



4050 Esplanade Way
Tallahassee, FL 32399-0950
850-488-2786

Ron DeSantis, Governor
Jonathan R. Satter, Secretary

ATTACHMENT A – STATEMENT OF WORK

FOR

MOBILE COMMUNICATION SERVICES

ITN NO: DMS-19/20-006

INVITATION TO NEGOTIATE

THE STATE OF FLORIDA

DEPARTMENT OF MANAGEMENT SERVICES

Table of Contents

- 1. Statement of Work Introduction..... 6
 - 1.1 Instructions for Response Blocks 7
 - 1.2 Mobile Communication Services Portfolio..... 7
 - 1.3 MCS Objectives..... 8
 - 1.4 MyFloridaNet..... 9
 - 1.5 End User Price Lists and Vendor’s Device List..... 9
 - 1.6 Evolving Technology 10
- 2. Contractor Staffing..... 11
 - 2.1 Staffing Responsibilities 11
 - 2.2 Key Staff Position - Account Manager 13
 - 2.3 Key Staff Position - Project Manager 14
 - 2.4 Key Staff Position - Business Operations Manager 14
 - 2.5 Key Staff Position - Engineering and Design Manager 15
 - 2.6 Key Staff Position - Operations and Security Manager 15
 - 2.7 Customer Support Team..... 16
- 3. Services and Devices for Mobile Communication Services..... 17
 - 3.1 Wireless Voice Services..... 17
 - 3.2 Wireless Data Service..... 17
 - 3.3 Wireless Data Service - IP Addresses..... 18
 - 3.4 Wireless Data Service – Access Circuit 18
 - 3.5 Wireless Data Service - Closed User Groups 20

3.6	Wireless Data Service – Network-to-Network Interface Design.....	21
3.7	Wireless Data Service –Traffic Mapping into MyFloridaNet.....	25
3.8	Wireless Data Service – Traffic Directly to the Internet.....	26
3.9	Wireless Data Service - Test Plan	28
3.10	State of Florida Coverage	28
3.11	Roaming.....	29
3.12	Security.....	29
3.13	Reviews of the Contractor’s Service.....	31
3.14	Emergency Services	32
3.15	Contractor’s Service Delivery Costs	33
3.16	Highly Available and Highly Reliable Design Characteristics	33
3.17	Reports, Updates, and Notifications Requirements	34
3.18	Service Level Agreement Operational Process.....	35
3.19	Customer Support	37
3.20	Contractor’s MCS Portal	38
3.21	Devices.....	39
3.22	Cooperation with Other Contractors	40
3.23	Customer Migration.....	41
3.24	Transition for Future Iterations of this Service.....	41
3.25	Contractor Meetings with DMS.....	43
3.26	Project Management.....	45
3.27	Project Management - Services Infrastructure Checklist	50

4.	Public Safety Service Plans and Devices.....	53
4.1	Deployable Technologies.....	53
4.2	Local Control	54
4.3	Local control portal.....	54
4.4	Public Safety Standards.....	54
4.5	Demonstration Devices.....	54
4.6	Public Safety Customer Support.....	55
4.7	Public Safety Reporting.....	55
4.8	Public Safety Marketing	55
5.	Business Operations	56
5.1	General Description of the SUNCOM Business Model.....	56
5.2	Communications Service Authorization and Billing Transaction Flowchart.....	56
5.3	Communications Service Authorization and Billing – Official Record.....	58
5.4	Communications Service Authorization and Billing - Interface with Contractor.....	58
5.5	Communications Service Authorization and Billing Service Catalog	59
5.6	Taxes and Government Sanctioned Fees	59
5.7	User Access Privileges for the Contractor.....	60
5.8	Work Orders.....	60
5.9	Inventory.....	61
5.10	Invoicing Requirements.....	61
5.11	Electronic Substantiating Detail File	61
5.12	Audit of Contractor Invoices.....	62

5.13	Mandatory Interface with the Contractor	62
5.14	Properly Authorized Work Orders.....	62
5.15	General Billing Requirements	62
5.16	Billing Start	62
6.	Direct Ordering and Billing	63
6.1	Services and Devices Sold to Direct-Billed Customers.....	63
6.2	Cost Recovery Rate.....	63
6.3	Contract Association on Direct-Billed Accounts	64
6.4	Monthly Reporting of Direct-Billed Accounts.....	64
6.5	Quarterly Reporting of Direct-Billed Accounts.....	65
6.6	Customers Liability	65

1. Statement of Work Introduction

This Attachment A – Statement of Work (SOW) describes cellular voice and data services, secure access to MyFloridaNet (cellular data-only devices), and other related telecommunication services, cellular phones, associated devices, accessories, and features, collectively referred to herein as Mobile Communication Services (MCS).

All requirements contained in this SOW are Contract requirements. Deliverables and associated financial consequences (hereinafter referred to as “Service Level Agreements” or “SLAs”) are specified on Attachment C – Service Level Agreements.

The intent of this procurement is to establish one (1) or more multi-year Contract(s) that meet the goals of the ITN, as stated in Section 1.5, Goals of the ITN, of that document. Any contracted services will be available for use by State agencies and political subdivisions of the State, municipalities, and nonprofit corporations in accordance with Chapter 282, Florida Statutes (F.S.).

This SOW contains operational and administrative objectives for MCS that will form the requirements for implementation and on-going support under any Contract resulting from this ITN.

This SOW is intended to reflect the requested service components DMS is seeking the Respondent to offer for MCS. This SOW includes references to service components that “must,” “shall,” or “will” be delivered; however, these SOW references to “must,” “shall,” “will,” and “minimum requirements” will not affect DMS’s determination of a Respondent’s responsiveness. DMS intends for these SOW references to become mandatory at the time of Contract execution (as reflected in DMS’s Request for Best and Final Offer (BAFO)). However, these SOW references may be subject to negotiation during the procurement and will be resolved through the terms of DMS’s Request for BAFO. The terms “will” and “shall” are used interchangeably.

The Request for BAFO may also provide for requirements in place of what may previously have been requests. For example, the word ‘should’ in this SOW may be replaced by the word ‘must’ in the final SOW attached to the Request for BAFO.

While the Department reserves the right to negotiate any term or condition during the negotiation process, the Contractor agrees that its Reply is based on the assumption that the terms and conditions of this SOW, as well as the Draft Contract (Attachment B to the ITN), apply as currently written.

If more than one (1) Contract is awarded, then the use of the terms “Contract,” “Contractor,” “Reply,” and “Respondent,” include the plural when applicable.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.
--

1.1 Instructions for Response Blocks

The SOW contains response blocks where Respondents are to provide information. Respondents may attach additional narrative with a reference to the corresponding SOW response block subsection. Respondents should base responses on the information provided in the applicable subsections and response blocks regarding operational and administrative processes and other aspects of the proposed services.

Responses to the SOW will be scored and will not be used to determine responsiveness. Respondents should provide responses to all response blocks seeking a response in the SOW.

If the Respondent inserts "N/A" or leaves a response block blank, they will receive zero points for that subsection. Replies are to be submitted in accordance with the ITN. See Subsections 3.7, 4, of the ITN for additional instructions on submitting a Reply.

The response blocks may contain approximate word counts in brackets, e.g., [Enter the response here – XXX words]. The word counts are provided as guidance to the length of the expected response; the word counts are neither minimum nor maximum limits.

By submitting a Reply to this ITN, the Respondent affirms that it has read, understood, and will comply with all of the statements, terms, and conditions contained in this SOW.

Do not provide pricing information in any SOW response block. Respondent is to submit pricing information separate from the response to this SOW, in accordance with instructions in the ITN.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

1.2 Mobile Communication Services Portfolio

Mobile Communication Services are described below as well as in the public safety services in Section 4.

1.1.1 Wireless Voice Services (WVS), includes plans and cellular phones, smart phones, tablets, and other similar devices capable of making voice calls to cellular devices (cellular voice) and to traditional phones on the Public Switched Telephone Network (PSTN). This set of services also provides broadband access for email, internet browsing, texting, and numerous applications.

1.1.2. Wireless Data Services (WDS), includes a similar set of broadband services and devices as WVS but does not provide cellular voice and does not include PSTN voice connectivity. This set of services can provide secure data access into MyFloridaNet (for additional information, see Section 1.4, MyFloridaNet, below).

Both sets of services include broadband data service plans governing the Customer's monthly allotment for broadband access.

1.1.3 Web portals for both WVS and WDS. Customers utilize the DMS Communications Service and Billing system (CSAB) to review all MCS offerings, which are found on the End User Price List (EUPL). Orders are either placed directly via MyFloridaMarketPlace (MFMP), CSAB, or direct with the Contractor. For additional information regarding the EUPL, see Section 5, Business Operations.

1.1.4. Accessories include, but are not limited to, antennas, phone cases, tablet cases, headphones and ear buds, chargers, screen protectors, foldable keyboards, belt clips, and hands-free kits.

1.1.5. Equipment includes, but is not limited to, smartphones, basic phones, air cards, hot spots, tablets, and public safety wearables (within the optional subsection on Public Safety Service Plans and Devices).

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

1.3 MCS Objectives

In accordance with the Department's objectives for MCS, the Contractor shall provide:

1. Services and devices that keep pace with rapidly evolving technologies and related service plans.
2. A range of rate plans with a wide variety of up-to-date features.
3. Customer support services, including the Contractor's MCS portal and superior staffing, with the best possible customer service.
4. Clearly articulated adoption of standards and designs in this SOW.
5. Complete and timely reporting on services to the Department and Customers.
6. Service strength with as much 4G/4G LTE or better service coverage as possible.
7. Highly-Available, Highly-Reliable (HA/HR) infrastructures.
8. Support for devices and software systems from different manufacturers.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

1.4 MyFloridaNet

MyFloridaNet (MFN) is the State's Multiprotocol Label Switching data network. MFN allows State agencies and other authorized users to communicate with each other. Information about MFN is available at:

https://www.dms.myflorida.com/business_operations/telecommunications/suncom2/data_services/myfloridanet_2

No response required. By submitting a Reply, Respondent has read and understands the statements contained in this subsection.

1.5 End User Price Lists and Vendor's Device List

This subsection applies to both WVS and WDS.

1.5.1 Creation of Initial EUPL and Vendor's Device List

Pricing information in the Contractor's BAFO will be used by the Contractor to create the EUPL and Vendor's Device List after Contract execution. The format of the EUPL and Vendor's Device List must be approved by the Department. The Contractor must have one (1) EUPL and one (1) Vendor's Device List that incorporate all offerings. The Department's current MCS EUPLs are available on the DMS website here:

https://www.dms.myflorida.com/business_operations/telecommunications/suncom2/voice_services/mobile_communication_services

1.5.2 Update Process to EUPL

Given the fast pace of technological progress, DMS anticipates that plans and devices will improve and undergo alterations, within the scope of the Contract, over the term of the Contract. Changes in service plans, features, devices, or technology offered by the Contractor in the same, alternative, or equivalent form and within the scope of the Contract are permissible updates. Updates may be prompted by the Contractor, DMS, or Customers. Some updates may be accomplished via the change request process described in Section 5.2, Change Request, of the Contract; however, at DMS's sole discretion, updates may require a Contract amendment.

Contractor-Requested Updates. The Contractor may request updates to its EUPL and Vendor's Device List throughout the Contract term. Such requests must be emailed to the DMS Contract Manager for review and approval. DMS has absolute discretion to approve or deny Contractor-requested updates.

The Contractor shall not offer Customers changes in plans, features, devices, or technology prior to obtaining DMS's written approval. The Contractor shall not offer any updated prices or rate structures until changes have been approved by DMS and DMS has published an updated EUPL.

When requested by DMS, the Contractor shall provide documentation on the requested update, including, but not limited to, market research and service and device specifications. DMS may review the information from the Contractor and any other source.

DMS will not approve an update request until and unless the criteria below is met to its satisfaction. However, DMS reserves the right to deny an update request even if all of the criteria are met. The Contractor shall:

1. Substantially demonstrate the pricing is competitive to market rates, specifically that it is equal to or less than rates for similar offerings in the State of Texas, State of California, and State of New York;
2. Fully demonstrate the pricing is related to and is in line with currently offered pricing for similar services and equipment within the EUPL and/or the Vendor's Device List; and
3. Fully demonstrate the proposed pricing is in accordance with Contract Section 3.2.2, Preferred Pricing.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

1.6 Evolving Technology

This section is applicable to all services and equipment, including devices.

The Contractor shall ensure delivery of services and devices that keep pace with rapidly evolving technologies and related service plans. The Vendor's Device List and EUPL must be kept up-to-date, in accordance with the process detailed within SOW Subsection 1.5, End User Price Lists and Vendor's Device List, offering the latest generation of devices and related service plans.

The Contractor's IP infrastructure must provide evolving technologies and offer Customers the latest generation of telecommunications infrastructure and devices.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.
2. Provide a detailed description of the following:
 - a. How Respondent will ensure delivery of services and devices that keep pace with rapidly evolving technology and related service plans.

- b. Describe the Respondent's commitment and plan to offer the latest generation of installed infrastructure supporting MCS (the Respondent's IP infrastructure).

[Enter response here – 1,500 words]

2. Contractor Staffing

This section is applicable to all services.

The terms “Contractor staff” and “staff” include all staff employed by the Contractor providing services under the Contract and by its subcontractors providing services under the Contract.

The Contractor shall provide sufficient, qualified staff to oversee and carry out the services of this Contract. The Contractor shall designate individuals in its organization to be contacts for DMS and its Customers in accordance with the following subsections.

2.1 Staffing Responsibilities

1. The Contractor staffing responsibilities include conducting all components of the Contract in a timely, efficient, productive, consistent, courteous, and professional manner.
2. The Contractor shall provide a sufficient number of Contractor staff to handle the workload projected for the start of the Contract and shall be scalable and flexible so staffing can be adapted as needed.
3. The Contractor shall devote the staffing time and resources necessary to successfully manage the Contract and provide the ongoing services, including having sufficient staff available for telephonic, email, and on-site consultations.
4. The Contractor shall provide each of its staff members orientation and training on all components of the Contract prior to allowing the staff member to work on any component of the Contract. The Contractor shall provide the DMS Contract Manager with documentation of this training upon request.
5. Key Staff.
 - a. The Contractor shall initially fill all key staff positions and keep the key staff positions filled throughout the term of the Contract. Key staff positions will be filled within thirty (30) days from Contract execution. **Attachment C, SLA-A1(a).**
 - b. The Contractor will only fill key staff positions with persons that fulfill the minimum job qualifications in accordance with this Section 2, Contractor Staffing.
 - c. DMS reserves the right to review and approve candidates being considered by the Contractor for a key staff position described in this Contract.

