher. Use or modify the following language to specify your agency requirements.

The platform shall support [#] devices initially. The solution shall support growth to [#] devices. The solution shall allow flexibility to increase the number of devices in any incremental amount up to the maximum number of devices.

### Multi-Tenancy

The proposed solution shall support the application of hierarchical policy requirements within the [Department’s/Agency’s] (“tenants”) hierarchical organizational structure, and shall support multiple configurations for each of the Mobile Device Management (MDM) requirements below. For example, each tenant may have different help desk contact information, policies, and organizational groupings and hierarchy.

### Solution Security

Data at rest encryption, data in transit encryption (Virtual Private Network [VPN]), and secure applications shall be provided by the proposed Mobile Device Management –Mobile Application Management (MDM-MAM) solution. These capabilities may be accomplished by separate products which are then integrated into the complete MDM-MAM solution.

#### General Security Controls

The offeror shall describe how the solution meets the following general controls/capabilities.

1. Ability to enroll an authorized device before applying any policy.
2. Ability to create Whitelist/Blacklist for device enrollment to include Operating System (OS) versions and device models
3. Allow enrollment of untrusted devices and anonymous/unknown users outside the enterprise into controlled access and network isolation zones as individuals or groups under the MDM
4. Ability to use an existing user attribute repository for enrollment to the new MDM system
5. Native ability with active (device scanning) and passive (on-access scanning) tools to detect, report, and alert on a compromised device (e.g., jail broken/rooted device, malware) and take policy action based upon compliance rules
6. Ability to lock the device or to erase (wipe) ONLY the managed data on a device under the following conditions:
   1. Blacklisted operating system or version (policy)
   2. Exceeding a set number of failed access attempts to the device or MDM application (policy)
   3. Exceeding defined interval for MDM synchronization/policy updates (policy)
   4. Detection of OS jail breaking or application tampering (policy)
   5. Any other stipulated policy violation requiring stated outcome
   6. Remote instruction from MDM (manual)
7. Password policy enforcement in support of **Homeland Security** Presidential Directive 12 (HSPD-12)/Special Publication (SP) 800-53/SP 800-63 requirements in support of Section C.4.2.3.6 User Authentication:
   1. Minimum complexity (length, composition, common words, etc.)
   2. Password lifetime limit
   3. Password re-use limits
   4. Password inactivity timeout (grace period) for device and MDM app
   5. Report password failures beyond policy threshold to MDM
   6. Maximum password attempts before lock or wipe
8. Ability to mask passwords when they appear in the Management GUI except for those administrators authorized based on RBAC authorizations
9. Ability to determine which administrative user made a configuration change in the MDM administrative environment as well as record the change made
10. Ability to determine which device user made a configuration change in the MDM console (self-service logging) as well as record the change made
11. Installation and configuration (update, revocation checking, revocation) of individual and group soft and hardware-based authentication certificates for the mobile device for the following purposes:
    1. Email (Secure/**Multipurpose Internet Mail Extensions** [S/MIME]) signing and encryption
    2. WiFi Configuration
    3. VPN Configuration
12. Ability to send/receive (encrypt and sign; decrypt and verify) messages that use Federal Information Processing Standards (FIPS) 140 certified Public Key Infrastructure (PKI) or S/MIME encryption, where email functionality is delivered by the solution
13. Ability to restrict downloading attachments, copying of data to/from removable media, or otherwise create separate spaces or virtual containers for separating agency data and applications from personal data
14. Ability to view the current Global Positioning System (GPS) location of a device or logical grouping of devices on a map (Optional)

#### FISMA or FedRAMP Requirements

The Mobile Device Management (MDM) solution shall be certifiable at a **Federal Information Security Management Act of 2002** (FISMA) Moderate Impact level (FIPS 199 Moderate or DoD 8500.2 MAC II) or higher. The response shall include either proof of certification, accreditation, or Authorization to Operate (ATO) in a federal environment, or a plan and timeline for achieving certification and/or ATO.

*[NOTE: insert FedRAMP requirements language]*

#### FIPS Requirements

The solution shall protect control and management data in transit between the Mobile Device Management (MDM) and the device using FIPS 140 certified cryptographic modules.

The offeror shall submit with their response proof of the solution’s FIPS 140-2 certification for cryptographic modules. All encrypted communications shall use a cryptographic module certified in accordance with a National Institute of Standard and Technology (NIST) Certified Cryptographic Module Validation Program under FIPS 140-2, level 1, certification. The offeror shall provide evidence of the solution’s NIST Certified Cryptographic Module Validation Program compliance, or that cryptographic operations in the solution rely on FIPS certified modules in the environment or operating system.

#### Containerization

If the proposed solution uses containers, offerors shall describe how the container meets the following requirements:

1. FIPS 140-2 encryption of data at rest
2. Remote and local (action-triggered) secure erasure of container data without impact the rest of the device
3. Protection of container from other applications; because of varying platform capabilities, this must be described on a platform-by-platform basis

Some solutions address data control through the use of containers on the mobile device that serve to separate enterprise and personal data, and protect data from access by uncontrolled applications. This is particularly helpful for BYOD scenarios, where the enterprise intends to limit interaction between agency and personal data. This approach is also used to protect data at rest if the underlying platform does not encrypt all data on the device.

#### IPv6 Support

On-premise portions of the Mobile Device Management (MDM) solution shall support IPv6 for network communications. Controls on network communications at the device shall apply to both IPv4 and IPv6 communications, including VPNs, logging/auditing and network black/white-listing. The offeror shall provide a description of the Internet Protocol (IP) based components of their solution and the status (compliant or non-compliant) of the proposed solution. If the proposed solution is not compliant at time of response submission, the offeror shall provide a Plan of Action and Milestones (PoAM) signed by a company official with an estimated timeline to achieve IPv6 compliance.

#### User Authentication

The proposed solution for the device shall support Personal Identification Number (PIN) or password authentication for the managed applications. The solution shall also be able to enforce a device PIN as provided in Task 2, Section C.4.2.3.1-7 Password Policy Enforcement.

The offeror shall include a web management portal as part of their proposed solution, and the web management portal shall be able to use Personal Identity Verification/Common Access Card (PIV/CAC) for primary authentication as indicated in HSPD-12 standards and guidance. Password fallback for specific accounts may be configurable; however they shall employ a second factor (token, SMS, voice response, etc.) to authenticate.

Offerors shall state how their proposed solution is capable of offering or supporting multi-factor authentication. Multifactor authentication involves authentication with any two of the following three authentication types:

* Shared Secret – Something the user knows, like a PIN or password
* Token – something a user possesses such as a cryptographic key, an RSA token (soft or hard), a challenge/response token, a PIV or CAC, Near Field Communication (NFC) Radio-Frequency Identification (RFID), or a key generator device like UbiKey
* Biometric – a sufficiently unique physical characteristic of the user, such as a fingerprint, iris or facial image

#### User Compliance

The offeror shall demonstrate the following capabilities. The proposed solutions shall enable the:

1. Ability to set up compliance rules to include custom compliance rules for profiles, devices, groups, and whitelist/blacklist
2. Ability to activate/deactivate a compliance rule
3. Ability to specify user and group rules for application compliance, such as required or prohibited applications on a device
4. Ability to provide enterprise level compliance reports, including lost/wiped/inactive devices, the number of devices total, the number of devices active, how much data is sent/received by devices, connection type
5. Support hierarchical policy enforcement as stipulated in Section C.4.2.2: Multi-tenancy

#### Alerting

The following alert capabilities shall be provided to notify agency operations staff via console display as well as appropriately via email and/or text message about devices under their management. The solution shall demonstrate the following capabilities:

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

#### Reporting

The solution shall provide the following capabilities:

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

The solution shall be able to produce the following types of reports.

#### Audit Reports

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

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

#### Privacy

The agency should define the PII requirements applicable to the agency from the guidance in this section.