- d. DMS reserves the right to require the replacement of any staff who serve in a key staff position or as part of the Customer Support Team, and the Contractor shall remove such staff no later than ninety (90) calendar days' from the date of DMS's notice to the Contractor.
 - e. Waiver. The Contractor may request a waiver of SLA-A1(b) from the DMS Contract Manager if it believes it has good cause to not fill a key staff position within the required timeframe. DMS will review any such requests on a case-by-case basis and respond within a reasonable timeframe. Determination of all waiver requests are at the sole discretion of DMS. SLA-A1(b) will be on hold while the Department is reviewing a request for waiver.
 - f. Vacancy.
 - i. It is understood and agreed that from time to time a vacancy may occur in key staff positions. For purposes of this Contract, a vacancy occurs when: the position is not initially filled; the position is not filled due to a resignation, retirement, termination, or reassignment; or the position is filled with a person who does not possess the minimum qualifications required to perform the job duties. A vacancy does not occur when: an employee is temporarily absent due to vacation, sick leave, or other temporary leave condition, such as training. In the case of a vacancy, the Contractor may arrange for the job duties to be provided by another employee who meets the minimum job qualifications until this position is filled. However, a temporary assignment will not suspend any Contractor Staffing SLAs. Key staff positions will be filled within ninety (90) days of vacancy or within the timeframe established by the Department after a waiver of the ninety (90) day requirement. **Attachment C, SLA-A1(b).**
 - ii. The Contractor shall notify DMS of all vacancies of key staff positions within fourteen (14) days of the vacancy. **Attachment C, SLA-A1(c).**
6. Staffing Organization Chart. The Contractor shall develop a Staffing Organizational Chart to be implemented throughout the Contract term. **Attachment C, SLA-A2.** The chart will include all staff resources assigned to all components of the Contract to be approved by DMS. The final Staffing Organizational Chart must contain names, titles, and number of staff (full-time and part-time) proposed to support the Contract. The Contractor's final Staffing Organizational Chart shall include a justification for the number of staff and the percentage of time each staff person will devote to the Contract.
7. Staffing Deficiencies. The Contractor is required to provide sufficient, competent, and capable staff to provide complete and timely services as required by the Contract. In the event DMS determines the Contractor has a staff deficiency, it will notify the Contractor in writing. A staff deficiency will include, at the Department's discretion, insufficient number of staff, or insufficient level of competency in staff, to provide complete and timely services under this Contract. A staffing deficiency will also include the retention of staff thirty (30) days past a Department Contract Manager's requirement to remove that staff member. The Contractor must remedy the identified staffing deficiencies by adding or replacing staff as required by the Department.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.
2. Provide a detailed description of the following:
 - a. How Respondent will ensure the dedication of its proposed key staff positions, including the proposed percent of time dedicated to DMS;
 - b. How Respondent will be prepared at all times to recruit credentialed, appropriately licensed, and highly qualified staff and the recruitment process for staff that will be assigned to the Contract;
 - c. Respondent's orientation and training for Respondent's staff assigned to the Contract;
 - d. How Respondent will ensure it employs all required positions and that there are sufficient staff to complete all requirements initially and throughout the duration of the Contract.

[Enter response here – 1,500 words]

2.2 Key Staff Position - Account Manager

The Contractor shall assign a dedicated, but not necessarily exclusive, Account Manager as the primary contact for DMS, unless DMS determines an exclusive Account Manager is in DMS's best interest at any point during the Contract term, including renewals. This is a required key staff position.

The Contractor is required to provide a full-time Account Manager for all services under the Contract. The Account Manager will be the senior manager and primary contact with responsibility for all day-to-day MCS issues, including, but not limited to, coordination and resolution of all MCS activities. The Account Manager will be a senior staff member able to carry DMS concerns to the Contractor's management personnel. The Account Manager or designated backup(s) must be available twenty-four (24) hours a day, 365 days of the year.

The Account Manager is required to participate in the various workgroups to accomplish services available under MCS.

The Account Manager shall possess the following minimum qualifications:

1. A minimum three (3) years' experience working with government clients in a government account management or sales role.
2. A knowledge of government business practices, including State practices and practices of Customers.
3. At least three (3) years' work experience in the telecommunications industry.

4. Strong verbal and written communication skills, including the ability to communicate effectively at all levels of an organization.

If the Contractor is providing Public Safety Services, the Account Manager must have experience in the Public Safety proposed services.

2.3 Key Staff Position - Project Manager

The Contractor shall assign a dedicated, but not necessarily exclusive, Project Manager, unless DMS determines an exclusive Project Manager is in DMS's best interest. This is a required key staff position.

The Project Manager shall oversee and take on the responsibility for the success of all projects. This individual will be the point of contact to coordinate all implementation and migration with DMS. This individual will manage and direct the planning of the Contractor's staff and resources.

The Project Manager is required to participate in the various workgroups to accomplish services available under MCS.

The Project Manager shall possess the following minimum qualifications:

1. The ability to be responsible for every aspect of all projects related to this Contract.
2. The ability to lead and direct teams to deliver projects within the constraints of schedule, budget, and resources.
3. Demonstrated knowledge and experience to appropriately apply a project management methodology to projects.
4. Experience using Microsoft Project and the ability to keep all projects updated frequently and accurately.
5. A current Project Management Professional certification from the Project Management Institute, Scrum Master Certification from Scrum Alliance, CompTIA Project+ certification from CompTIA, a Lean Six Sigma certification, or other equivalent project management certification approved in writing by DMS.

2.4 Key Staff Position - Business Operations Manager

The Contractor shall assign a dedicated, but not necessarily exclusive, Business Operations Manager, unless DMS determines an exclusive Business Operations Manager is in DMS's best interest. This is a required key staff position.

The Business Operations Manager shall oversee business operations, including billing, ordering, and related business operational procedures. The Business Operations Manager, acting as the DMS advocate, will be a Contractor senior staff member able to carry DMS concerns to the Contractor's management personnel. As the advocate, the individual must have the authority to direct the Contractor's staff to effect business operational procedures and related outcomes.

The Business Operations Manager is required to participate in the various workgroups to accomplish services available under MCS.

The Business Operations Manager shall possess the following minimum qualifications:

1. A minimum of three (3) years' experience working with government clients.
2. Knowledge of government business practices, including State practices and practices of Customers.
3. Strong verbal and written communication skills, including the ability to communicate effectively at all levels of an organization.

2.5 Key Staff Position - Engineering and Design Manager

The Contractor shall assign a dedicated, but not necessarily exclusive, Engineering and Design Manager, unless DMS determines an exclusive Engineering and Design Manager is in DMS's best interest. This is a required key staff position.

The Engineering and Design Manager shall function as the point of contact for all engineering and design issues. The individual will be responsible for directing all aspects of engineering and design concerns for the services. The individual must have the authority to direct the Contractor's staff. The individual or designated backup(s) must be available twenty-four (24) hours a day, 365 days of the year to manage and oversee restoration of services and to respond to State requests.

The Engineering and Design Manager is required to participate in the various workgroups to accomplish services available under MCS.

The Engineering and Design Manager shall possess the following minimum qualifications:

1. A minimum of three (3) years' experience leading an engineering team responsible for services similar in size and scope to services available under MCS.
2. A Bachelor of Science degree or higher in an engineering discipline. Equivalent foreign degrees are also acceptable.
3. Five (5) years or more of engineering work experience.

2.6 Key Staff Position - Operations and Security Manager

The Contractor shall assign a dedicated, but not necessarily exclusive, Operations and Security Manager, unless the Department determines an exclusive Operations and Security Manager is in DMS's best interest. This is a required key staff position.

The Operations and Security Manager shall serve as the engineer capable of communicating with other engineers as needed to resolve day-to-day issues. The individual will communicate with DMS and engineers from other Contractors providing telecommunications to the State and, if applicable, subcontractors. The individual will function as the point of contact for the day-to-day networking, service, and security issues, typically those involving real-time concerns. The

individual must have the authority to direct the Contractor's staff. The Operations and Security Manager, or a designated backup(s), must be available twenty-four (24) hours a day, 365 days of the year as required to manage operational and security concerns and respond to State requests.

The Operations and Security Manager is required to participate in the various workgroups to accomplish services available under MCS.

The Operations and Security Manager shall possess the following minimum qualifications:

1. A Bachelor of Science degree or higher in a computer science, information technology, engineering, or similar discipline. Equivalent foreign degrees are also acceptable. Equivalent work experience of five (5) years is acceptable.
2. Experience with business continuity and disaster recovery, including experience in development of disaster recovery plans.
3. Experience with information security architecture and security tools.
4. Knowledge of telecommunications industry best practices for service performance and security and applicable laws and regulations as they relate to security.
5. Knowledge of current technologies and processes used to establish and maintain networks with respect to security of MCS.

The Operations and Security Manager should possess the following minimum qualifications:

1. It is preferred, but not required, that the Operations and Security Manager be a Certified Information Security Manager, a Certified Information Systems Security Professional, or hold another current industry-recognized security certification.

2.7 Customer Support Team

The Contractor shall provide a Customer Support Team for this Contract. This team is not required to be full-time staff (part-time staff is acceptable) or exclusively dedicated to this Contract. However, the appropriate amount of staff at any given time (for example evening, weekend and holiday staffing may be less than weekday business hours) from the Customer Support team must be available twenty-four (24) hours a day, 365 days of the year. The Customer Support Team shall provide:

1. Timely Customer training in reaction to changes in services and features offered.
2. Timely resolution of service requests.
3. Full staffing for projects to implement new technologies, related services, and equipment features that are supported by the industry.
4. Timely closure for operational changes.
5. All applicable deliverables by the due dates as provided in the SLAs.

The Customer Support Team shall include at least one (1) named individual to act as the CSAB Administrator, with responsibilities described in Subsection 5.7, User Access Privileges for the Contractor.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3. Services and Devices for Mobile Communication Services

3.1 Wireless Voice Services

This subsection is applicable only to WVS.

The Contractor must provide WVS using digital technology as the primary communication mode. WVS will include cellular phones, smart phones, tablets, and other similar devices capable of making voice calls to cellular devices and to traditional phones on the PSTN. WVS will also include broadband access for email, internet browsing, texting, and numerous applications, such as those providing real-time traffic information.

International calling must be disabled by default, but Customers will be permitted to place an order to enable international calling. The Contractor shall provide Customers with the option of having texting disabled. The Contractor will coordinate directly with the Customer regarding texting capabilities.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.2 Wireless Data Service

This subsection is applicable to only Wireless Data Service.

The Contractor must provide WDS. The Contractor will provide non-proprietary wireless broadband data communications. For State agencies, security policy requires the Contractor's broadband data access to terminate on MFN by default. There may be instances where the Department's policy will permit broadband data access to terminate directly on the internet.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.3 Wireless Data Service - IP Addresses

This subsection is applicable to only Wireless Data Services.

The following are minimum requirements:

1. DMS will provide the Contractor work orders containing IP addresses to be associated with wireless devices. The Contractor must configure MCS devices with IP address as part of the activation and setup for the device. The Contractor must configure both 1) public IP addresses owned by the State and Other Eligible Users and 2) private IP addresses furnished by DMS and Other Eligible Users. Since not all private IP address space is available for use on MFN, a mutually agreed upon private IP address allocation block assignment (or other agreed upon method) will be finalized within the negotiation process.
2. The Contractor is required to provide publicly routable IP addresses as needed to support all Customers.
3. The Contractor will associate a particular wireless device with its closed user group (if any). The Contractor will assign an IP address to each wireless device and update the work order in CSAB with the specific IP address assigned before the Contractor closes the work order. A record of each closed user group and the associated wireless devices (including the electronic identifier and IP addresses) is maintained in CSAB.
4. The IP address assigned to a particular wireless device must be permanently assigned unless and until a work order provides that the Contractor change the address. Static IP addressing is acceptable as long as the address is coded (hard or electronically) within the device permanently. A unique IP address dynamically assigned to the device is acceptable as long as the address remains permanently assigned to that particular device. The dynamic IP address assignment mechanism must permanently assign the same address to the same device from an IP address pool assigned to a particular closed user group.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.
--

3.4 Wireless Data Service – Access Circuit

This subsection is applicable only to Wireless Data Services.

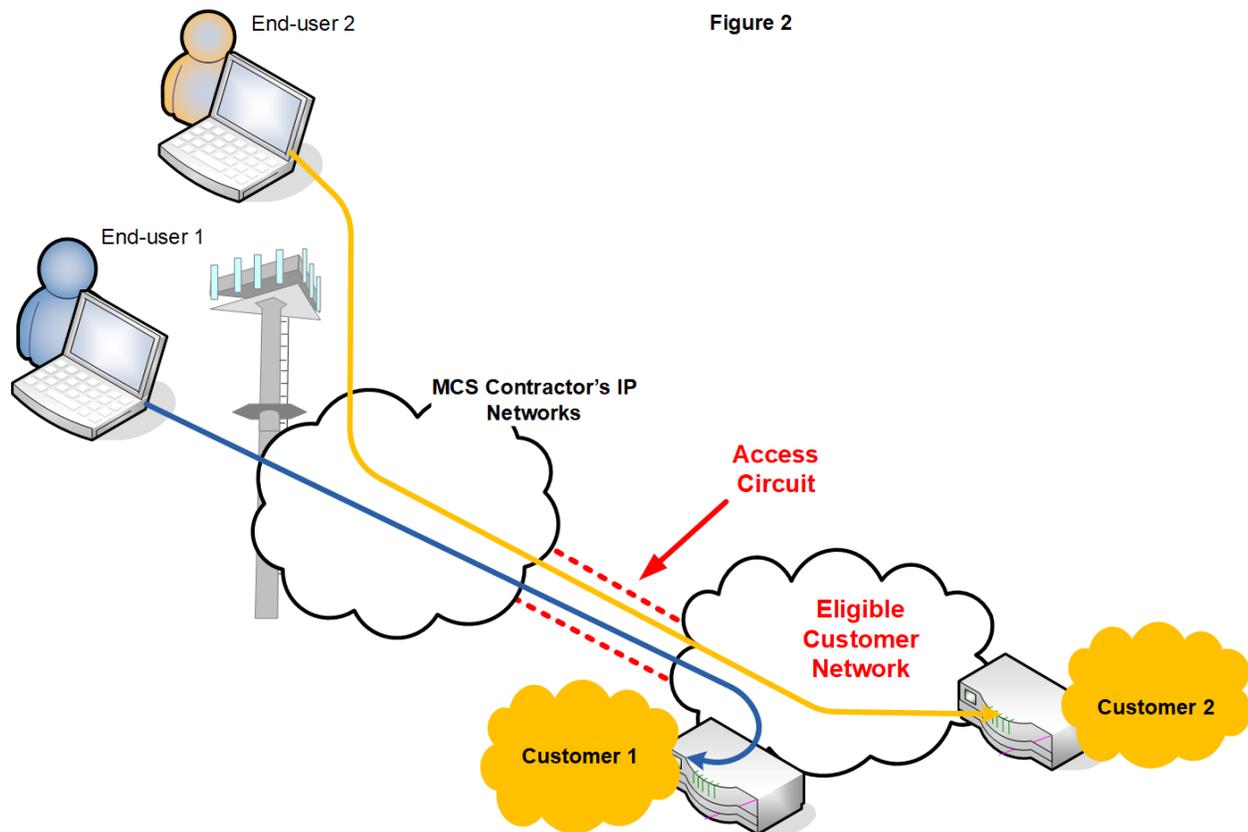
Where Customers have non-MFN networks (for example, non-State Agency Other Eligible Users), Contractors may utilize the Contract to provide their End-users with wireless connectivity into that Customer's network.

This design requires an access circuit between the Contractor's IP networks and an Other Eligible User's (OEU's) network. These access circuits are not offered by DMS as a SUNCOM service. DMS is not involved in ordering, billing, provisioning, payment, network support, or other aspects of these circuits. OEUs utilize their organization's procurement procedures to purchase their access circuit. All aspects of this wireless connectivity access are the responsibility of the OEU's organization and the Contractor, not DMS.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.

Access Circuit

Figure 2



No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

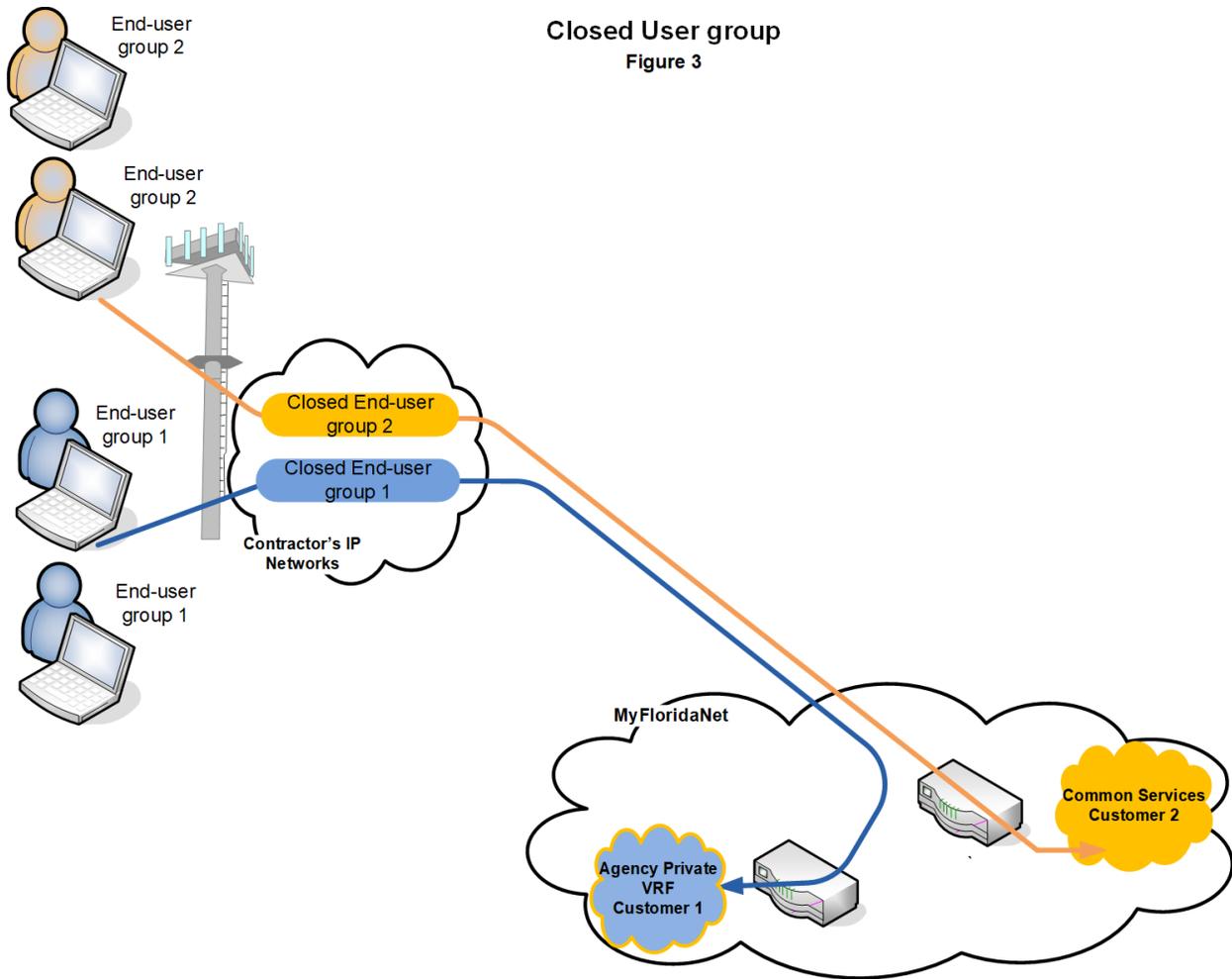
3.5 Wireless Data Service - Closed User Groups

This subsection is applicable to only Wireless Data Services.

The Contractor must develop, implement, and maintain a closed user group isolation method for WDS. The design must result in the segregation of all IP traffic into individual closed user groups. DMS may consider a virtual circuit, Virtual Local Area Network, or Virtual Routing and Forwarding (VRF) to be an acceptable closed user group design configuration method. Other Contractor-provided isolation methods are acceptable as long as the isolation method provides equivalent isolation design outcomes, as determined by DMS. The Contractor-created and maintained isolation method is required to be in continuous operation providing separation of wireless data traffic into distinct closed user groups.

At all points between the wireless data device and MFN, Customer traffic must be isolated from all other traffic within the Contractor's IP networks. There must be no alternate paths into or out of the isolated environment and no means for other entities or devices to access the isolated environment.

The Contractor will place each device in the closed user group as defined by the CSAB work order. Customers will have the ability to have multiple closed user groups configured within the Contractor's IP networks. No IP communications will be permitted between closed user groups within the Contractor's IP networks.



No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

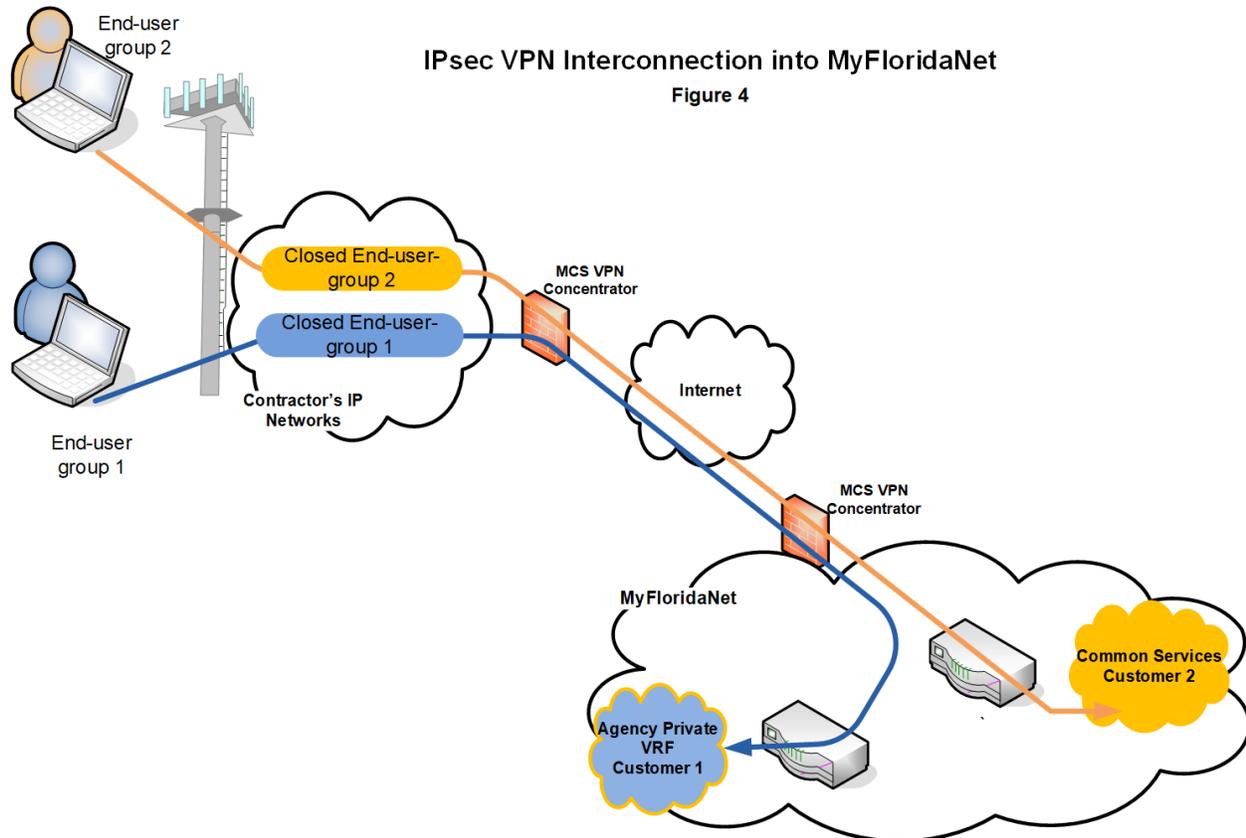
3.6 Wireless Data Service – Network-to-Network Interface Design

This subsection is applicable only to Wireless Data Services.

The Contractor must work with DMS and the MFN contractor to establish a network-to-network interface as shown in Figure 4 to route wireless data traffic across the internet to MFN. For redundancy, the interface design must use IPsec tunnels which connect to two (2) geographically separate gateways approved by DMS.

In each network-to-network interface location the Contractor must provide equipment and a corresponding design that will function as an IPsec Virtual Private Network (VPN) concentrator. Each interface will be configured with internet connectivity for the concentrators. The interface

design must utilize a primary and secondary interconnection scheme preventing any downtime or performance impact to the connectivity with MFN or downtime for the service. Each interface will function equivalently, including the available internet bandwidth capacity, operational software images, and overall configuration. The interface locations must always automatically failover.



The interface design must support VPN connectivity through the use of IPsec tunnels between the Contractor's IP networks and MFN. The Contractor configures IPsec tunnels to create closed user groups for traffic between the Contractor's IP networks and MFN. The Contractor routes closed user group traffic originating in the Contractor's IP networks to MFN via the internet, in coordination with DMS and the MFN contractor. Using a design selected by the Contractor and approved by DMS, wireless data devices must be provisioned to continuously operate within closed user groups.

The interconnectivity design, agreed on by the Contractor and DMS, must provide redundancy with automatic failover between MFN's two (2) VPN interconnection locations. The Contractor's interconnectivity design must be configured for the Contractor to monitor network connectivity between the Contractor's IP networks and MFN. In the event of a connectivity issue between the Contractor's network and MFN, the interconnection design must automatically failover and start

routing traffic within the failover metric. **Attachment C, SLA-B1.** Successful failover means the interconnection with MFN operates without any loss of performance compared to the interconnection performance prior to failover. Performance is measured by the Contractor's suite of Simple Network Management Protocol (SNMP) tools. After the failure has cleared the Contractor's interconnectivity design will, over time, automatically reestablish the tunnels to the MFN primary concentrator. The Contractor is not responsible for connectivity loss if the MFN VPN concentrators fail simultaneously.

DMS will provide the Contractor with the configuration parameters for each closed user group's IPsec tunnel. The Contractor must adhere to the configuration parameters while provisioning the concentrators. The Contractor must configure a unique IPsec tunnel for each closed user group's IP traffic as specified by DMS. The closed user group naming convention (or network identifier) will be mutually agreed upon by DMS and the Contractor. Each closed user group's network identifier must correlate to a unique IPsec tunnel.

DMS will provide the Contractor with the MFN tunnel termination IP addresses, IPsec pre-shared authentication keys, and tunnel configuration parameters for each tunnel. All information regarding IP addresses, IPsec authentication keys, and tunnel configuration parameters must be treated as secure State data. At no time will the Contractor transmit this information in clear text.

The Contractor must configure each unique IPsec tunnel to terminate on the primary MFN IPsec concentrator and also configure the tunnel to failover to the MFN secondary IPsec concentrator. DMS will provide the Contractor with two (2) unique publicly routable IP addresses for each closed user group's IPsec tunnel (primary and secondary). The Contractor will use one (1) of the two (2) addresses to terminate the tunnel at the MFN primary concentrator location, and the other address will be used to terminate the failover tunnel at the MFN secondary concentrator location. The Contractor must provide and use at least two (2) publicly routable IP addresses for its IPsec interconnection design; one (1) IP address for the primary tunnel termination and one (1) to terminate the secondary tunnel.

The Contractor will ensure that each wireless data device that traverses the IPsec interconnection will have a unique IP address permanently configured within the wireless modem or device (smartphone, handheld computer, laptop, etc.). Using the IP address provided by the Contractor, the Contractor must statically or dynamically assign each device within a unique closed user group a permanent IP address. The Contractor must configure each unique closed user group within its IP networks using the applicable IP addresses. At the MFN ingress point, each closed user group must be logically mapped into the appropriate MFN VRF. Adds, moves, or changes within a closed user group's configuration require a work order.

The Contractor must upgrade the network-to-network interface when the encrypted throughput, processor utilization, or port speed reach seventy-five percent (75%) of capacity. Internet bandwidth must be upgraded by the Contractor if bandwidth utilization reaches seventy-five percent (75%) of capacity. All network-to-network interface upgrades must improve capacity by

at least twenty percent (20%). **Attachment C, SLA-B2.** All upgrades are at no cost to the Department or Customers.

The Contractor will give DMS, and the MFN network monitoring tools, read-only SNMP access to monitor performance of the network, including network-to-network interface components. The Contractor must establish monitoring of SNMP performance metrics, which are measured over each five-minute sample.

The primary and secondary VPN concentrators must support the following IPsec parameters:

IPsec Parameters	
IKA (SA)	Main Mode
Encryption Strength	3DES
Authentication	Pre-Shared Key
Diffie-Hellmans (D-H) Groups	2 or 5 (group-5 preferred)
Perfect Forward Secrecy	Pfs
Data Integrity Hash Algorithm	SHA
IPsec (SA)	Quick Mode
Security Association (SA) Lifetime	86,400 seconds (maximum)
Authentication Type	HMAC-SHA
Security Association (SA) Lifetime	28,800 seconds (maximum)
Simultaneous Active Tunnels	1,000 (minimum)

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.
2. Describe the Respondent's commitment to the appropriate industry standards.
3. Describe the design.

4. Describe the portion of the design used to trigger the automatic failover.
5. Describe the failover and failback processes.
6. Describe how you will maintain the security of your MFN interconnection.