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

The proposed solution shall safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)” and in accordance with M-06-16: Protection of Sensitive Agency Information [http://www.whitehouse.gov/sites/  
default/files/omb/memoranda/fy2006/m06-16.pdf](http://www.whitehouse.gov/sites/) and M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information [http://www.whitehouse.gov/  
sites/default/files/omb/memoranda/fy2007/m07-16.pdf](http://www.whitehouse.gov/sites/). An Ordering Activity will determine what data elements constitute PII according to Office of Management and Budget (OMB) Policy, NIST Guidance and Ordering Activity policy. An Ordering Activity may request that PII be kept within U.S. Data Centers.

The solution provider shall disclose privacy-impacting features that cannot be disabled.

#### Service Delivery Model

The Mobile Device Management (MDM) Solution shall be delivered by the offeror as a full solution including all hardware, software, hosting, and installation services, using one a [Select one: on premises, cloud, hybrid] model as follows:

The agency should decide which delivery model it wants before issuing the RFP. Choose one of the following paragraphs and delete the other two.

1. Cloud Based ‑ For the purposes of this request a Cloud Only solution is a solution that has all hardware/software components of the solution running in the a non-government hosted cloud data center. The offeror shall show how they provide all required hardware to the network edge of their cloud data center. The offeror is responsible for all aspects of system and software performance for solution components within their cloud data center.
2. On Premise ‑ For the purposes of this request an On-Premise solution is a solution that has all hardware/software components running completely within federal Government controlled data centers and network. After installation, the Federal Government will be responsible for operating the infrastructure and devices, application store and container management.
3. Hybrid ‑ For the purposes of this request a Hybrid solution is a solution where the components are distributed across federal Government data centers and the offeror’s cloud data center. It is anticipated that the offeror will provide all required hardware to the network edge of their cloud data center. The offeror will clearly describe all hardware/software components that will be within federal Government data center and those components within the offeror’s cloud data center. The offeror shall be responsible for all aspects of system and software performance for solution components within their cloud data center.

The Help Desks should be operationally located within the Continental United States (CONUS).

## Task 3 – Mobile Device Management

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

The offeror shall describe its compliance with the requirements in the table below.

| **MDM Requirements and  Offeror Capabilities and Experience** | **Required  or Optional** | **Section** | **Description** |
| --- | --- | --- | --- |
| 1. **General MDM Capabilities**. The offeror shall address/describe how their proposed solution meets all 10 of the mandatory general MDM requirements. | Required | 2.3.1 |  |
| 1. **Device Enrollment**. The proposed solution shall demonstrate the 20 capabilities identified regarding the ability to add a device to an MDM management domain. | Required | 2.3.2 |  |
| 1. **Device Profiles**. The offeror shall support the 21 items related to the creation of per-user and per-group device profiles. | Required | 2.3.3 |  |
| 1. **Device Feature Management**. The proposed solution shall demonstrate the 7 required features and capabilities identified regarding device feature management. | Required | 2.3.4 |  |
| 1. **Data Management**. The proposed solution shall demonstrate the ability to read, write transmit and receive data on mobile devices as well as with backend systems/repositories to include meeting FIPS 140 requirements. | Required | 2.3.5 |  |
| 1. **Data Collection** The proposed solution shall demonstrate the ability to collect and report on the 6 data points identified. | Required | 2.3.5.1 |  |
| 1. **Continuity of Operations and Disaster Recovery**. The proposed solution shall describe how it performs Continuity of Operations (COOP) and Disaster Recovery (DR). | Required | 2.3.5.2 |  |
| 1. **File Management**. The proposed solution shall demonstrate that it is able to hold a set of Commercial Off-the-Shelf (COTS) and/or enterprise applications with respective data/files in a FIPS 140 secured space (e.g., whole device encryption, container or **virtual desktop infrastructure** [VDI]) solution. It The proposed solution shall also demonstrate how it is able to share files between applications, between mobile devices, and/or between devices and hosted file servers based on application and security requirements. | Required | 2.3.5.3 |  |
| 1. **Personal Information Management**. The proposed solution shall demonstrate ability to provide/enable a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities, as well as be capable of synchronizing files and data between the devices and file servers by the use of a secure encrypted connection. | Required | 2.3.5.4 |  |
| 1. **Security Content Automation Protocol (SCAP) Support**. The proposed solution shall demonstrate the ability to support server-side components, including asset management, configuration management, patch management, and remediation capabilities. | Required | 2.3.6 |  |
| 1. **Device Inventory Management**. The proposed solution shall demonstrate the ability to include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information? Does it record, track and manage the 16 pieces of information identified in inventory management. | Required | 2.3.7 |  |
| 1. **Device Inventory Reports**. The proposed solution shall demonstrate the ability use the identified filters to run or export device inventory reports associated with the device, OS, and applications. | Required | 2.3.8 |  |
| 1. **System Performance Reports**. The proposed solution shall demonstrate the ability to run system performance reports using the identified filters. | Required | 2.3.9 |  |
| 1. **MDM Security/Compliance Reports** The proposed solution shall demonstrate the ability to run MDM security/compliance reports using the identified filters. | Required | 2.3.10 |  |
| 1. **Classified Data**. The offeror shall describe the ability of the proposed solution to access classified data up to the SECRET level via a mobile device. | Optional | 2.3.11 |  |
| 1. **PIV/CAC Support**. The offeror shall describe how the proposed solution is capable of supporting the use of PIV/CAC cards to support digital signatures, encryption, or access to enterprise resources. | Optional | 2.3.12 |  |
| 1. **Biometric Support**. The offeror shall demonstrate the ability for the proposed solution to offer biometric support such as fingerprint or face recognition. | Optional | 2.3.13 |  |
| 1. Network Monitoring. The offeror shall demonstrate the basic diagnostic functions related to monitoring device network quality and performance. | Optional | 2.3.14 |  |

### Mobile Device Management (MDM) General Requirements

The offeror shall describe how the proposed solution meets the following general requirements:

1. Ability to enforce enterprise rules while allowing Agency/Bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities
2. Ability to take the following action upon a group of devices from a search: reassign to group (any type of logical grouping) ‑ user or device groupings are an example
3. Ability to assign profile to one or many groups (any type of logical grouping) ‑ user or device groupings are an example
4. Ability to view required applications from the Mobile Application Store (MAS)
5. Ability to view and run reports on user and device information for all Smartphones
6. Ability to run reports by groups of users to include location
7. Ability for the solution to support a Software Development Kit (SDK) or Application Programming Interface (API) Framework to integrate with existing or future Enterprise Applications
8. Ability for the MDM solution to be able to be monitored from industry standard tools (e.g., HP OpenView, SCOM, etc.)
9. Ability for the MDM solution to integrate certificates from the solution’s internal PKI system to mobile devices as well as third party public PKI providers such as VeriSign; PKI shall support HSPD-12 and associated NIST standards
10. Ability for the MDM to perform its functions from within a secure VPN (FIPS 140) used to transport all enterprise data (i.e., no MDM control data transported unencrypted across the open internet)

### Device Enrollment

Enrollment adds a device to the Mobile Device Management (MDM) domain. The offeror shall demonstrate that the proposed solution meets the following required capabilities:

1. Ability to set a Target Platform (Apple, Android, etc.) for profile provisioning
2. Ability for Target Device Model to be used for profile provisioning
3. Ability to specify minimum OS version for profile provisioning
4. Ability for Target Device Ownership (GFE, Personal etc.) to be used for profile provisioning
5. Ability to edit any field for a "live" or "active" profile
6. Ability for a user with appropriate authorization to self-enroll an agency or BYOD device
7. Ability to centrally manage multiple devices for a single user (user device view)
8. Ability to have different policies or grouping for multiple devices under one user (i.e., tablet policy, phone policy)
9. Ability to apply multiple policies to devices simultaneously (user is member of group policy X, with device policy Y) – when multiple controls conflict, the most restrictive control takes precedence
10. Ability to use external directory service repository for enrollment
11. Ability for system to require users have read policy and signed agreement for enrollment
12. Ability to set support email and phone information for registration messages
13. Ability to set a URL to redirect user to upon successful enrollment
14. Ability to edit an enrollment activation notification message to the user (email and/or SMS)
15. Ability to set a default Device Ownership type upon enrollment for different groups
16. Ability to use internal user list for enrollment for different groups
17. Ability to set support email and phone information for registration messages for different groups
18. Ability to edit an enrollment activation notification message to the user or group of users (email and/or SMS)
19. Ability to send a user or group an activation enrollment message (email or SMS)
20. Ability to support over-the-air provisioning and hierarchies

### Device Profiles

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

The solution shall demonstrate the following profile capabilities:

1. Ability to create a profile template
2. Ability to copy profiles
3. Ability to edit a "live" or "active" profile
4. Ability to set Profile Removal Permission (who can remove a profile from a device or user)
5. Ability to set Profile Start Date (when the profile starts applying to associated devices)
6. Ability to set Profile End Date (when the profile stops applying to associated devices)
7. Ability for an edited profile to automatically update devices that currently have the profile
8. Ability to push a profile to any individual device
9. Ability to automatically remove profiles from devices whose state changes from qualifying to not qualifying; this may happen as a result of changing a profile to be more exclusive
10. Ability to support multiple profiles being applied to a single device (most restrictive rules apply)
11. Ability to delete a profile from the MDM system
12. Ability to set a description for a profile
13. Ability to manage the following via a profile
    1. Allow installing applications
    2. Control use of camera or other sensors and recording devices
    3. Control use of installed applications, including default applications
14. Allow multiple Wi-Fi configurations for multiple profile's
15. Ability to manage device Wi-Fi settings via a policy via a MDM policy
16. For a profile: Control Wi-Fi Security Type: None, WEP, WPA/WPA2, Enterprise (any)
17. For a profile: Ability to support multiple VPN configurations for a profile.
18. For a profile: Support VPN Connection (or Policy) Type: IPSec (Cisco), Juniper SSL, FS SSL, and Custom SSL, etc.
19. For a profile: Ability to support a VPN connection Proxy for a VPN configuration
20. Ability to support multiple email/calendar/contact configurations per profile
21. Allow multiple Web Clip/Web Shortcut configurations per profile
22. Ability to support hierarchies

### Device Feature Management

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

1. Multi-OS Support – Manage multiple operating system devices such as RIM’s BlackBerry, Apple’s iOS, Google’s Android, Microsoft’s Windows Phone, etc.
2. Device passcode enforcement (complexity, length, presence) in compliance with Section C.4.2.3.1-7 Password Management
3. Installation of applications (See MAM)
4. Camera (enable/disable)
5. Control all radios/communications:
   1. Wi-Fi (enable/disable)
   2. Bluetooth (enable/disable)
   3. NFC (enable/disable)
6. Ability to enable or disable specific hardware component and uses: Enable blue tooth headphone, disable Bluetooth keyboard
7. GPS (enable/disable)
8. Store enterprise data to removable media (disable)
9. Roaming (enable/disable) – (Optional)
10. Microphone (enable/disable) – (Optional)
11. Geofencing for device features; enable or disable features based on device location – (Optional)
12. Geomasking ‑ Geomasking for applications; enable or disable location data based upon policy and state – (Optional)

### Data Management

Data Management is the ability to read, write, transmit and receive data on mobile devices as well as with backend systems/repositories to include FIPS 140 requirements.

#### Data Collection

The solution shall be able to collect and report on the following data:

1. Roaming status
2. Last policy update time
3. Last synchronization time
4. Jailbreak/root status
5. Available program memory
6. Available storage memory

#### Continuity of Operations and Disaster Recovery

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

#### File Management

The Government seeks solutions that have the capability to secure data, files, and applications (for example pdf files or word docs) on a mobile device. Devices may be GFE or BYOD. The offeror shall demonstrate that the solution is able to hold a set of Commercial Off-the-Shelf (COTS) and/or enterprise applications with respective data/files in a FIPS 140 secured space (e.g., whole device encryption, container or VDI) solution, whether that is within a secured container or secured within the device OS. The offeror shall also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and file servers based on application and security requirements.

#### Personal Information Management

The offeror shall demonstrate the solution’s ability to support a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities. To ensure that the information is available to other mobile and desktop devices the user may have, as well as for business continuity, backup/restore, and e-discovery purposes, solution providers must be able integrate functionality with a variety of email, calendaring and contact applications, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection. The offeror shall also demonstrate the solution’s PIM capability to support multiple types of Federal Enterprise Email Systems from different vendors. Please identify which on premise and cloud-based mail systems are supported, such as Microsoft Exchange, Lotus Notes, Gmail, MS 360, Lotus Domino, MS Exchange or Zimbra.

#### Security Content Automation Protocol Support

Security Content Automation Protocol (SCAP) provides the ability to automate security checks and configuration. Offerors shall describe the SCAP support for the server-side components in their solution, including asset management, configuration management, patch management and remediation capabilities.

The request is only considering server SCAP support at this time. SCAP for devices is not currently a requirement.

### Device Inventory Management

The solution shall include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information. At a minimum the solution shall be able to record, track and manage the following information:

1. Device Manufacturer/Model
2. GFE or personal (BYOD) device
3. Carrier
4. Wireless Number
5. MAC Addresses
6. International Mobile Equipment Identity (IMEI)
7. SIM module data
8. Storage capacity
9. OS and Version
10. Device up time
11. Encryption Capability
12. User Name
13. Email
14. Phone number
15. Agency information
16. Supervisor contact information

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

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

### Device Inventory Reports

The solution shall demonstrate the capability to run inventory reports. Device Inventory reports includes all data associated with the device, OS and applications. Device reports shall be run and/or exported as needed, and shall support the following filters:

1. Device Models
2. Operation System and build level
3. Last Access times (access time not compliance check)
4. Application inventory
5. Last Compliance Check
6. Device Compliance (ability to report on rooted/jail broken devices, policy, etc.)
7. Carrier
8. Network Card IDs (MAC address)
9. Agency Assignment
10. BYOD or GFE (personal device or government furnished)
11. Security Policy Assignment (policy currently applied to device)

### System Performance Reports

The solution shall demonstrate the capability to run system performance reports. System performance reports include key performance data to provide insight into the usage of the devices, reliability of the solution, and performance of devices. System performance reports will be run as needed and shall support the following filters:

1. Concurrent Connections
2. Peak Time Usage
3. Total active user and device counts
4. Bandwidth utilization trends
5. End-to-End testing results
6. Authentication processing times
7. Email/calendar/contact sync durations
8. Connection failure rate to/from device for the MDM system

#### Mobile Device Management Security/Compliance Reports

The solution shall demonstrate the capability to run security/compliance reports. Security reports include all data relevant to the monitoring and support of the system’s vulnerabilities and defenses, including attempts at fraud. Security status reports will be run as needed and shall support the following data:

1. Non-compliant devices
2. Device wipe actions
3. Passcode reset actions
4. User/devices with failed authentication
5. Aggregate data on failed authentications
6. Devices with blacklisted applications
7. Jail broken devices
8. Device anti-virus versions
9. Mobile management agent

### Classified Data (Optional)

Some Managed Mobility users may require the ability to access classified data up to the SECRET level via mobile devices. If your solution supports these capabilities, please describe how this is accomplished and indicate the specific impact to pricing for this solution, inclusive of exact dollar amounts.

### Personal Identity Verification/Common Access Card Support (Optional)

Offerors may optionally offer solutions that support the use of PIV/CAC cards or PIV-derived credentials per associated NIST standards to support digital signatures, encryption, or access to enterprise resources.