[Enter the response here as needed to provide a complete response]

3.7 Wireless Data Service –Traffic Mapping into MyFloridaNet

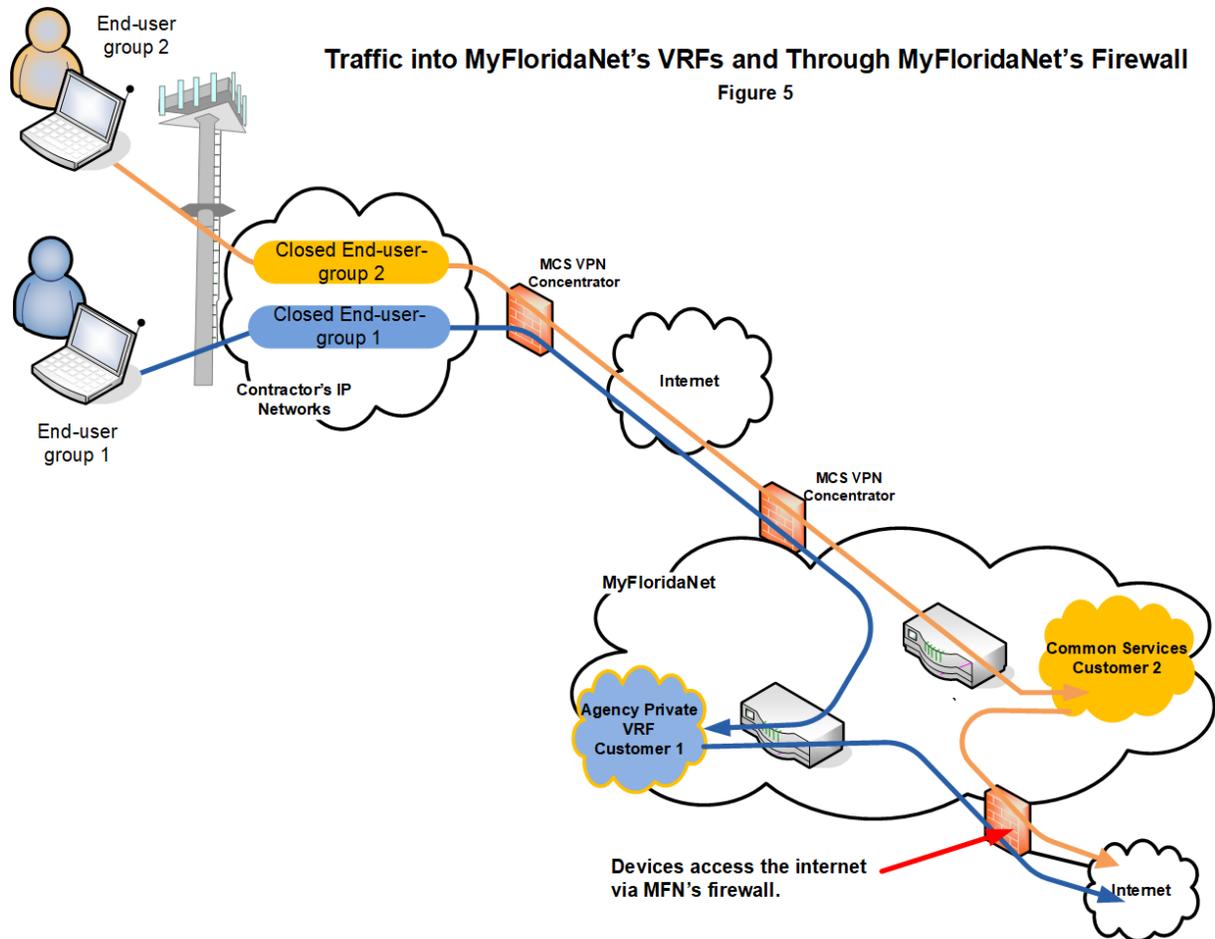
This subsection is applicable to only Wireless Data Services.

The Contractor shall coordinate and communicate with the MFN contractor and other MCS Contractors.

For traffic to MFN, the Contractor must route wireless data traffic across the Contractor's IP networks utilizing IPsec tunnels (one (1) unique IPsec tunnel per closed user group). DMS retains control related to security policies on access into MFN and its intranet as well as IPsec tunnel configuration parameters. All Customer wireless traffic must be in a closed user group within a unique IPsec tunnel in a manner such that it can be mapped into the appropriate MFN VRF by the MFN contractor.

If permitted by the applicable Department security policies, once wireless data traffic is within MFN it accesses the internet via the MFN firewall.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.



No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.8 Wireless Data Service – Traffic Directly to the Internet

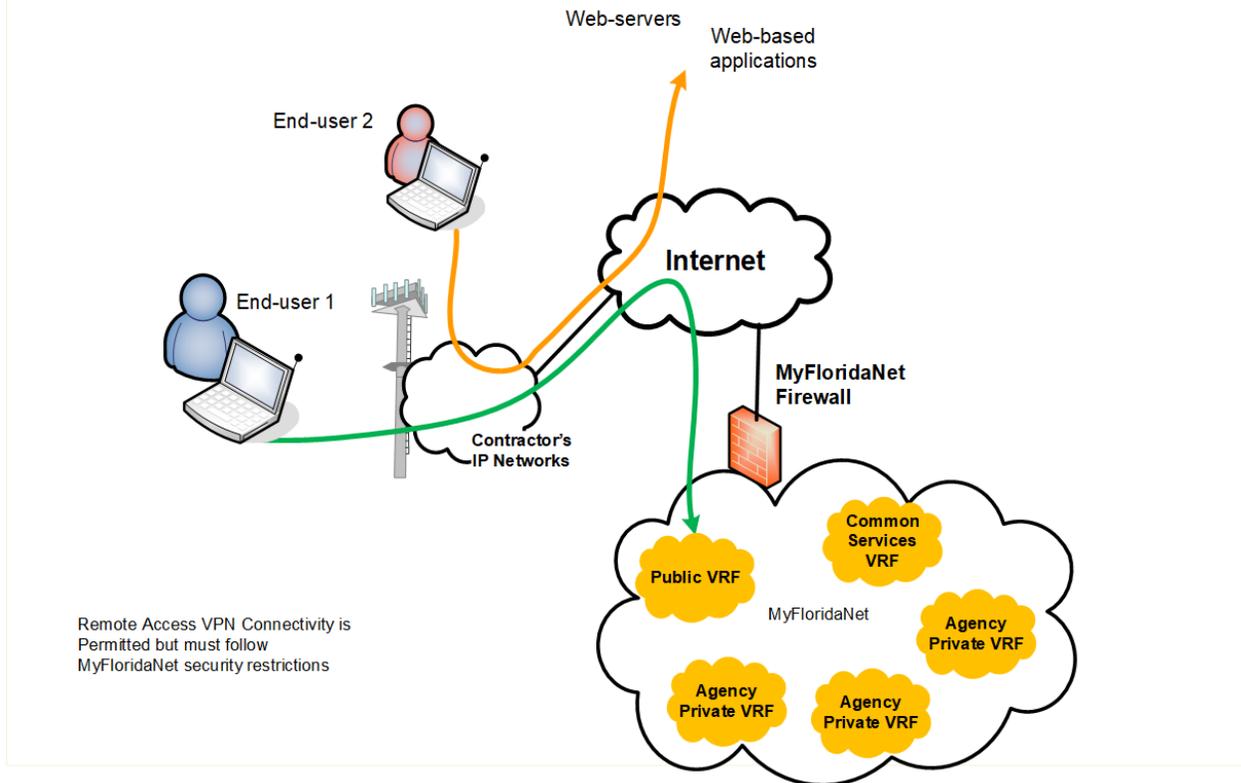
This subsection is applicable to only Wireless Data Services.

Customers can have their traffic sent directly to the internet. Routing wireless traffic direct to the internet provides simplicity for connectivity to web-servers and web-based applications. Sending traffic to the internet also permits Customers to use encrypted VPN traffic to access their IP networks via a Public VRF connection.

For this connectivity, the Contractor is not responsible for the reliability of traffic within the internet.

Routing Wireless Traffic Directly to the Internet

Figure 6



The Contractor is not required to create closed user groups for Customers that have their traffic routed directly to the internet. Under this option, the Contractor is not required to permanently assign the same IP address to a particular wireless device.

When MCS traffic is routed directly to the internet, if the MCS Customer is not an MFN Customer, they do not have to comply with DMS security policy restrictions for traffic to MFN. The Contractor must comply with DMS security policies and those policies of the OEUs. Specifics of the DMS security policy requirements will be detailed in the post-Contract engineering meetings and may vary during the life of the Contract.

A synopsis of the MFN security policy. MFN Customers must access the internet via the MFN firewall and avoid using an alternate internet access that might create a backdoor into MFN. Under certain restrictions, MFN security policy permits MFN Customers to use remote-access VPN connectivity to gain access to their MFN intranet network. The Contractor is not responsible for the specifics of how Customers configure their VPN connectivity.

No response required. By submitting a Reply, Respondent has read and understands the statements contained in this subsection.

3.9 Wireless Data Service - Test Plan

This subsection is applicable to only Wireless Data Services.

The Contractor is responsible for on-going testing of the WDS's transport system (the interconnection between MCS and MFN) to ensure proper performance. The Contractor is responsible for testing each component, including wireless modems (before and after installation, if requested by the Customer), interconnection, interconnection failover, and closed user group configurations. The Contractor must demonstrate successful interconnection failover for each tunnel between the primary and secondary VPN concentrators as part of the Services Infrastructure Checklist signoff and as required by DMS.

All test plans and actual testing must be coordinated with and approved by DMS and the Customer. The test plan need only cover WDS elements. Once approved by DMS, the plan must be included in the WDS Operations Guides.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.10 State of Florida Coverage

The Contractor shall:

1. Provide the same or better level of coverage as that described in the Contractor's Reply;
2. Maintain up-to-date State coverage maps on its website, accessible to all Customers.
3. Provide service strength with as much 4G/4G LTE or better (5G) service coverage as possible.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing all minimum requirements listed above.
2. Describe the Respondent's State geographic coverage.
3. Demonstrate in detail any future plans for enhancement and expansion of the Contractor's State coverage.
4. Provide a service area State coverage map. The map shall be geographically accurate and drawn to a scale of 1:1,000,000 (1 inch=15.78 miles) or less. The coverage map

shall include, at a minimum, county boundaries, cities, and major highways. Note the decibel (db) level used in maps for the Respondent's acceptable service level.

[Enter the response here as needed to provide a complete response]

3.11 Roaming

This subsection is applicable to both WVS and WDS.

The Contractor must not charge for roaming within the Contractor's nationwide footprint.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.12 Security

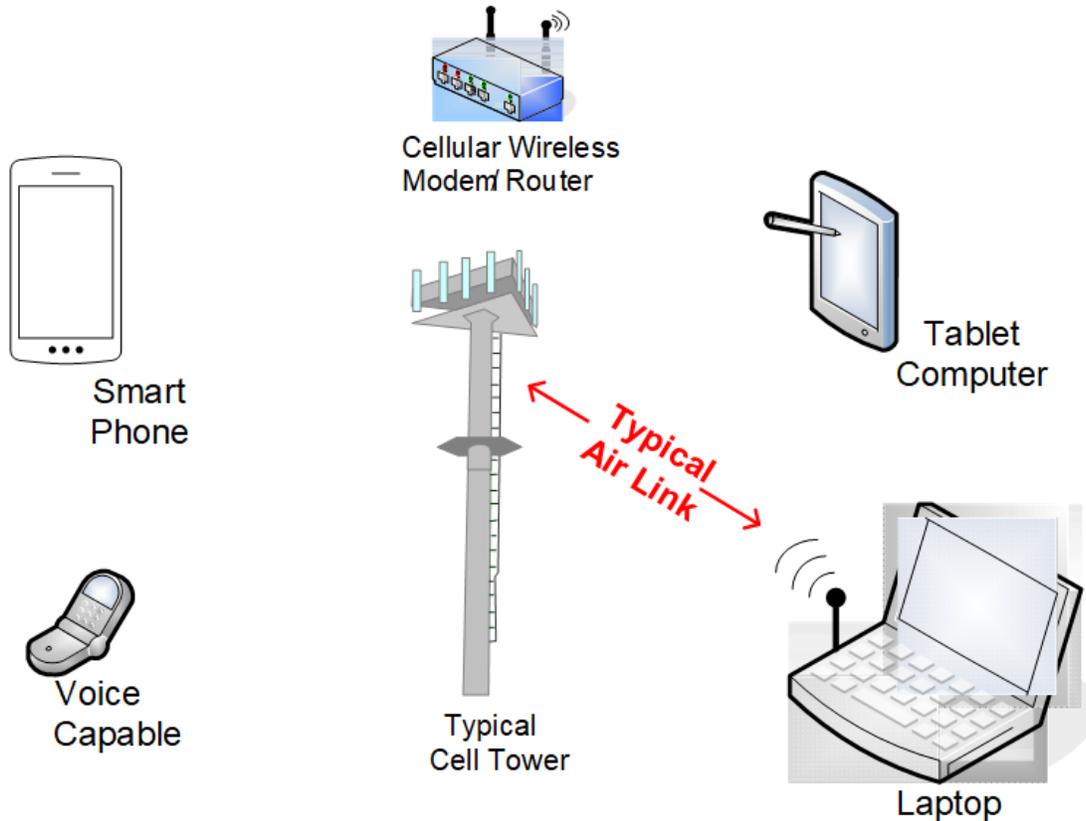
This subsection is applicable to both WVS and WDS.

The Contractor must ensure that all traffic is secured between the Customer's device and the Contractor's antenna/tower (i.e., the air link in Figure 1). Encryption across the air link is not required as long as the traffic transport method provides security equivalent to IPsec 56-bit strength. No wireless traffic transport is permitted that does not meet this minimum traffic transport security requirement.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Security

Figure 1



In addition to the minimum security requirements elsewhere in this SOW, the Contractor must continually enhance its ongoing security features. The Contractor's security features must block unauthorized access into MFN and OEU networks and thwart potential attacks.

The Contractor must maintain physical, electronic, and procedural safeguards to protect the security of its internal systems as well as MFN and OEU networks. The Contractor must secure traffic by employing strong user authentication, making certain only authorized devices connect to the Contractor's wireless network, the MFN network, and OEU networks. The authentication process must associate the End-user to a particular device.

The Contractor must implement internal and external security procedures to guard its networks and applications against unauthorized access. The Contractor will provide DMS a copy of the Contractor's associated security procedures upon request.

The Contractor must perform fraud detection, monitoring, and prevention services consistent with industry common best practices on a 24x7x365 basis to reduce Customer vulnerability to fraudulent activities. Fraudulent calls will be the sole responsibility of the Contractor. DMS and its Customers will bear no responsibility for such calls, including, but not limited to, number theft by cloning, multiple calls at the same time, international calls on an unauthorized telephone, and calls to areas of known fraud. The Contractor shall proactively monitor calling volume and patterns. The Contractor shall immediately report unusual calling volumes and patterns to the Department and Customer, such as usage or cost doubling from the previous month. If fraud is detected outside of normal business hours, the Contractor will notify the Department's Product Manager and Customer via email. Should the Department or Customer declare such activity as fraudulent, the Contractor shall immediately deactivate the service.

Given the statements in this subsection:

1. Describe in detail how the Respondent's proposal will fulfill the minimum requirements of this subsection.

3.13 Reviews of the Contractor's Service

This subsection is applicable to both WVS and WDS.

DMS Test Accounts. Upon request from DMS, the Contractor shall provide up to ten (10) WVS accounts and associated devices (with voice and broadband feature functionality) and up to ten (10) WDS accounts and associated devices to allow DMS to test the Contractor's service. All test devices must be premium (highest functionality) devices. All test accounts and devices must be configured to operate only on the Contractor's network throughout the continental United States. The Contractor must provide the test accounts and devices at no charge and with no limitations on DMS's use of the accounts and devices. DMS will administer the test accounts, including activating, deactivating, and supervising.

Customer Demonstration Reviews. Prior to making an initial order for service, Customers may request, and the Contractor will provide, wireless demonstration equipment (including airtime) for testing. All demo accounts and devices must be configured to operate only on the Contractor's network throughout the continental United States. Demo devices must be provided at no charge for thirty (30) Business Days. The Contractor will post on its portal the step-by-step procedures to obtain the demo devices. The Contractor shall coordinate directly with the Customer regarding demo accounts and devices.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.14 Emergency Services

This subsection is applicable to both WVS and WDS.