### Biometric Support (Optional)

Agencies with strong authentication requirements may need biometric support per associated NIST standards such as fingerprint or face recognition with their mobile devices. The ability for the Mobile Device Management (MDM) to manage this capability may be combined with PIV/CAC support.

### Network Monitoring (Optional)

Network Monitoring is the monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by enterprise devices).

The solution may include a device application that performs basic diagnostics, such as:

1. Verify network connection and performance
2. Test authentication settings
3. Verify certificates
4. Verify Domain Name System (DNS) functionality
5. Verify connection to services (mail, MDM, etc.)

## Task 4 – Provide Mobile Application Management

Mobile application management (MAM) is a type of security management related to the use of specific mobile applications. In general, MAM provides security for the types of software products installed on smartphones, tablets and mobile devices.

The offeror shall describe its compliance with the requirements in the table below.

| **MAM Requirements and  Offeror Capabilities/Experience** | **Required or Optional** | **Section** | **Description** |
| --- | --- | --- | --- |
| 1. **Application Deployment.** The proposed solution shall demonstrate the ability to support the 6 controls and capabilities identified for application deployment. | Required | 2.4.1 |  |
| 1. **Mobile Application Store**. The proposed solution shall include MAS that allows users to select private enterprise applications for installation on managed devices, integrated into the Managed Mobility MDM portal, which allows application provisioning by group policy and mandatory application deployment. | Required | 2.4.2 |  |
| 1. **Mutual Authentication**. The proposed solution shall demonstrate the ability for applications to mutually authenticate to ensure the communications channel is not intercepted. | Required | 2.4.3.1 |  |
| 1. **Application Installation Control**. The proposed solution shall demonstrate the solution’s process to support relevant authorizations and approvals (including change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance, including the ability to monitor application usage. | Required | 2.4.3.2 |  |
| 1. **Blacklisting/Whitelisting**. The proposed solution shall demonstrate the capability, managed through user and group policies, to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting). | Required | 2.4.3.3 |  |
| 1. **Application Environment Requirements**. The proposed solution shall demonstrate the capability to detect and enforce device environment conditions such as those listed. | Required | 2.4.3.4 |  |
| 1. **Application Signing**. The proposed solution shall support requiring digital signatures for application installation. | Optional | 2.4.3.5 |  |
| 1. **Third-Party Application mutual Authentication**. The proposed solution shall offer the ability to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc. | Optional | 2.4.4 |  |

### Application Deployment

The solution shall support the following controls and capabilities for application deployment:

1. Commercial Application Store (iOS App Store, Google Play, etc.) (enable/disable)
2. Reporting of installed applications
3. Blocking application purchase
4. Application whitelisting/blacklisting
5. Staged/controlled application deployment (limit deployment by policy, group, location, etc. to facilitate gradual deployment of new or updated applications)
6. Authentication of users accessing the MAS either directly using User Authentication per Section C.4.2.3.6, or via MDM utilizing approved PKI alternative authentication methodologies such as Kerberos Constrained Delegation if MAS is not integrated into MDM.

### Mobile Application Store (MAS)

The solution shall include MAS to allow users to select private enterprise applications for installation on managed devices. This capability shall be integrated into the Managed Mobility Mobile Device Management (MDM) portal, and allow application provisioning by group policy, and mandatory application deployment.

The MAS shall support the following capabilities:

1. Ability to add an application from a Commercial Application Store to the MAS
2. Ability to add an enterprise application to the MAS via a web GUI
3. Ability to add additional metadata to and report on metadata on any application added to the MAS (etc. name, description, version, OS, keywords, etc.)
4. Ability to specify the effective date for an internal application
5. Ability to specify the expiration date for an internal application
6. Ability to specify the minimum operating system and model for an internal application
7. Ability to download internal and public applications from MAS
8. Ability to categorize, group or tag applications (e.g., business applications, scientific applications, etc.)

### Application Security

#### Mutual Authentication

Mobile Device Management (MDM) applications on the device and services shall mutually authenticate to ensure the communications channel is not intercepted. The mutual authentication shall be certificate-based, with installation-specific certificates deployed to the server during deployment and to the device during provisioning.

#### Application Installation Control

The offeror shall demonstrate the solution’s process to support relevant authorizations and approvals (include change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance. This includes the ability to monitor application usage.

#### Blacklisting/Whitelisting

The solution shall provide the capability to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting). This capability should be managed through user and group policies.

#### Application Environment Requirements

The solution shall be able to detect and enforce device environment conditions or enact required policy enforcement rules if device environment conditions cannot be enforced. Examples include:

1. Minimum or specific operating system versions
2. Required presence or absence of other applications
3. Absence of privilege escalation (“rooting” or “jail breaking”)

#### Application Signing

The solution shall support requiring digital signatures for application installation, from both commercial and private application stores and direct application push/deployment. It is permissible to meet this requirement through OS capabilities.

### Third-Party Application Mutual Authentication (Optional)

The Mobile Device Management (MDM) solution shall offer the ability to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.

# Labor Types

The offeror shall provide Labor Types for both professional and technical expertise that fully meet the requirements of all tasks in support of the solutions specified in this SOW, including full life cycle management as applicable, and the analysis, planning, design, specification, implementation, integration and management of required services and equipment.

The offeror shall provide:

* Installation support to Government-site(s), as identified in *Attachment B – Support Locations*.
* Proposed Labor Types for each Task as specified in *Attachment D – Pricing Template.*

## Personnel Requirements

The offeror has ultimate responsibility for managing the order, for achieving the expected performance results, and for determining the appropriate staffing in support of its technical approach.

* The offeror shall provide experienced personnel to perform the required services. The Government and the offeror understand and agree that the services to be delivered are non-personal.
* Offeror personnel shall conform to standards of conduct and code of ethics, which are consistent with those applicable to Government employees. Offeror personnel shall obtain authorization to have access to Agency support sites and Government facilities, and shall obtain CACs for computer access, if required.
* All offeror employees shall be fluent in spoken and written English [optional].
* Background Checks [As required]: All [Project Name] offeror employees shall submit a Questionnaire for National Security Positions (Standard Form 86 (SF86)) to the [Agency] Personnel Security Manager. A favorable SF-86 is required before gaining access to a U.S. Government Local Area Network (LAN), if required. The offeror, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the order [As required].
* The Contracting Officer may require the offeror to remove from the job site any offeror employee who is identified as a potential threat to the health, safety, security, general well-being or operational mission of the installation and its population.
* In order to ensure a smooth and orderly startup of work, the key personnel specified in the offeror's proposal shall be available on the effective date of the order. If these personnel are not made available at that time, the offeror shall notify the contracting officer and show cause. If the offeror does not show cause, the offeror may be subject to default action.
* The offeror-supplied personnel are employees of the offeror and under the administrative control and supervision of the offeror. The offeror, through its personnel, shall perform the tasks prescribed herein. The offeror shall select, supervise, and exercise control and direction over its employees (including offeror subcontractors) under this order. The Government shall not exercise any supervision or control over the offeror in its performance of contractual services under this order. The offeror shall be accountable to the Government for the action of its personnel.

## Proposed Personnel

The offeror shall assemble a [Project Name] project team with the required knowledge and experience to perform the work described under this task order, and if applicable, any additional qualifications described in *Section 3.3 ‑ Special Qualifications and Certifications*.

The core project team shall be composed of qualified professionals with strong technical backgrounds. The Offeror shall propose appropriate Connections II Labor Type(s) and personnel experience levels (a mix of senior, mid, and entry levels) that meet the minimum required qualifications, based on the complexity and scale of the Agency’s specific [Project Name] tasking. [If additional labor types are necessary, the offeror may request a modification to add them to the contract.]

The offeror shall ensure that its employees have all required professional certifications and licenses (current and valid) for each applicable task and labor type category before commencement of work.

The offeror shall identify, by name, the proposed Key Personnel (e.g., the key management and technical personnel who will work under this order, such as the PM).

The proposed [Project Name] project team structure and an organizational chart shall be included in the proposal, with the names, positions and resumes of any proposed key personnel.

## Special Qualifications and Certifications

Insert in this section any additional special qualifications, certifications, license requirements, etc. that pertain to this particular task. For example, if it is a very large and complex job, a highly qualified PM with Project Management Professional (PMP) credentials might be requested.

The PM should possess the intellectual and leadership qualities necessary to plan, manage, develop, articulate and carry out to completion the [Project Name] project. [If required, the proposed PM shall have a PMP certification, and shall have experience developing a PMP for large, complex projects similar to [Project Name].]

# Travel and Other Direct Costs (ODC/Un-priced Items)

## Travel

The offeror shall comply with the Travel and Per Diem requirements as described in Section G.5.1.2 of the Connections II contract including conditions and limitations applying to travel associated with work performed under this SOW.

### Local Travel

If travel within the local vicinity is required, travel reimbursements for local travel are not authorized; neither is the use of a Government vehicle.

### Distance Travel

If travel outside the local vicinity is required, costs incurred by offeror personnel for travel, including costs of lodging, other subsistence, and incidental expenses, shall be considered reasonable and allowable only to the extent that they do not exceed the rates and amounts set by the Federal Travel Regulations. See FAR 31.205-46(a)(2)(i).

As part of the Price Proposal, the offeror shall provide any anticipated travel costs, to include origination, destination, and the number of trips, number of persons, and a breakdown of lodging, meals, transportation and related costs.

Prior written approval by the [Agency] Contracting Officer is required for all travel directly and identifiably funded by the [Agency] under this order. The offeror shall therefore present to the Contracting Officer an itinerary for each planned trip, showing the name of the traveler, purpose of the trip, origin/destination (and intervening stops), and dates of travel, as far in advance of the proposed travel as possible, but in no event less than three weeks before travel is planned to commence.

For cost effectiveness, economy class travel must be used on all official travel funded under this Task Order. Business class travel shall only be used under exceptional circumstances, and in compliance with the Federal Travel Regulations (FAR 31.205-46).

## Other Direct Cost (ODC/Un-priced Items)

For other direct costs proposed (e.g. travel, per diem, etc.), which are considered necessary for the completion of the work, the offeror shall provide sufficient information to establish the basis for the estimate of such cost.

The Offeror shall provide a breakdown for un-priced items and/or Other Direct Costs (ODCs) in the Price Proposal. The breakdown shall identify any “open market” items.

# Invoice Requirements

The offeror shall meet and comply with the Billing and Invoice requirements as described in **Sections C.3.4 Billing, G.5.1 General Billing Requirements, and G.6 Payment of Bills** of the Connections II contract. The baseline requirements for Connections II contract for Invoicing and Billing including the handling of the Associated Government Fee, approval for payment of supplies/services, resolution of billing disputes, and the option for Agency to pay by electronic funds transfer shall apply.

## Detailed Billing Requirements

The offeror shall comply with the detailed billing requirements defined in **Section C.3.4** and the general billing requirements in **Section G.5** of the Connections II contract when submitting a proper bill for each order.

## Invoice Address, Data Format and Delivery Method

The offeror shall be capable of directly billing each customer at the address given by the Agency in the order and shall also have the capability to centrally bill designated customers through GSA. The baseline requirements for direct and centralized billing as defined **Section C.3.4** of the Connections II contract shall apply.

### Invoice Address

The Offeror shall send invoices directly to the address (electronic mail or postal/physical address) designated by the Agency’s authorized Ordering Entity. This address will be determined at the time the order is placed.

|  |
| --- |
| **Remove this context box when finalizing the SOW**  Agency has two options for how to receive invoices whether by electronic (email method) or to require hard copies. Or both. Suggested Requirements:  The offeror shall provide the signed original invoice via email:  [Agency provide an email here]  The offeror shall also provide via postal/physical address an additional copy of the invoice to the Contracting Officer and COR or provide [n] copies of the signed original to:  Name of Agency Department  POC Name/Position and Title  Email  Mailing Address  Street, City, Zip  Inquiries regarding payment of invoices should be directed to [Agency provide an email here] |

### Invoice Submission

The offeror shall comply with the detail billing requirements defined in Section C.3.4 and the general billing requirements in Section G.5 of the Connections II contract when submitting a proper bill for each order.

A proper invoice must include the following items:

1. Contractor name and address
2. Contractor representative
3. Contract number
4. Order number(s)
5. Accounting Control Transaction (ACT) number (assigned by the OCO on the order)
6. Period of performance (month services performed for work request orders, month
7. Deliverable completed for fixed price orders)
8. Bill number
9. Customer’s name and address
10. For Fixed Price Orders, products delivered and accepted, listed by deliverable number;
11. For Time and Materials orders, labor charges accepted during the period of performance
12. Travel and per diem charges
13. Total billed amount
14. Prompt payment discount offered (if applicable)

### Billing Cycle and Data Elements

The offeror shall invoice on a monthly basis. The invoice shall include the period of performance covered by the invoice. The labor categories with total labor hours incurred for the period and other direct costs shall be reported on the invoice and shall be calculated for the current billing month. A Year-to-date total from project inception to date shall also be provided. If subcontracting is proposed, one consolidated invoice from the prime contractor shall be submitted in accordance with other terms and conditions of the RFQ.

| **Remove this context box when finalizing the SOW**  Agency has option to specify the format and agency-specific data elements for invoice content.  Suggested Requirements:  The offeror shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date. The following data elements shall be provided on the Invoice, at a minimum:   1. Labor Type (Contractor Employee) 2. CONNECTIONS II labor category 3. Monthly and total cumulative hours worked 4. Burdened hourly labor rate 5. Cost incurred not billed |
| --- |

### Electronic Funds Transfer (EFT)

| **Remove this context box when finalizing the SOW**  Agency has option to specify the method of delivery for invoice and payments.  Insert additional agency-specific requirements here.  Below is a standard ‘boilerplate” requirements for EFT. |
| --- |

The offeror shall cooperate with the Government to allow payment of bills via Electronic Funds Transfer (EFT) to the extent feasible in accordance with **Section G.6.3 Use of Electronic Funds Transfer** of the Connections II contract.

## Billing for Other Direct Costs (ODCs) or Unpriced Item

The offeror may invoice monthly on the basis of cost incurred for ODC or unpriced item.  The invoice shall include the period of performance covered by the invoice and the item number and title.

| **Remove this context box when finalizing the SOW**  Agency has option to specify the format and agency-specific data elements for ODC and unpriced items.  Suggested Requirements:  The offeror shall provide the following detailed information for each invoice submitted, as applicable.  Spreadsheet submissions, in MS Excel format, are required.   1. ODCs or unpriced items purchased 2. Date delivery accepted by the Government 3. ODC or unpriced item number 4. Project to date totals 5. Cost incurred not billed 6. Remaining balance of each item |
| --- |

### Invoice for Travel Expenses

The offeror may invoice monthly on the basis of cost incurred for cost of travel comparable with the Joint Travel Regulations/Federal Travel Regulation (JTR/FTR).  Long distance travel is defined as travel over 50 miles.  The invoice shall include the period of performance covered by the invoice, and the CLIN number and title.  Separate worksheets, in MS Excel format, shall be submitted for travel.

| **Remove this context box when finalizing the SOW**  Agency has option to specify the format and agency-specific data elements for submitting Travel charges. Suggested Requirements:  The offeror shall provide the following detailed information for each invoice submitted for travel expenses. The Total Cost for Travel shall identify all current travel on the project and their total CLIN/Task costs billed.  The listing shall include separate columns and totals for the current invoice period and the project to date:   1. Travel Authorization Request identifier, approver name, and approval date 2. Current invoice period 3. Names of persons traveling 4. Number of travel days 5. Dates of travel 6. Number of days per diem charged 7. Per diem rate used 8. Total per diem charged 9. Transportation costs (rental car, air fare, etc.) 10. Total charges 11. Explanation of variances exceeding 10% of the approved versus actual costs 12. Indirect Handling Rate. |
| --- |

[Agency may add Agency-specific billing and invoice payment processing requirements here]

# Section 508

All Electronic and Information Technology (EIT) procured through this task order must meet the applicable accessibility standards at 36 CFR 1194, unless an Agency exception to this requirement exists. The **Section 508 Standards Summary** is viewable at: <https://www.section508.gov/index.cfm?fuseAction=stdsSum#technical>

The offeror shall indicate for each line item in the schedule whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the proposal must indicate where full details of compliance can be found (e.g., the offeror's website or other exact location).