The Contractor shall provide emergency services, a crucial aspect of MCS, as described in this section.

3.14.1 911/E911

The Contractor is required to fully comply with federal and State-mandated emergency service requirements, including 911 and E911 services.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.14.2 Department of Homeland Security Programs

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) Emergency Communications Division (the Office) collaborates with the public and private sectors to ensure the national security and emergency preparedness communications community has access to priority telecommunications and restoration services to communicate under all circumstances. The Office manages the Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS), Telecommunications Service Priority (TSP), and Next Generation Network Priority Service (NGN-PS) programs.

The Contractor must participate in at a minimum TSP, GETS, WPS, and NGN-PS in support of the State's emergency preparedness efforts. For additional information see <https://www.dhs.gov/oec-communications-portfolio-management>.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.14.3 Emergency Support Function 2

Background. DMS provides communications assistance during emergencies and disasters. DMS is the lead agency for communications under direction of the Florida Division of Emergency Management. Section 282.702(7), F.S., directs DMS to cooperate with any federal, state, or local emergency management agency in providing for emergency communications services.

DMS is the first point of contact for telecommunications service providers for equipment and services coordination to provide communications support statewide before, during, and after emergencies or disasters. The National Response Framework is part of the United States

National Strategy for Homeland Security, which details fifteen (15) Emergency Support Function Annexes. In Florida, the DMS Emergency Support Function 2 (ESF-2) consists of a dedicated team of telecommunications professionals with expertise in radio systems, voice/data/network communications, and project management.

The Contractor is required to participate in ESF-2 activities and respond to the needs of the State. The Contractor shall deliver the specified quantity (up to 100 of each) of activated wireless (WVS and WDS) devices within twenty-four (24) hours of receiving the ESF-2 request. The devices will be delivered at Contract costs, with the only additional cost being reasonable expedited shipping. The Contractor shall use commercially reasonable efforts to deliver devices to any accessible (officially ordered safe to enter) location within the Contractor's service area as directed by ESF-2.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.
--

3.15 Contractor's Service Delivery Costs

This subsection is applicable to both WVS and WDS.

The Contractor will not charge the Department or Customers for service delivery or infrastructure costs. The Contractor can only charge for services and equipment contemplated in the EUPL, Vendor's Device List, and the Contract.

There will be no costs to activate a service or device. Customers may cancel service at any time without any costs.

The Contractor is financially responsible for its connection to MFN, including, but not limited to, the network-to-network interface, VPN concentrators, circuits, infrastructure components, bandwidth upgrades, equipment, and software.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.
--

3.16 Highly Available and Highly Reliable Design Characteristics

MCS functionality provides support for mission-critical agency Customers. The Contractor shall provide infrastructures, hardware, software, and processes designed to be HA/HR, by, at a minimum:

1. Providing designs to eliminate single points of failure, including minimal convergence times.
2. Utilizing redundant (or backup systems) hardware and software providing continuous availability when a critical component fails or is removed from service for maintenance.
3. Utilizing automated interactions between systems or services to detect when a component has failed.
4. Utilizing multiple physical data paths within an infrastructure to eliminate a potential impact on performance when a path fails or is taken out of service.
5. Utilizing equipment with dual power supplies plugged into separate sources of power, which may include the use of a generator for backup power.
6. Maintaining the entire MCS infrastructure at normal operational functionality and not permitting anything to impact performance, regardless of cause.

Given the statements in this subsection:

2. Describe in detail the proposed offering for this subsection, addressing the design objectives listed above.
3. Describe how the Respondent will provide validation of their HA/HR design to DMS allowing DMS to perform Contract oversight.

[Enter the response here - 500 words]

3.17 Reports, Updates, and Notifications Requirements

This subsection is applicable to both WVS and WDS.

DMS requires the following reports and data, at a minimum, to accomplish Contract oversight:

1. The Contractor shall provide reports, updates, and notifications in accordance with the following section and subsections of this SOW:
 - a. Monthly SLA Compliance Report, SLA-B3 (Subsection 3.18.5)
 - b. Monthly Escalation Activity Report, SLA-B4 (Subsection 3.19.1)
 - c. Quarterly Zero Usage Report, SLA-B5 (Subsection 3.19.2)
 - d. Escalation Procedure and Escalation Procedure Updates, SLA-B6 (Subsection 3.19.3)
 - e. Maintenance Notifications, SLA B7, B8, B9 (Subsection 3.19.4)
 - f. Weekly Transition Status Reports during Transition (Subsection 3.24)
 - g. Project Management Tracking Log, SLA-D9 (Subsection 3.26.2.2)
 - h. Project Status Report, SLA-D10 (Subsection 3.26.2.3)
 - i. Incumbent Contractor Weekly Migration Report, SLA-D14 (Subsection 3.26.5)
 - j. Non-incumbent Contractor Weekly Migration Report, SLA-D15 (Subsection 3.26.5)

- k. Monthly Public Safety Service Plans and Devices Report, SLA-E1 (Section 4)
- l. Direct-Billed Accounts Monthly Report, SLA-G2 (Subsection 6.4)
- m. Direct-Billed Accounts Quarterly Report, SLA-G3 (Subsection 6.5)

2. The Contractor shall provide any of the items below upon request from the Department:
 - a. Identification and validation of products/services and rates;
 - b. Compilation of statistics on products/services from a high level to a detailed level;
 - c. Inventory of devices;
 - d. Services and devices trend information;
 - e. Identification and validation of Contractor's Customer billing (to include all charges, service taxes, surcharges, refunds, and adjustments); and
 - f. Ad hoc reports, which will be at no cost and include a report delivery timeframe within two (2) Business Days of receipt of request.

Given the statements in this subsection:
Describe in detail the proposed offering for this subsection, addressing all minimum requirements listed above.

[Enter the response here – 250 words]

3.18 Service Level Agreement Operational Process

This subsection and all sub-subsections are applicable to both WVS and WDS.

3.18.1 General SLA Requirements

1. The Contractor will pay SLAs by giving the Department a credit in the amount owed. If the last billing cycle of the service, the Contractor will refund the amount due in the form of a check.
2. SLA credits restart each month based on the review process and monthly billing cycle.
3. Unless there is an explicit reference to "business days," all SLA credits are applicable based on calendar days. A calendar day starts at 12:00 AM and ends at 11:59 PM, Eastern Time.
4. All SLA credits are payable to DMS.
5. The billing reconciliation for SLA violations takes place once final determination of SLA credits has been completed.

3.18.2 Reporting and Review

1. Each month, the Contractor, its subcontractors, and DMS participate in a review and scrubbing of all data related to SLAs. Based on this review, credits are developed.

2. DMS is not required to explicitly request or otherwise initiate the SLA review and validation process in order to receive SLA credits.

3.18.3 SLA Holds

1. If time is a factor in the calculation of the SLA, the SLA clock may be suspended, in the Department's discretion, if the Contractor has documented in its ticketing system at least one (1) of the reasons listed below:
 - a. The Customer provided incorrect information in its order, including an incorrect address.
 - b. The Customer did not attend a confirmed scheduled appointment.
 - c. The Customer was unresponsive to calls or emails.
 - d. A site readiness requirement was not fulfilled by the Customer.
2. The SLA clock may also be suspended as identified in Attachment C – Service Level Agreements.
3. The Contractor shall troubleshoot to the fullest extent feasible, whether or not the SLA clock is suspended.

3.18.4 Contractor SLA Accountability

1. SLAs apply regardless of whether the violation was a result of human error, poor engineering design, tardy dispatch, dispatch without required repair or diagnostic tools, exceeding the scope of an approved maintenance change request that causes performance degradation (deterioration in quality, level, or standard of performance of a system, service, feature, or functionality), or any other reason.
2. With the exception of the Contractor's failure to provide the requisite notice (see Section 3.19.4), SLAs will not apply during scheduled upgrade or maintenance windows (including emergency scheduled maintenance). SLAs will apply for all other service element impacts during and after the scheduled maintenance window.
3. DMS will make the final determination on the Contractor's compliance with SLAs.

3.18.5 Compliance Report

1. The Contractor shall deliver a timely and comprehensive SLA Compliance Report on a monthly basis. The Contractor shall provide backup detail (justification) to DMS upon request. Final acceptance of this report is at the sole discretion of the DMS Contract Manager. The report will be provided to the DMS Contract Manager. **Attachment C, SLA-B3**. The SLA Compliance Report must:
 - i. allow DMS to assess performance against measurable service levels;
 - ii. include all SLAs in Attachment C – Service Level Agreements;
 - iii. state "N/A" for SLAs for which no services have been delivered during the Implementation Phase;

- iv. not be locked or password protected;
 - v. include adequate documentation, as determined by the Department, to demonstrate the Contractor's reported monitoring; and
 - vi. be approved by DMS with regard to format, content, and level of detail.
2. If the SLA Compliance Report fails to accurately reflect an SLA violation, additional information may be utilized by the Department in determining SLA compliance in the Department's sole discretion.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.
--

3.19 Customer Support

This subsection is applicable to both WVS and WDS.

The Contractor shall provide the following to the Department's designated recipient(s):

1. Monthly Escalation Activity Reports. This report must be provided on a monthly basis and detail the number of calls and emails related to requests for escalation assistance for technical and administrative support. The format must allow DMS to understand the relative importance of the issues within the escalation queue. Relative importance could be determined by the number of devices impacted or the length of time the Customer has been attempting to obtain a resolution to the issue. The format, content, and level of detail must be approved by DMS. The report will be provided to the DMS Project Manager. **Attachment C, SLA-B4.**
2. Quarterly Zero Usage Reports. This report must include a high-level summary of End-user devices that show no usage (i.e., zero minutes, zero texts, and zero data) for three (3) consecutive months. The format, content, and level of detail must be approved by DMS. The report will be provided to the DMS Project Manager. **Attachment C, SLA-B5.**
3. Escalation Procedure and Escalation Procedure Updates. This procedure must be developed and employed for unresolved network issues, Customer issues, or concerns that are not addressed in a timely manner. The procedure must include names, titles, phone numbers, and email addresses of contacts in the Contractor's escalation chain. The Contractor shall notify the DMS Product Manager in writing of any unresolved issues or issues that have been outstanding for more than ten (10) business days. Escalation procedures are to be updated by the Contractor when either DMS or the Contractor identify the need for an update. **Attachment C, SLA-B6.**
4. Notifications. Notifications must be provided for planned, emergency, and unplanned maintenance. The Contractor shall send an electronic notification which informs DMS of 1) a planned maintenance which may potentially cause a service outage; 2) emergency maintenance when it may cause a service outage and when there is an outage impacting a generalized area; and 3) unplanned maintenance for significant unplanned

maintenance and when there is a significant performance impact over a generalized area. The notification must include an impact statement, date, time, and estimated duration of the maintenance. **Attachment C, SLA-B7, B8, and B9.**

5. Customer Support Team. The Customer Support Team shall address situations on a daily basis that have not been addressed within the customer support processes.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.
2. Describe the process which will allow DMS to support its Customers and End-users with timely notifications.
3. Describe the corporate commitment to providing DMS the information it requires for notifications on significant performance impacts to WVS and WDS.
4. Describe the corporate commitment to providing DMS the necessary Customer Support Team staffing (resources) for escalations to address situations not readily addressed within the operational processes.
5. Describe the use of an escalation procedure related to situations which have not been addressed within the normal customer support processes.

[Enter the response here as needed to provide a complete response]

3.20 Contractor's MCS Portal

This subsection is applicable to both WVS and WDS.

The Contractor shall provide an easy-to-use MCS portal that allows Customers to manage their End-user WVS and WDS devices, device management, and associated services. At a minimum, the portal must allow Customers' designated administrators to view the specifics of and add, change, and cancel devices and services. As changes are made, corresponding billing changes must take place automatically.

The Contractor is responsible for the general content and management of and for hosting the portal. All MCS-specific content must be approved in writing by the DMS Product Manager before publication.

The Contractor's MCS portal must include, at a minimum:

1. service definitions;
2. available features and options;
3. training materials;
4. product support information;
5. ordering procedures;

6. user guides;
7. whitepapers;
8. equipment definitions and specifications;
9. maintenance information;
10. product configuration options;
11. diagrams; and
12. other information approved in writing by the DMS Product Manager.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.

[Enter the response here - As needed to provide a complete response]

3.21 Devices

This subsection is applicable to both WVS and WDS.

The Contractor must provide all applicable software and firmware for each device offered under the Contract and corresponding support. The Contractor must provide a link to the manufacturer's website where Customers can download current software updates/releases and software version release notes. The Contractor must work with the Customer and make a device recommendation based on a case-by-case analysis of the intended use of the device. All devices offered under MCS must be certified by the Contractor to operate with the performance parameters claimed by the manufacturer. The Contractor will remove any device that does not meet the manufacturer's and the Contractor's performance claims from the Vendor's Device List.

1. Excluding activations involving number portability, the Contractor shall ship in-stock devices (including replacement devices) activated, registered, and ready-for-use.
2. If the Contractor is unable to ship in-stock devices, or if a device is out-of-stock, the Contractor must notify the Customer.
3. Account changes made in the MCS portal should be automatic, and account changes made by phone or email should be within one (1) Business Day, with the exception of devices that are out of stock or otherwise unavailable, and excludes account changes involving number portability.
4. Shipping and handling fees are the responsibility of the Contractor, except for emergency and/or expedited orders. During the ordering process, Customers have the ability to approve related expedite fees prior to shipment. Responsibility and liability for loss or damage for all orders shall remain with the Contractor until final inspection and acceptance, when all responsibility shall pass to the Customer.
5. The Contractor shall provide credit and/or replacement for freight-damaged or defective items and replace the items within two (2) Business Days after notification by the

Customer. The Contractor shall provide expedited 24-hour delivery as requested by the Customer for new, replacement, and upgrade devices.

6. The Contractor may invoice the Customer an expedite charge.
7. The Contractor will be responsible for the credit and/or replacement of any freight-damaged or defective products at time of delivery. The Contractor shall not require the Customer to deal directly with the manufacturer. Within five (5) Business Days of a Customer's request, the Contractor shall provide the Customer with a prepaid return label or prepaid self-addressed container suitable for the item's return.
8. The Contractor must accept returns of items shipped in error and credit the Customer for the full amount. Within five (5) Business Days of the Customer's request, the Contractor shall provide the Customer with a prepaid return label or prepaid self-addressed container suitable for returning the item. Delivery of correct items will be at no cost to the Customer.
9. The Contractor shall not impose any restocking fee under any circumstance.
10. Device provisioning errors must be corrected by the Contractor.
11. The Contractor shall not provide salvaged, distressed, outdated, or discontinued merchandise.
12. The Contractor shall obtain and pass through to the Customer any and all warranties obtained or available from the manufacturer/licensor of the cellular product.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing all minimum requirements listed above.

[Enter the response here – 250 words]

3.22 Cooperation with Other Contractors

This subsection is applicable to both WVS and WDS.

The Contractor must fully cooperate with DMS, Customers, and other contractors providing telecommunications services to the State. The Contractor must not commit or permit any act which will interfere with the performance of work by any other Contractor or Customers.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.
2. Describe the corporate commitment to interact and work collaboratively with other Contractors and subcontractors, creating a team of SUNCOM service providers.