# Proposal Instruction to Offerors

This section provides instructions to prospective offerors on preparing and submitting a proposal in response to this solicitation.

**SOLICITATION CLOSING DATE AND TIME: ALL OFFERS MUST BE RECEIVED ON OR BEFORE 3:00 PM EDT ON:**  [DD MM YYYY].

**REQUIRED SUBMISSIONS:**

Proposal shall be submitted to the attention of: [Agency Point of Contact]

**HARD COPY ADDRESS:** **ELECTRONIC COPY:**

Agency Name and Email Address

POC Name

Mailing Address

Telephone

Email

No offer received after the due date and time will be considered.

## General Instructions

### Materials Submitted

The Offeror is advised that all submissions and related material become the property of the U.S. Government and will not be returned. The technical and price proposals, if accepted by the Government, will form binding parts of the task order that results from this solicitation. Therefore, care must be taken to properly address the requirements set forth in each of the tasks. In the event of any conflict between the Connections II contract and the proposal in any resulting task order, the Connections II Contract shall govern.

### Format

[If the Agency wishes to use electronic format only, it may delete references to hard copy submittal in the sample text below.]

All materials shall be in typeface Times New Roman or Arial (no smaller than 11 point), double-spaced on 8½” x 11” white paper with one inch margins all around. Tables and illustrations may use a reduced font style, but not less than 8 point, and may be single-spaced. Each page must identify the submitting Offeror in the header or footer.

The offeror’s proposal shall consist of physically separate volumes that are individually titled and numbered on the exterior of the top covers as stated in Table 2 below. **DO NOT INCLUDE PRICING IN THE TECHNICAL AND PAST PERFORMANCE VOLUMES:** THE OFFEROR IS ADVISED THAT COMBINING TECHNICAL AND PRICING VOLUMES IN THE OFFEROR’S PROPOSAL IS NOT RESPONSIVE TO THE SOW.

Table 2. Number of each Type of Proposal Volume

| **Volume** | **Volume Title** | **Copies** | **Format** | **Page Limitations** |
| --- | --- | --- | --- | --- |
| Volume I | Technical Proposal  Technical Approach  Management Approach | 1 Hard Original +  [n] Hard Copies + 1 Electronic Copy | PDF | [n] pages maximum not including Executive Summary (2 pages max) |
| Volume II | Price Proposal | 1 Hard Original  1 Electronic Copy | EXCEL – Pricing Template | No page limit |
| Volume III | Appendices  Past Performance  Resumes of Key Personnel  PMP [if required] | 1 Hard Original +  1 Electronic Copy | PDF  PDF  PDF | [n] pages  [n] pages maximum per Resume  No page limit |

### Proprietary Data

Each page of the offeror’s proposals shall be reviewed and marked as to proprietary data content by the offeror in strict compliance with FAR 52.215-1. Also see FAR 3.104-4. A single blanket statement at the front of the proposal is not acceptable. Failure to mark every page will subject the proposal to public release through Freedom of Information Act (FOIA) requests.

## Preparation of Technical Proposal

The Technical Proposal in response to this solicitation shall address how the offeror intends to carry out the SOW requirements contained in *Section 2*. The offeror’s Technical Proposal must demonstrate a clear understanding of the requirements, the adequacy of the solution approach in meeting the goals and objectives of the [Project Name] project, and fulfill the offeror’s implementation responsibilities.

Technical Proposals are limited to [n] pages in length and shall be written in English. Each page must be numbered consecutively. Pages that exceed the page number limitation will not be evaluated.

Any page in the Technical Proposal that contains a table, chart, graph, etc., not otherwise specifically excluded below, is included within the above page limitation for the Technical Proposal. All critical information from appendices shall be identified and summarized in the Technical Proposal. Not included in the page limitation are the following:

* Cover/Title Page
* Table of Contents
* Executive Summary (2 pages maximum)
* Dividers
* Table summarizing qualifications of proposed personnel

The Technical Proposal will consist of the following information:

* Technical Approach
  + Task 1
  + Task 2
  + Task [n]
* Management Approach
  + Overall management approach summary
  + Project Management Plan [if required]
* Proposed Personnel Qualifications and Certifications
  + Resumes of Key Personnel
* Past Performance
  + Past Performance Worksheet

The Technical Proposal shall include a detailed description of the offeror’s technical solution for each task in Section 2, including the associated equipment, equipment services, labor, and installation. At a minimum, the offeror shall organize its response in the Technical Proposal to contain the following information.

### Executive Summary

This section summarizes the key elements of the offeror’s strategy, approach, methodologies, personnel and implementation plan. The Executive Summary will not count towards the [n] page limitation and shall not exceed 2 pages in length.

### Technical Approach

The offeror’s Technical Approach shall demonstrate a clear understanding of the requirements. The Technical Approach shall include a description of the overall approach and the specific strategy (i.e., implementation plan, testing methodology and risk mitigation strategy) being proposed to complete this task order. The Technical Approach shall be specific and complete, presenting concisely how the offeror will fulfill the task requirements described in *Section 2*. Marketing literature is not acceptable.

### Management Approach

The detail requested from the offeror supporting its management approach should be relative to the size and complexity of the overall task. For simple and straightforward jobs, for example, the plan may simply be a high-level completion schedule.

[The offeror shall submit a management approach summary that includes the offeror’s approach to meeting the requirements of the SOW. This shall include a high-level completion schedule describing all key activities and associated completion dates.]

[The offeror shall submit a draft PMP based on the offeror’s proposed technical approach using *Attachment A ‑ PMP Template*. The offeror’s PMP will be evaluated as part of the offeror’s management approach. The PMP shall be submitted as an appendix in Volume III with no size limit if required.]

### Proposed Personnel Qualifications and Certifications

The offeror shall describe the skills, qualities and capacities of its proposed Project Manager and other key personnel to meet both the minimal qualifications described in *Section 2* as well as their ability to meet the task order implementation and schedule challenges.

The offeror shall include in an appendix in Volume III the resumes for all the proposed key personnel candidates, up to a total number of [n]. Key personnel resumes may not exceed [2] pages in length and shall be in chronological order starting with most recent experience.

Each key personnel resume shall be accompanied by a signed letter of commitment from each candidate indicating his/her: (a) availability to work in the stated position, in terms of months; after award; and (b) intention to support and work for a stated term of the service. [Optional: The offeror's proposed key personnel shall also submit a minimum of three (3) references of professional contacts within the last three years. The offeror should provide a current phone, fax address, and email address for each reference contact.]

### Past Performance

The offeror shall use the past performance template provided in *Attachment F – Past Performance* Worksheet. The offeror shall provide [n] past performance references for projects of a similar type, size and scope to that described in the solicitation, and submit them as an appendix in Volume III.

When providing past performance, the references provided shall include solution installations that are similar to the solution being offered within this Request for Proposal (RFP)/SOW.

If other partner solutions are being used to fulfill the requirement identified in the RFP/SOW, describe how the solution has been tested and sold to other government agencies. Also explain if the solution is working at full capacity today.

Offerors shall submit the following information as part of their proposal:

* The offeror shall describe its past performance directly related to contracts it has held within the last 5 years that are similar in scope, magnitude and complexity. Offerors shall provide a minimum of three (3) relevant examples of mobility management projects the offeror has completed.
* Offerors shall provide relevant past performance documentation and references for services comparable to those described in the SOW. Past performances listed may include those entered into by the Federal Government, state and local government agencies, and commercial customers. Offerors should notify each of their private-sector (commercial) references that they may be contacted by the [Agency] and authorize them to provide the past performance information requested. References other than those identified by the offeror may also be contacted by the Government, and the information received from them may be used in the evaluation of the offeror’s past performance.

The offeror shall provide with the proposal a summary of the required past performance information as shown in *Appendix F ‑ Past Performance Worksheet*.

## Preparation of Price Proposal

Below is suggested text. Please modify or delete text as needed.

The offeror shall submit their Price Proposal in the form of a Microsoft Excel Workbook, which is included as *Attachment D – Pricing Template.*  The Pricing Template is used to facilitate the delivery of prices in the required format. In populating all Excel worksheets, the offeror shall present the data (e.g., item number, unit prices, quantities, and summarized prices) in a manner where all computations can be traced to the maximum extent possible. The offeror may add rows, columns, or worksheets to accommodate the required pricing information.  See also: *Attachment C – Pricing Requirements.*

[Failure by the offeror to use the prescribed pricing template may result in non-compliance.] The Price Proposal (Volume II) must be submitted under separate cover from the Technical Proposal (Volumes I and III). There is no page limit for the Price Proposal. The offeror must provide sufficient detail and supporting information to allow a complete analysis of each line item price.

# Evaluation Factors and Basis for Award

The Government will evaluateeach of the offeror’s proposals to determine if the support services offerings satisfy the specific requirements under each task. The evaluations will be based on the evaluation factors defined in this section.

## Evaluation Methodology and Basis for Award

Suggested General Evaluation Language   
(Agency may remove or modify the text below)

The Government may award a contract based on the initial proposal without discussions or negotiations with offerors, in accordance with FAR 52.215-1. Therefore, it is important that each proposal be fully compliant, without exception to any requirement, clause or provision. Offerors should submit initial proposals which respond most favorably to the SOW’s requirements.

The Government intends to evaluate offeror’s proposals in accordance with Section 7 of this SOW and make a contract award to the responsible offeror whose proposal represents the best value to the U.S. Government.

The Technical Proposal will be evaluated by a technical evaluation committee using the technical criteria shown below.

Price has not been assigned a numerical weight. Offerors are reminded that the Government is not obligated to award a negotiated contract on the basis of lowest proposed price, or to the offeror with the highest technical evaluation score. Agencies must state the following when

using tradeoff process: ‘The solicitation shall state whether all evaluation factors other than cost or price, when combined, are significantly more important than, approximately equal to, or significantly less important than cost or price.’

As technical scores converge, price may become a deciding factor in the award. Therefore, after the final evaluation of proposals, the contracting officer will make the award to the offeror whose proposal offers the best value to the Government considering both technical and price factors.

## Evaluation Approach – Trade Off or Lowest Price Technically Acceptable

Note: The Agency is required to select the evaluation approach (i.e., Trade Off or Lowest Price Technically Acceptable (LPTA) Approach. Once a method has been selected, delete all information in this SOW relevant to the method that was NOT selected.

Suggested Evaluation Language if Trade-Off Approach is Selected by the Agency   
(Agency may remove or modify the text below)

The Government anticipates awarding a task order to the offeror whose quote represents the best value, price and other factors considered.

The Government intends to evaluate proposals and may award a contract without discussions. However, the Government reserves the right to conduct discussions if determined by the contracting officer to be necessary. Therefore, each initial offer should contain the offeror’s best proposal from both a price and a technical standpoint.

Proposals received in response to this solicitation will be evaluated by the [Agency] pursuant to the FAR and in accordance with FAR 52.215-1, and as set forth in *Section 7 ‑ Proposal Instructions to Offerors*, one award will be made by the contracting officer to the responsible offeror whose proposal, conforming to the solicitation, is determined most advantageous to the Government, all technical and price factors considered.

The formula set forth herein will be used by the contracting officer as a guide in determining which proposals will be most advantageous to the Government.

Suggested Evaluation Language if LPTA Approach is Selected by the Agency   
(Agency may remove or modify the text below)

The lowest price technically acceptable source selection process is appropriate when best value is expected to result from selection of the technically acceptable proposal with the lowest evaluated price.

The evaluation factors and significant sub-factors that establish the requirements of acceptability should be set forth in this section.

If the contracting officer documents the file pursuant to FAR 15.304(c)(3)(iii), past performance need not be an evaluation factor in lowest price technically-acceptable source selections.

If the contracting officer elects to consider past performance as an evaluation factor, it shall be evaluated in accordance with FAR15.305. However, the comparative assessment in FAR 15.305(a)(2)(i) does not apply.

If the contracting officer determines that the past performance of a small business is not acceptable, the matter shall be referred to the Small Business Administration for a Certificate of Competency determination, in accordance with the procedures contained in subpart and U.S.C. 637(b)(7).

Award will be made to the offeror whose proposal represents the lowest price technically acceptable as defined in FAR 15, Subpart 15.101-1. The offeror’s proposal will be evaluated with regard to its ability to meet the tasks set forth in the SOW. To result in an award, the offeror’s proposal must demonstrate the ability to satisfy all technical requirements as set forth in *Section 2*, and must conform to all required terms and conditions.

The award will be made on the basis of the lowest-evaluated price of proposals meeting or exceeding the acceptability standards for non-price factors.

Proposals will be evaluated for acceptability but not ranked using non-price factors.

## Technical Evaluation Criteria

The Government will review the responses to this solicitation to ensure that offerors have addressed the requirements for Tasks 1 [through n] and are sufficient in detail and clarity to allow the Government to determine if the proposed support services, equipment, and equipment services are acceptable. If they are found unacceptable, the Government retains the right to conduct further discussions.

The Government will evaluate the offeror’s proposal based upon the following four factors: technical approach, management approach, proposed personnel, and past performance*.* Within these factors, the Government will evaluate the sub-factors identified in Table 3 below. To achieve an acceptable rating, the offeror’s Technical Proposal must achieve a pass rating on all sub-factors.

With regard to how the Government will evaluate the offeror’s core capabilities, the offeror should review Section 2.2 of this document.

The Agency is required to develop a Source Selection Plan (SSP)/Technical Evaluation Plan (TEP) to describe how each of these factors will be rated. Depending on the approach used, the SSP/TEP may select an adjectival rating system, a points system, or any other approved system.

Table 3. Offerors’ Proposal Factors and Sub-factors

| Technical Evaluation Criteria |
| --- |
| * Factor 1 ‑ Technical Approach |
| * Sub-factor 1 ‑ Task 1 |
| * Sub-factor 2 ‑ Task [n] |
| * Factor 2 ‑ Management Approach |
| * Factor 3 ‑ Proposed Personnel |
| * Sub-factor 1 ‑ Project Manager Qualifications/Certifications |
| * Sub-factor 2 ‑ Technical and Other Personnel Qualifications/Certifications |
| * Factor 4 ‑ Past Performance |

Suggested Evaluation Language for Technical Evaluation of Technical Criteria   
(Agency may remove or modify the text below)

The following evaluation criteria will serve as the standard against which all proposals will be evaluated and will serve to identify the significant discussion items that offerors should address in their proposals.

The factors and sub-factors are presented below. Factors are [of equal importance or listed in descending order of importance]. Sub-factors are [of equal importance or listed in descending order of importance].