[Enter the response here - 100 words]

3.23 Customer Migration

This subsection is applicable to both WVS and WDS.

This subsection addresses the migration to services under this Contract. **Attachment C, SLA-B10.**

The Contractor shall:

1. Provide all reporting activities listed in SOW subsection 3.27.5(1)(b) and SOW subsection 3.27.5(1)(c).
2. Assist as necessary to migrate existing Customers to this Contract.
3. Not charge any non-recurring charges as part of the migration.
4. Not charge for service activations and SIM cards.
5. Provide end-users with the option to maintain their existing cellular device(s) and/or phone number(s) at no charge.
6. Coordinate and communicate with DMS and Customers throughout all aspects of the migration.
7. Complete the migration in one-hundred and twenty (120) calendar days.
 - a. For incumbent Contractors, this commences with DMS acceptance of the Services Infrastructure Checklist and ends when all Customers are identified as either migrated or no longer receiving services from the Contractor.
 - b. For non-incumbent Contractors, this commences with DMS acceptance of the Services Infrastructure Checklist and ends when all Customers identified as purchasing services from the non-incumbent Contractor are migrated.
 - c. Migration does not include new Customers or Customers changing their services after migration.

Given the statements in this subsection:

1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.

[Enter the response here – 1,000 words]

3.24 Transition for Future Iterations of this Service

This subsection is applicable to both WVS and WDS.

This subsection defines requirements associated with the end of the Contract to transition to the replacement contract for future iterations of these services or similar services.

The Contractor shall provide transition duties until all Customer services have been transitioned, migrated, or discontinued and the Contractor has billed Customers their final invoices and resolved all disputed charges.

The Contractor shall develop and implement a transition plan and perform all tasks identified in the plan in a timely manner to mitigate service disruptions (see subsection 3.23).

The Contractor shall participate in meetings with the State, Customers, and other service provider(s) as reasonably required by the State in planning for the transition.

There shall be no additional cost to DMS or Customers for transition activities.

The Contractor shall timely and consistently coordinate and communicate with DMS and Customers, and other service providers, throughout all phases of the transition to ensure an orderly and efficient transition of services to any replacement contract.

The Contractor will be required to perform end-of-service transition activities, which may take place at any time during the Contract term, and end-of-Contract transition services prior to the expiration or termination of the Contract. The full transition of existing services to replacement services and contracts is hereby explicitly made a criterion for completing the Contract Transition Plan.

Upon request by DMS, the Contractor will be required to submit a transition plan for services within sixty (60) days with sufficient detail for DMS's review and approval. DMS reserves the right to request modifications. The plan must include and describe in detail:

1. How the transition will be accomplished in the least disruptive way.
2. The Contractor's commitment to continue to provide services and Contract resources under the existing terms and conditions of the Contract during the transition, including any restrictions and/or limitations.
3. The Customer impact and the Contractor's commitment to minimizing any impact (e.g., business needs, complexity of service, services impacted by special programs, etc.).
4. Identification of tasks dependent upon the State's data or resources.
5. Identification of all Customers by service type and unique product identifier.
6. Plan for transparent transition of services to support the continued billing, collection, and remittance of cost recovery rate for services.
7. Use of industry-accepted project management methodology throughout the transition process.

Overlapping services may be required when transitioning from one large infrastructure to another, and transition may take multiple years to complete. DMS will not be obligated to maintain Contract services for any set number of users or locations during the transition.

The Contractor is required to work with DMS, Customers, and any other DMS contractor as expeditiously as possible in order to transition.

The Contractor agrees to:

1. Cooperate with all entities to ensure an orderly and efficient transition of services. These efforts include taking all necessary steps, measures, and controls to ensure minimal disruption of services during the transition.
2. Maintain staffing levels that are sufficient to handle a smooth, complete, and expedient transition.
3. Transfer all applicable knowledge, including, but not limited to, the devices, software, and third-party Contract services.
4. Provide all data related to the delivery of services, requested by DMS, that is not a tangible or intangible licensed product that existed before Contract work began. The Contractor shall bear the burden of proving existence before Contract work began, including, but not limited to, databases and other repositories of information (for example, operational, user, and administrative information).
5. Upon request, promptly deliver to DMS, whether or not previously made available, all up-to-date guides, manuals, and training materials including operational, user, administrative, and any other guides and procedures the Contractor follows. All documentation created for the purpose of supporting, operating, maintaining, upgrading, and enhancing services, including, but not limited to, design documents and device configurations for services, shall be promptly delivered to DMS upon request, whether or not previously made available.
6. Assist DMS and any other DMS contractor with the planning and installation of any services to facilitate business continuity.
7. Respond promptly and completely to all questions related to the transition.
8. Provide all services and functions necessary for a complete, smooth, and expedient transition.
9. Assist the Department with the installation of network-to-network connections to facilitate continuity for MCS sites. Network-to-network connections will be paid for by the Department.

At the time DMS initiates the transition plan, the Contractor shall provide the DMS Contract Manager a weekly Transition Status Report. The report shall include all impacted Customers. The format, content, and level of detail must be approved by DMS.

After each End-user service transition is completed and the transition status and the billing account status both achieve 100% completion on the Transition Status Report for two (2) consecutive weeks, the Contractor may delete the service line item from the next weekly Transition Status Report.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.
--

3.25 Contractor Meetings with DMS

This subsection is applicable to both WVS and WDS.

This subsection includes requirements applicable to subsections 3.26.1 through to and including 3.26.4.

The Contractor is required to attend all meetings referenced in this section plus ad hoc meetings as DMS deems necessary. Meetings will be held either at the DMS offices in Tallahassee, Florida or virtually. DMS may, at its sole discretion, require the Account Manager and other Contractor's staff attend the meeting in person or allow remote attendance via a mutually agreed-upon conferencing service. For virtual meetings the Contractor will be responsible for providing the video conference call bridge.

For all meetings referenced herein, the Contractor is responsible for the business and administrative tasks associated with the meetings, including, but not limited to, creation of a meeting agenda developed in conjunction with DMS, preparing of any materials, meeting minutes, and other meeting planning efforts. SLA violations include, but are not limited to, inadequate participation of required staff and inadequate preparation. Meeting preparation must include background materials and reports.

3.25.1 Weekly Conference Call

The Contractor shall initially participate in a weekly conference call with DMS to discuss and provide status updates on all open or unresolved issues in the escalation queue. It is the responsibility of the Contractor to coordinate and initiate the call at a time acceptable to the Department's staff. The call frequency is expected to be modified by DMS to monthly or quarterly during the initial Contract term, which is in DMS' sole discretion and dependent on implementation and migration.

3.25.2 Monthly Operational Meetings

The Contractor is required to hold monthly meetings with DMS to review and audit, at a minimum, customer support, escalations, security, and SLA reporting services. These meetings may include, but are not limited to, discussions of the network and all of its services, review of operational concerns, technical updates/changes, SLA Compliance Report, Escalation Activity Report, Direct-Billed Monthly Report, Direct-Billed Quarterly Report, security, policy, design, and administrative topics. While there will be discussions of current and future services, these meetings are not sales meetings. Agendas for these meetings will include operational and administrative items, including, but not limited to, review of operational concerns, reviewing and auditing phone tree accuracy, updates to the staff notification process, and any proposed operational changes.

3.25.3 Project Management Monthly Review Meetings

The Contractor is required to hold monthly meetings with DMS for project management during the Project Implementation Phase. **Attachment SLA-C1**. The Project Implementation Phase

starts with DMS acceptance of a completed Services Infrastructure Checklist. The Contractor will set the agendas for these meetings, which will include, at a minimum, details of the previous period's achievements, the progress on upcoming and existing activities, changes, identified risks and recommendations to mitigate risk, forecasts, project progress, a list of discussion points, and action items with the associated responsible party and due date.

3.25.4 Project Implementation Phase – Project Kickoff Meeting

The Project Kickoff Meeting will take place during the Project Implementation Phase within thirty (30) days of Contract execution. **Attachment SLA-C2**. The agenda for this meeting will include, at a minimum, introductions, review of staffing roles, and review of project scope. The Contractor's Key Required Staff are required to attend the Project Kickoff Meeting.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

3.26 Project Management

This subsection is applicable to both WVS and WDS.

The Contractor must provide project management services in accordance with the DMS regulations set forth in Chapter 74-1, F.A.C., for Project Management.

All Project Management documents must be submitted as either a Microsoft Word 2016 (or higher) document or Adobe pdf. The Project Management Implementation Schedule shall be submitted as a Microsoft Project document. All project management documents will be submitted to the DMS Contract Manager.

The following subsections contain the minimum requirements for MCS Project Management:

3.26.1 Project Management - Project Charter and Project Management Plan

1. The Contractor shall create a Project Charter (see **Attachment C, SLA-D1**). The Project Charter must formally authorize the existence of a project and provide DMS and the Contractor's Project Manager with the authority to apply organizational resources to project activities. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Chapter 74-1, F.A.C.
2. The Contractor shall create a Project Management Plan (see **Attachment C, SLA-D2**). The Project Management Plan must describe how the project is monitored, controlled, and executed. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Chapter 74-1, F.A.C.

The plans listed below are additional components of the Project Management Plan. However, the plans listed below are deliverables separate from the Project Management Plan and subject to final acceptance by DMS.

3. Readiness Plan. (See **Attachment C, SLA-D3.**) The Contractor must deliver a detailed organizational Readiness Plan and associated plans that outline a readiness methodology, approach, activities, dependencies, and assumptions for key stakeholders to successfully support project activities.
4. Communications Management Plan. (See **Attachment C, SLA-D4.**) The Contractor must develop a Communications Management Plan that defines all communication touch points between the Project and all impacted stakeholders. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Chapter 74-1, F.A.C.
5. Risk Management Plan. (See **Attachment C, SLA-D5.**) The Contractor must submit an acceptable Risk Management Plan that defines all potential areas of Customer and Department risk and the related risk strategy.
6. Requirements Management Plan. (See **Attachment C, SLA-D6.**) The Contractor must submit an acceptable Requirements Management Plan. The Contractor is responsible for managing all business requirements, including confirmation, design, development, testing, and validating that they are ultimately met during implementation. The Contractor's Project Manager will work with DMS to develop and administer a plan to effectively manage requirements throughout the Project.
7. Disaster Recovery Plan. (See **Attachment C, SLA-D7.**) The Contractor must deliver a detailed Disaster Recovery Plan and associated plans that outline a disaster recovery methodology, backup procedures, recovery plan, restoration plan, rebuilding process, testing of the disaster recovery plan and record of plan changes. The plan will include the following, at minimum:
 1. Plan Objectives.
 2. Assumptions.
 3. Definition of Disaster.
 4. Recovery Teams.
 5. Team Responsibilities.
 6. Internal and External Communications.
 7. Federal, State, Local Roles and Responsibilities.
 8. Services Restoration.
 9. Support Timeline.

3.26.2 Project Management - Implementation Phase

The Project Implementation Phase starts after DMS acceptance of the Project Charter and ends with DMS acceptance of a completed Services Infrastructure Checklist. Each of the items described in this section is a deliverable that must be submitted to, and accepted by, the DMS Project Manager.

1. Project Management Implementation Phase Schedule. The Contractor shall create a Project Management Implementation Phase Schedule. **Attachment C, SLA-D8**. The document must be baselined, be resource loaded with predecessors, successors, durations, costs, and calculated earned value metrics Cost Performance Index (CPI) and Schedule Performance Index (SPI), and updated every two (2) weeks as needed until the completion of the Project Implementation Phase. This must be accompanied with a narrative which includes the current status of the project, actions that have taken place in the last two (2) weeks, any new risks and their associated risk mitigation plans, any new issues, identification of any tasks more than ten percent (10%) behind schedule, and a plan to complete the task(s).

The Contractor shall create and maintain a Microsoft Project 2016 (or higher) schedule to incorporate all project activities to the agreed-upon work breakdown structure level. The schedule must include, at a minimum, task durations, start and finish dates (baseline and actual), predecessors and successors, resources, deliverables, and milestones, and must calculate CPI and SPI earned value metrics. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Chapter 74-1, F.A.C.

2. Project Management Tracking Logs (Risks, Issues, Action Items, Decisions, and Operational Changes requested). The Contractor shall create Project Management Tracking Logs (tracking logs.) **Attachment C, SLA-D9**. These are updated as necessary, as determined by the Contractor and DMS.

The Contractor must identify, assess, document, and recommend mitigation strategies by updating and submitting to DMS the tracking logs at a minimum of bi-weekly to reduce project risks and issues. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Chapter 74-1, F.A.C.

3. Project Status Report. The Contractor shall create Project Status Reports. **Attachment C, SLA-D10**. The Contractor must provide bi-weekly Project Status Reports, which are due via email to the DMS Contract Manager each Thursday by 5:00 PM Eastern Time, and must include:
 - a. A narrative description of significant project activities that have been conducted or are underway.
 - b. The progress-to-date on project activities.

- c. An explanation of any tasks/activities that are behind-schedule and a plan to bring them current.
- d. Notification of issues or risks that have been encountered and their resolution or plan for future resolution.
- e. Upcoming deadlines.

3.26.3 Project Management - Guides

The Contractor shall create the following guides. These guides are deliverables subject to final acceptance by DMS. The Contractor shall update the guides when necessary as determined by either DMS or the Contractor. **Attachment C, SLA-D11.**

1. WDS and WVS Operations Guides. The Contractor shall create and maintain WDS and WVS Operations Guides describing the operational relationship between the Contractor and DMS. The guides must establish procedures to be followed by the Contractor while delivering services. This includes engineering, operational, and business processes for service delivery. At a minimum, the guides must include ordering, troubleshooting, trouble reporting, service provisioning, SLA monitoring, and invoicing processes.
2. WDS and WVS User Guides. The Contractor shall provide WDS and WVS User Guides that provide a set of instructions for the End-user. The User Guides must also contain device specifications, such as a recommendation of number of simultaneous users that each device can support.

3.26.4 Project Management - Closure

The Contractor shall create project closure documentation. (See **Attachment C, SLA-D12.**) The project closure documentation must include a lessons learned document, final schedule, and retrospective of the project.

3.26.5 Project Management - Implementation Plan and Customer Specific Migration Plans

1. Implementation Plan. The Contractor must submit a detailed Project Implementation Plan to the Contract Manager. (See **Attachment C, SLA-D13.**) The Implementation Plan must address all activities in the Project Implementation Phase, which starts after the acceptance of the Project Charter and ends with DMS acceptance of a completed Services Infrastructure Checklist.
 - a. The Implementation Plan must outline an implementation, approach, activities, dependencies, and assumptions for key stakeholders to support a successful project implementation. The Implementation Plan shall include, at a minimum:
 - i. Schedule of activities, including all Services Infrastructure Checklist Activities.

- ii. Resource allocation.
 - iii. Implementation and migration preparation planning and impact analysis.
 - iv. Network support.
 - v. Operations Centers (operational and security).
 - vi. Day-to-day operational support services.
 - vii. Training – cross reference training section.
 - b. The Contractor shall provide weekly reporting regarding migration. **Attachment C, SLA-D14.** The reporting, which shall exclude any information regarded as Customer Proprietary Network Information (CPNI), should detail the number of current End-users per agency/entity, the progress of migration, and note any End-users that have notified the Contractor they will no longer be using its service. This report shall include details on the Contractor's communication with Customers regarding notification of this Contract and required Customer actions. This report is due to the DMS Contract Manager on a weekly basis, commencing with the completion and DMS acceptance of the Services Infrastructure Checklist and ending when all End-users are identified as either migrated or no longer receiving services from the Contractor. The format, content, and level of detail must be approved by DMS.
 - c. Non-Incumbent Contractors shall provide weekly reporting regarding migration. **Attachment C, SLA-D15.** The reporting, which shall exclude any information regarded as CPNI, should detail the number of End-users identified as purchasing services from the Non-Incumbent Contractor per agency/entity, and the progress of migration. The reporting shall include details on Contractor's communication with Customers regarding notification of this Contract. This report is due to the DMS Contract Manager on a weekly basis, commencing with the completion and DMS acceptance of the Infrastructure Checklist and ending when all End-users identified as purchasing services from the Non-Incumbent Contractor are migrated. The format, content, and level of detail must be approved by DMS.
2. Individual Customer-Specific Migration Plans. The Contractor must submit these plans in accordance with the requirements in this section to DMS and the Customer. **Attachment C, SLA-D16.** The Contractor will be responsible for creating Individual Customer-Specific Migration Plans as each existing and new Customer migrates to MCS, which shall exclude any information regarded as CPNI. Additionally, a migration plan may be required if a Customer undertakes a significant or complex change in how it operates under MCS. These plans will vary based on the proposed service and the complexity of the service migration, but must include, at a minimum:
- i. Schedule of activities, which is consistent with the Project Implementation Phase schedule.
 - ii. Resource allocation.
 - iii. Migration and preparation planning.
 - 1. Impact analysis.

- 2. Stakeholder communications plan.
- iv. Migration management.
- v. Training – cross reference training section.

Given the statements in subsection:

- 1. Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed above.

[Enter the response here - 500 words]

3.27 Project Management - Services Infrastructure Checklist

This subsection is applicable to all Contractors.

The Contractor must complete the Services Infrastructure Checklist provided below in accordance with this subsection and submit the checklist to the DMS Contract Manager and DMS Product Manager. **Attachment C, SLA-D17.** The Contractor will be required to complete a series of readiness activities before DMS accepts services, systems, and processes as ready for production. The Project Implementation Phase will close only when all items on the Services Infrastructure Checklist are complete and accepted by DMS in writing. Upon request, the Contractor will be required to provide DMS any documentation necessary to demonstrate Contractor's compliance with the Services Infrastructure Checklist prior to DMS written approval of the Final Services Infrastructure Checklist. The Contractor shall not deliver any services to Customers until the Project Implementation Phase is closed. The Contractor may engage with Customers for planning purposes before the close of the Project Implementation Phase.

All requirements on the Services Infrastructure Checklist must be fulfilled in accordance with the Contract including, but not limited to, the SOW. Additional requirements may be added to the Services Infrastructure Checklist at the discretion of DMS.

DMS must approve in writing all items listed in the Services Infrastructure Checklist before the Contractor is permitted to charge for any service or device to Customers. The timeline for the Contractor's completion of the Services Infrastructure Checklist will be approved in writing by the DMS Project Manager during development of the project Implementation Plan. Any changes to the Services Infrastructure Checklist, including requirements and timeline, must be approved in writing by the DMS Project Manager, in DMS' sole discretion.

Infrastructure Checklist	
Section Reference	Requirement
SOW Section 2	
2.1 - 2.6	All required key staff positions have been filled with individuals who possess the required minimum qualifications, and the final Staffing Organizational Chart has been approved by DMS.
2.7	The Contractor has demonstrated that its Customer Support Team is staffed and trained.
SOW Section 3	
3.5	Contractor's closed user group isolation method is developed and approved by DMS.
3.6	The Network-to-Network Interface is operational.
3.7	Closed user group traffic successfully mapped into MFN and as permitted is able to access the internet via the MFN firewall.
3.8	MCS traffic is routed directly to the internet.
3.9	A test plan has been finalized, and an interconnection failover for each IPsec tunnel between the primary and secondary VPN concentrators has been successfully tested.
3.12	Security and fraud services are ready for production.
3.13	Processes related to test and demonstration accounts for WVS and WDS are final.
3.14	Emergency services programs are ready for production.
3.16	Design characteristics have been reviewed and are ready for production.
3.17	Reports and reporting options are ready for production.
3.18	SLA processes are ready for production.
2.7 and 3.19	The Customer Support Team is staffed and trained.

3.20	The Contractor's portal is operational.
3.21	The Contractor has provided the link to the manufacture's website. The Contractor has provided its EUPL and Vendor's Device List.
3.26.1 (1)	The Contractor has provided an acceptable Project Charter.
3.26.1 (2)	The Contractor has provided an acceptable Project Management Plan.
3.26.1 (3)	The Contractor has provided an acceptable Readiness Plan.
3.26.1 (4)	The Contractor has provided an acceptable Communications Management Plan.
3.26.1 (5)	The Contractor has provided an acceptable Risk Management Plan.
3.26.1 (6)	The Contractor has provided an acceptable Requirements Management Plan.
3.26.1 (7)	The Contractor has provided an acceptable Disaster Recovery Plan.
3.26.3 (1)	The Contractor has provided the WDS and WVS Operations Guides
3.26.3(2)	The Contractor has provided the WDS and WVS User Guides
3.26.5(1)	The Contractor has provided the Implementation Plan.
SOW Section 4	
4	Public safety services are ready for production.
SOW Section 5	
5.4	The Contractor is ready to implement transactions utilizing the DMS approved method of implementation in CSAB.
5.7	The Contractor has demonstrated the ability to provide CSAB billing account and user management activities.
5.9	The Contractor has demonstrated the ability to maintain a corresponding inventory.
5.10	The Contractor has demonstrated the ability to invoice DMS for all fulfilled orders.
5.11	The Contractor has demonstrated the ability to provide a detailed invoice substantiation file and do so in a mutually agreed upon secured delivery method.

SOW Section 6

6

The Contractor has demonstrated the MFMP Punchout catalogs are ready, and the Contractor is ready to accept orders through MFMP.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

4. Public Safety Service Plans and Devices

The requirements of this Section 4 are only applicable if the Contractor is providing public safety services, as identified in the Contractor's BAFO. If applicable, must adhere to all minimum requirements of this SOW, including those of this subsection.

4.1 Deployable Technologies

The Contractor must have mobile communication units that are deployable technologies. Generally, the Contractor will deploy these mobile communication units during emergency situations to the affected area. The Contractor will install these units during emergencies and may use existing satellite, microwave, or radio systems for backhaul. The Contractor must have a robust regionalized deployable strategy, ensuring that deployable network equipment is available and fully operational, with the required backhaul and/or networking capabilities, throughout the State. The Contractor must coordinate and cooperate with DMS, and any federal, State, or local emergency management agency in providing for emergency communications services, including the Department of Emergency Management, and all other entities that are part of the ESF-2 function.

These deployable technologies are generally characterized as the following:

1. Cell on Wheels: a cellular base station on a trailer with an expandable antenna mast and usually a microwave or satellite link back to the main controller.
2. Cell on Light Truck: A cellular base station on a light truck platform with an expandable antenna mast and usually a microwave or satellite link back to the main controller.
3. System on Wheels: a full base station and controller on a trailer/truck/big rig/etc. This is a fully self-contained cellular system that can provide an island system with no need for satellite/microwave link back; applicability of this type of deployable technology may be limited if there is no internet connectivity.
4. Unmanned Aerial Systems (UAS) and Robotics: Deployable UAS (e.g., drones) in the Class G uncontrolled airspace (400' above ground level), fixed, multi-rotor, and tethered UAS, some of which are capable of providing hot spot and wide-area

coverage. Similar waterborne vehicles include remotely operated vehicle and unmanned underwater vehicle.

5. Other systems: Includes, but is not limited to, vehicular network systems and man-packs.

4.2 Local Control

The Contractor must provide priority and preemption to public safety entities during times of emergency. The priority and preemption will be determined and invoked by the public safety entities through a local control portal. The local control portal shall allow the Customer to enact and deactivate priority and preemption, which shall be controlled by authorized Customers.

The Contractor's public safety service plans and devices must not be throttled during an emergency.

4.3 Local control portal

In addition to the requirements of subsection 3.20 Contractor's MCS Portal, the Contractor shall provide a public safety portal (dashboard). The information held in this dashboard shall include, but is not limited to, the status of the Statewide network and alerts on outages. All features and functionality shall be available to DMS in real-time at all times. The number of DMS dashboard users shall be determined by DMS, and each user shall have a unique log-in and password.

4.4 Public Safety Standards

Public safety service plans and devices shall be in compliance with 3rd Generation Partnership Project Technical Specification 33.180.

The Contractor's public safety service plans and devices must perform to the most recent version of the standards described in TL-9000 Quality Management, ISO 9001, ATIS-100009 Overview of Standards in Support of Emergency Telecommunications Service, ITU-T Y.1271 framework on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks.

4.5 Demonstration Devices

Upon DMS request, in addition to any other test devices required by this SOW, the Contractor shall provide wireless demonstration equipment (including airtime) for use by the Department for the purposes of testing and evaluation at no additional cost. The demonstration equipment shall be made available for a minimum period of sixty (60) Business Days. Any demonstration equipment, forms, and processes shall be provided, managed, and maintained by the Contractor. The Contractor will coordinate directly with any other State agencies regarding public safety service demonstration equipment, notifying the Department in advance of these activities.

4.6 Public Safety Customer Support

The Contractor must provide a dedicated help desk number for support of its public safety service plans and devices.

The Contractor must develop and abide by an escalation procedure specific to public safety real-time network issues and public safety End-user issues. The procedure must include names, titles, phone numbers, and email addresses of contacts in the Contractor's public safety escalation chain. The Contractor shall notify the DMS Product Manager in writing of any unresolved user issues or real-time network issues that have been outstanding for more than ten (10) Business Days.

The Contractor should limit access to the public safety plans to only Customers that are Public Service Entities as recognized by the First Responder Network Authority.

4.7 Public Safety Reporting

The Contractor shall timely provide a monthly Public Safety Service Plans and Devices Report to the Department's Contract Manager. **Attachment C, SLA-E1**. The report shall contain public safety Customer agency, End-user usage, End-user devices, rate plans, and any other related information DMS requires. This report shall not include any information that is considered CPNI. The format, content, and level of detail must be approved by DMS.

4.8 Public Safety Marketing

In addition to any other Customer webpages required by this SOW, the Contractor shall provide specific information on its MCS portal related to its public safety service plans and devices. This should include, at a minimum, information on ordering, devices, apps, service offerings, and accessories.

The Contractor shall provide the Department with a copy of all materials used by Contractor, and its subcontractors, to promote or advertise public safety specific service plans and devices to Florida's public safety user community. The Contractor will submit this information to the DMS Project Manager once per quarter, or as requested by DMS.

Mission critical Push-to-Talk (PTT) devices and services shall not be advertised or marketed to State public safety entities as "mission critical," as defined by the National Public Safety Telecommunications Council (NPSTC), until demonstrated to the Department that the Contractor's PTT is in compliance with NPSTC's requirements, and approved in writing by, the Department.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

5. Business Operations

All services can be direct ordered by the Customers via email, phone call, or the Contractor's MCS portal. The Contractor shall also accept orders through CSAB and MFMP. Billing may be through CSAB or direct billed to the Customer. DMS shall make the final determination on which services are ordered and / or billed through CSAB, MFMP, direct ordered, or direct billed.

This subsection is applicable to DMS-billed services, unless otherwise stated.

5.1 General Description of the SUNCOM Business Model

In accordance with subsection 282.703(2), F.S., DMS has developed a system of equitable billings and charges for Customers. The CSAB system is the ordering, billing, incident management, and inventory system referred to in Chapter 60FF-2, F.A.C., that the Contractor is required to utilize.

When Customers log-in to CSAB, they can perform the following functions:

1. Establish and maintain Customer accounts.
2. Manage billing accounts.
3. View a comprehensive list of available MCS offerings.
4. Place orders.
5. View their complete inventory of services and invoices with associated and detailed charges.

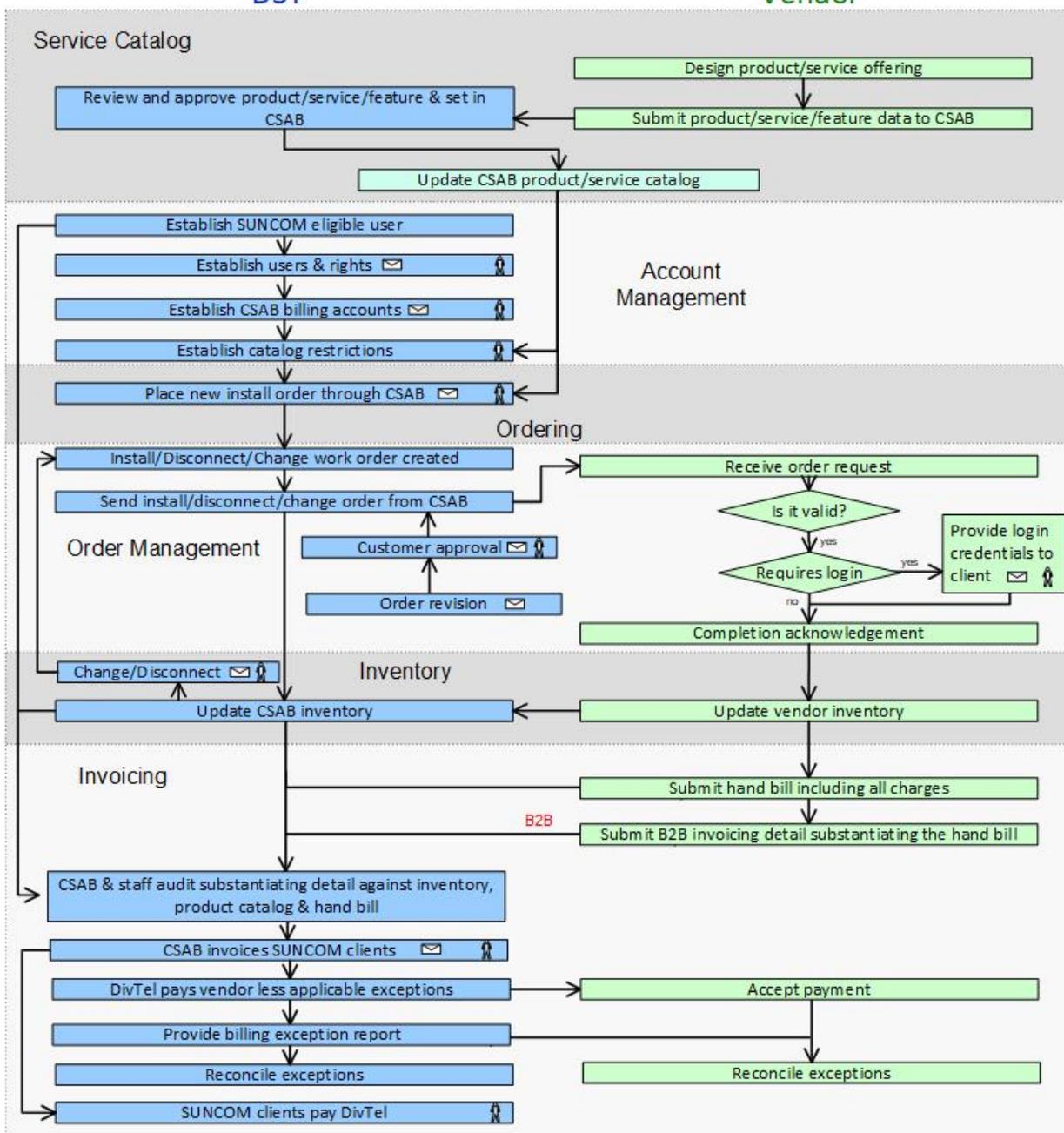
For DMS-billed MCS accounts, the Contractor will bill DMS monthly for services rendered to all Customers and provide DMS with substantiating details in electronic files (for example, comma delimited). The Contractor will include in the substantiating detail charges with unique identifiers for each transaction (for metered services) and service account.