Factor 1 ‑ Technical Approach. The extent to which the proposal demonstrates a clear understanding of the statement of work and the degree to which the proposed implementation approach is technically and managerially sound and likely to meet the objectives of the [Project Name] project as described in this solicitation. The technical approach must be realistic, directly relevant to the achievement of results and must seek to maximize results within budget resources.

* Sub-Factor 1 ‑ Planning and Design. The extent to which the proposed solution meets all the [technical] requirements of Task 1.
* Sub-Factor n‑ The extent to which the proposed solution meets all the [technical] requirements of Task n.

Factor 2 ‑ Management Approach

* The proposed solution shall describe the extent to which it uses a program management approach appropriate to the size and complexity of the project, and clearly demonstrate how the proposed technical solution for each task will achieve expected results. The offeror’s project management summary and schedule [and its formal Project Management Plan (using the template found in Attachment A)] will be evaluated against these criteria.

Factor 3 ‑ Proposed Personnel

* Sub-Factor 1 ‑ Qualifications and Demonstrated Ability of the PM. The proposed PM shall demonstrate the qualifications and ability to successfully lead this project, including the ability to work constructively at multiple levels of organizations, including senior levels of Government and business.
* Sub-Factor 2 ‑ Qualifications and Demonstrated Ability of the Proposed Technical Staff and Key Personnel. The members of the proposed project team, including Subject-Matter Experts (SMEs), shall demonstrate the experience and ability to successfully meet the project milestones, targets, and goals.

Factor 4 ‑ Past Performance

* The offeror and major subcontractor(s) past performance will be evaluated. A major subcontractor (if applicable) is defined as a subcontractor named in the proposal whose total price exceeds 15% of the offer’s bottom line total price, including fixed fee. The contracting officer will utilize existing databases of contractor performance information (i.e., PPIRS) and solicit additional information from the references provided in this SOW. The [Agency] may also use performance information obtained from sources other than those identified by the offeror/subcontractor.

## Price Evaluation Criteria

Suggested Evaluation Language for Price Evaluation Criteria   
(Agency may remove or modify the text below)

No points are assigned to the price proposal evaluation. While the technical evaluation criteria are significantly more important than price, price remains important.

Price will primarily be evaluated for realism, allow-ability, and reasonableness.

This evaluation will consist of a review of the price portion of an offeror’s proposal to determine if the overall price proposed is realistic for the work to be performed, if the price reflects an accurate understanding of the requirements, and if the price is consistent with the Technical Proposal.

Evaluation of the price proposal will consider but not be limited to the following:

* Price reasonableness, price realism and completeness of the price proposal and supporting documentation
* Overall price control/price savings evidenced in the proposal (avoidance of prices that exceed reasonable requirements)
* The amount of the proposed fee, if any

Price realism is an assessment of the accuracy with which proposed prices represent the most probable cost of performance within each offeror’s technical and management approach. A price realism evaluation will be performed as part of the evaluation process as follows:

* Verify the offeror’s understanding of the requirements
* Assess the degree to which the price proposal accurately reflects the technical approach
* Assess the degree to which the prices included in the Price Proposals accurately represent the work effort included in the respective Technical Proposals

The results of the price realism analysis will be used as part of the Agency’s best value/tradeoff analysis.

Although technical evaluation criteria are significantly more important than price, the closer the technical evaluation scores of the various proposals are to one another, the more important price considerations will become. The evaluation of proposed prices may therefore become a determining factor in the award as technical scores converge.

# Task Order Award

The Task Order Award will be made to the responsible offeror whose proposal is in the best interest of the [Agency], given the outcome of the [Agency]’s evaluation of each offeror’s technical excellence, management and business risk factors, and proposed price. In selecting the Task Order Award, the [Agency] will consider the quality offered for the evaluated price. The relative quality of offers will be based upon the [Agency]’s assessment of the tradeoffs between the technical excellence offered in the offeror’s proposal and whether it provides added value, added capability, and/or reduced management and business risk.

# Organizational Conflicts of Interest

The guidelines and procedures of FAR Subpart 9.5 will be used in identifying and resolving any issues of organizational conflicts of interest at the task order level.

In the event that a task order requires activity that would create or has created an actual or potential conflict of interest, the offeror shall:

* Notify the task order Contracting Officer (CO) of the actual or potential conflict, and not commence or continue work on any task order that involves a potential or actual conflict of interest until specifically notified by the task order CO to proceed.
* Identify the conflict and recommend to the task order CO an alternate tasking approach which would avoid the conflict.

If the task order CO determines that it is in the best interest of the Government to issue or continue the task order, notwithstanding a conflict of interest, a request for waiver shall be submitted in accordance with FAR 9.503. In the event that the offeror was aware of facts required to be disclosed or the existence of an actual or potential organizational conflict of interest and did not disclose, when known, such facts or such conflict of interest to the task order CO, the Government may terminate this contract for default.

In the event that a task order issued under this contract requires the offeror to gain access to proprietary information of other companies, the offeror shall be required to execute agreements with those companies to protect the information from unauthorized use and to refrain from using it for any purpose other than for which it was furnished.

# List of Acronyms

|  |  |
| --- | --- |
| API | Application Programming Interface |
| ATO | Authority to Operate |
| ATO | Authorization to Operate |
| BPI | Baseline Privacy Interface |
| CAC | Common Access Cards |
| CO | Contracting Officer |
| CONUS | Continental United States |
| COOP | Continuity of Operations |
| COR | Contracting Officer Representative |
| COTS | Commercial Off-the-Shelf |
| DNS | Domain Name System |
| DR | Disaster Recovery |
| EST | Eastern Standard Time |
| FAR | Federal Acquisition Regulation |
| FFP | Firm Fixed Price |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FSSI | Federal Strategic Sourcing Initiative |
| GFE | Government Furnished Equipment |
| GPS | Global Positioning System |
| GSA | General Services Administration |
| GUI | Graphical User Interface |
| IP | Internet Protocol |
| HSPD-12 | Homeland Security Presidential Directive 12 |
| LAN | Local Area Network |
| LPTA | Lowest Price Technically Acceptable |
| MAM | Mobile Application Management |
| MAS | Mobile Application Store |
| MDM | Mobile Device Management |
| NFC | Near Field Communication |
| NIST | National Institute of Standard and Technology |
| OCONUS | Outside the Continental United States |
| ODC | Other Direct Costs |
| OMB | Office of Management and Budget |
| OS | Operating System |
| PIM | Personal Information Manager |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PM | Project Manager |
| PMP | Project Management Professional |
| PoAM | Plan of Action and Milestones |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| PST | Pacific Standard Time |
| RFID | Radio-Frequency Identification |
| RFP | Request for Proposal |
| S/MIME | Secure/**Multipurpose Internet Mail Extensions** |
| SCAP | Security Content Automation Protocol |
| SCOM | System Center Operations Manager |
| SDK | Software Development Kit |
| SME | Subject Matter Expert |
| SOW | Statement of Work |
| SP | Special Publication |
| SSP | Source Selection Plan |
| T&M | Time and Material |
| TEMS | Telecommunications Expense Management System |
| TEP | Technical Evaluation Plan |
| VDI | **Virtual Desktop Infrastructure** |
| VPN | Virtual Private Network |

# Attachments

Double-clicking the attachments may produce the error “Word cannot start the converter mswrd632.wpc,” which is a known Microsoft issue (<http://support.microsoft.com/kb/973904>). Microsoft provides the following workaround: right-click on the embedded attachment (instead of double-clicking) and then select “Document Object” and then use “Open” (instead of “Convert”) from the pop-up menu.

## Attachment A – Project Management Plan



## Attachment B – Support Locations



## Attachment C – Pricing Requirements



## Attachment D – Pricing Template



## Attachment E – Past Performance Worksheet



## Attachment F – Task Order Deliverables