5.2 Communications Service Authorization and Billing Transaction Flowchart

The Contractor will use seven (7) Business-to-Business (B2B) transactions between DMS and Contractor, as depicted on the next page:

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

SUNCOM Steady State Business Process



B2B means a Business to Business electronic messages, batch files and/or Application Program Interfaces (APIs) exchanging all of the electronic data necessary to the transaction. CSAB will provide alternative manual input options to the vendor for low volume transactions, but will not manually input any data on behalf of the vendor.

SUNCOM Client action required SUNCOM Client notified

5.3 Communications Service Authorization and Billing – Official Record

CSAB is the authoritative source of all data. The CSAB system is the official record of the inventory and costs of SUNCOM services, including MCS. If the Contractor claims any inaccuracies in CSAB data, the data will be considered accurate unless substantially proven otherwise, at DMS' sole determination.

The Contractor shall not enable or ask DMS or Customers to input ordering and/or invoicing data into CSAB on behalf of the Contractor.

5.4 Communications Service Authorization and Billing - Interface with Contractor

The Contractor shall use Application Programming Interfaces (APIs) to implement transactions between CSAB and the Contractor. DMS will test and approve the interface prior to Contractor accepting orders for services and devices. The following requirements apply with regard to the Contractor's APIs with CSAB:

1. The Contractor's API enables data transfer between CSAB and the Contractor's system.
2. When data is sent from CSAB, the Contractor's API must send back an acknowledgement to CSAB.
3. The Contractor's API will perform functions automatically at near real-time.
4. The Contractor shall develop and maintain functional crosswalks between the Contractor's system and CSAB, which maps the data elements in CSAB to equivalent data elements in the Contractor's system. The Contractor will also support DMS' efforts to create functional crosswalks.
5. It is the Contractor's responsibility to ensure data has been received by CSAB, including resending data that has not been acknowledged by CSAB.
6. The Contractor shall provide a testing environment for quality assurance, accessible by DMS.

5.4.1 Batch Routines

The second method the Contractor shall utilize to implement transactions with CSAB is through batch routines, which are periodic exchanges of data files containing a large number of records. An example of a batch routine is monthly delivery of invoicing substantiation files (B2B-6), due to the large volume of data.

5.4.2 Manual Review and Data Entry by Contractor Staff

The third method the Contractor may utilize to implement transactions within CSAB is by manual review and data entry. The Contractor can use CSAB screens to view a submitted order from a Customer and mark that order as fulfilled, rather than use B2B-3 and B2B-4 transactions.

The Contractor shall only use manual review and data entry as a method of last resort and only with prior written approval by DMS Contract Manager. The Contractor shall not use manual review and data entry for invoicing substantiation (B2B-6).

5.5 Communications Service Authorization and Billing Service Catalog

MCS services and devices must be approved by DMS and entered into the CSAB Service Catalog prior to making them available for use or purchase by any Customer. DMS will have sole discretion over the CSAB Service Catalog and any updates.

The Contractor shall use the following three (3) types of charges for the billing of MCS services:

1. One-time charge: a single payment for a service or item (e.g., hardware installation).
2. Monthly charge: monthly fixed and recurring charge
3. Metered charge: incremental charge based strictly on usage of the service (e.g., data overage charges).

The Contractor shall comply with the requirements of Chapter 60FF-2, F.A.C., in its use of CSAB.

5.6 Taxes and Government Sanctioned Fees

The Department and Customers do not pay State or federal taxes. Taxes are defined here to include payments that the Contractor is required to collect by law and pay to public entities.

Government-sanctioned surcharges and fees, if the Customer is not exempt, must be collected by the Contractor and may be payable by the State. Any new or modified government-sanctioned surcharge or fee must be provided to DMS for review and approval. If approved, the Contractor can then submit a request to update the CSAB Service Catalog.

The standard process whereby the Contractor submits a request for inclusion of services in the CSAB Service Catalog and DMS approves them must be implemented for a new or modified surcharge or fee with the following additional requirements:

1. The catalog item must be tagged as a government-sanctioned surcharge or fee.
2. The description field provided by the Contractor must clearly identify the surcharge or fee.
3. The Contractor must provide the DMS Contract Manager with information sufficient for DMS to develop formulas that replicate the charges through calculations against invoicing substantiation data. The DMS Product Manager will approve the Contractor request if the update to the CSAB Service Catalog is in accord with the amendment.
4. The surcharge or fee must be billed at the inventory ID level and not billed as a lump sum.
5. The Contractor must give DMS advance notification of anticipated surcharge or fee changes with the DMS-approved effective date the charges will be incurred and the amount/percentage.

Non-government sanctioned surcharges and fees, such as activation fees and termination fees, are not chargeable under this Contract.

5.7 User Access Privileges for the Contractor

The Contractor's user CSAB access privileges must be approved and monitored by a Contractor-assigned CSAB Administrator. User access privileges allow the following functions:

1. Manually receive and closeout orders to the Contractor.
2. Review past orders submitted to the Contractor.
3. Review a robust set of inventory data for services provided by the Contractor.
4. Other access as allowed by DMS.

DMS reserves the right to terminate CSAB user access privileges of any Contractor staff without cause or notice.

5.8 Work Orders

Customer work orders are sent to the Contractor as B2B-3 transactions. The Contractor can log-in to CSAB as prompted by a CSAB email to see submitted orders. The Contractor is required to respond to the Customer with distinct B2B-4 fulfillment data for each item, or service, in a work order. Multiple item orders with only a single order number are not fulfilled until every item is delivered.

Some key data elements in addition to CSAB-assigned Inventory ID are:

1. Order ID – identifies a request for one (1) or more items. This ID is associated with everything in a “shopping cart” when a Customer “checks-out.”
2. Work Order ID – is associated with each item request within an order that can be fulfilled separately from the rest of the order and requests action for one (1) Service Installation ID.
3. Installed Option ID – identifies the service, feature, or hardware from the CSAB Service Catalog that was requested in the work order.
4. Service Installation ID – identifies the service account resulting from order fulfillment. It is the unique inventory entry in CSAB and is equivalent to, but not the same as, distinct IDs used by Contractor to track status, usage and charges (e.g., circuit ID, phone number, hardware serial number, etc.).

The Contractor is required to provide all of the required fulfillment data in CSAB.

The Contractor shall not charge the Department for any orders from which key fields data, installation dates, or disconnect dates are missing or incorrect. The effective bill date cannot be more than forty-five (45) days from the date the order is closed. **Attachment C, SLA-G1.**

Some orders will include configuration data, including IP addresses, to enable establishing closed user groups on MFN.

5.9 Inventory

Every order, and many other actions related to MCS services, is permanently logged into CSAB. This inventory is a basis for DMS audits of Contractor charges; i.e., if a billed service is not in the inventory or the inventory shows it was not active during the invoicing period, DMS will dispute the charge. The CSAB inventory is also a useful tool for DMS, Customers, and Contractor to see what has been ordered, its status, location, cost, any associated comments, etc.

CSAB inventory is structured around key data elements. Inventory records are not valid without these key fields. CSAB by default has primacy when there are discrepancies between the inventories of the Contractor and CSAB.

The Contractor is required to maintain a corresponding inventory as a basis for invoicing DMS. Periodic reconciliation may be implemented between CSAB and the Contractor's inventory through B2B-5 transactions, at DMS' sole discretion. This will avoid waiting until the Contractor invoices DMS to discover these inconsistencies and having to resolve them through billing disputes. DMS will provide for an exchange of inventory data throughout the month using transaction B2B-4. There is no manual substitute for this process.

5.10 Invoicing Requirements

The Contractor will invoice DMS for all fulfilled orders based on a calendar month with invoices and electronic details submitted to DMS. **Attachment C, SLA-F1**. Invoices to DMS will consist of: 1) invoices for payment on an unchangeable format (e.g., paper) that reflect the total wholesale charges for the month (referred to herein as a, "handbill"), and 2) electronic detail files that substantiate all billable services. The total of substantiated detail charges must match the payment requests on each of the handbills. All credits due must be reflected on the invoice related to the first available billing cycle after the credit has been determined. Both the handbill and electronic files for the CSAB portion must be received no later than the 10th calendar day of each month.

5.11 Electronic Substantiating Detail File

The invoice substantiation file consists of electronic detail listing all billable services and activities with all unique IDs necessary to be auditable bases for all charges. The detail file must include all charge data on one-time purchases, active service periods, and incremental activities. All charges must be attributable to distinct identifiers for the services as negotiated in the CSAB Service Catalog, and each discrete charge must be distinguished by a service identifier. Metered charges must also include date/time stamps for each billing event and the dates of the billing cycle (start

and end). The file must be provided to DMS using a mutually agreed-upon, secured delivery method, and mutually agreed-upon format.

5.12 Audit of Contractor Invoices

DMS will audit invoices to validate all charges against the current inventory of provided services and the prices associated with the CSAB Service Catalog. If the electronic substantiating detail provided by the Contractor contains some errors but: a) is complete (i.e., contains all of the required data elements); b) substantially corresponds with the CSAB inventory and CSAB Service Catalog; and c) matches the handbill, then DMS will send an audit exception report (B2B-7) to the Contractor detailing any disputed charges. At this time, this is a manual process. At any time during the Contract term, this may become an electronic process, at DMS' sole discretion. DMS staff will request credits/debits for any audit exceptions on the current invoice and work with Contractor staff to reconcile charges and system data to resolve the exceptions within one (1) billing cycle from receipt of dispute. If Contractor has not resolved audit exceptions within one (1) billing cycle, the charges will be adjusted as determined by DMS.

5.13 Mandatory Interface with the Contractor

All work orders will be submitted to the Contractor via CSAB or similar system as deployed by DMS. Direct billed Customers will interface solely with the Contractor.

5.14 Properly Authorized Work Orders

No WDS will be provisioned unless the Contractor has a properly authorized work order submitted by DMS through CSAB. Direct billed Customers will interface solely with the Contractor.

5.15 General Billing Requirements

The Contractor will maintain a detailed database that uniquely identifies each pricing component. The CSAB Service Catalog contains unit prices and all qualifiers that are applied to unit prices in order to create an unambiguous database of WDS billable line items. A specific billing code shall have only one (1) unit amount.

5.16 Billing Start

The Contractor shall meet the following criteria to complete billing starts:

1. All bills should commence on the 1st and run through the end of the month based on the completion date. Fractional charges are based on the effective bill date.
2. The Contractor cannot retroactively bill for services received before the, the start date of a Purchase Order in MFMP, or is otherwise ordered by the Customer.

No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this section.

6. Direct Ordering and Billing

This section is applicable to WVS and certain approved WDS items.

The Department has no obligation to assume payable commitments on behalf of SUNCOM or SUNCOM Customers in instances where a vendor or SUNCOM Contractor submitted an invoice directly to a SUNCOM Customer.

The Contractor will accept orders from Customers for all WVS devices, rate plans, and services through MFMP. All direct-billing will be done in accordance with Rule 60FF-2.007, F.A.C. The Contractor will cooperate with the Department and MFMP (and any authorized agent or successor entity to MFMP) to deliver direct-billed WVS devices, rate plans, and services.

The Contractor will work in cooperation with the MFMP vendor. All items available for purchase by any Customer that are listed on the most recent DMS-approved EUPL will be exhibited on the MFMP website as a Punchout catalog for Customers. The MFMP Punchout catalog shall be updated by the Contractor within one (1) Business Day of any updated EUPLs being posted on the Department's website. By acceptance of an MFMP purchase order, the Contractor agrees to all MFMP terms and conditions.

6.1 Services and Devices Sold to Direct-Billed Customers

The Contractor will not make any service or device available to any Customer that has not been approved by DMS. If a new service or device is approved, the Department will add the service or device to the EUPL and provide a SUNCOM price for the Contractor to market to Customers. The Contractor shall not display or represent any other prices to Customers.

6.2 Cost Recovery Rate

The Contractor will charge Customers the established rates, plus the SUNCOM Cost Recovery Rate (CRR). The CRR will be included on all monthly-recurring Contractor's charges and invoices.

The Department will be responsible for providing notification regarding the CRR to Customers. The Department will provide: i) notification on the MFMP website Punchout catalog, and ii) notification in a mutually agreeable format for OEUs not currently ordering through the MFMP website Punchout catalog.

The Contractor shall provide the Department with the CRR on all services sold to Customers that are direct-billed. The CRR will be assessed on the monthly recurring charges after all discounts, adjustments, and credits are taken into account. Additional charges, including but not limited to devices, taxes, surcharges, or regulatory fees, will not be included in the assessment of the CRR.

The Department may modify the CRR through a written amendment to the Contract with ninety (90) days prior written notice to the Contractor. If mutually agreed upon, modifications to the CRR may take effect earlier than the ninety (90) days.

The CRR will be the same for all Contractors providing MCS. In the event that the Department authorizes a Contractor to collect a lower CRR than on this Contract, the Department will incorporate the lower CRR into this Contract via amendment. The Contractor shall have sixty (60) calendar days after the amendment effective date to charge the CRR on the direct-billed invoices.

The Contractor will remit all funds collected pursuant to the CRR to the Department in the form of a quarterly check. The check will be accompanied with a complete Direct-Billed Quarterly Report. The check will be sent no more than forty-five (45) days after the end of the calendar quarter to cover the cost recovery amounts collected for the previous quarter. **Attachment C, SLA-G1.**

Fees collected for the CRR will be thirty (30) days in arrears after the billing month in which the charges are invoiced on the direct-billed invoice. The Contractor will be required to remit funds associated with this requirement only when payment has been collected from the Customers that are direct-billed under this Contract.

6.3 Contract Association on Direct-Billed Accounts

All direct-billed accounts established with Customers will include a corporate identifier for this Contract assigned by the Contractor in the billing system.

6.4 Monthly Reporting of Direct-Billed Accounts

The Contractor will provide reporting and auditing in accordance with Rule 60FF-2.005, F.A.C. Additionally, the Contractor will provide the Department with an accurate Direct-Billed Monthly Report in an Excel format via e-mail of all direct-billed accounts including, but not limited to: the Customer's billing account name, Customer corporate identifier, number of active lines, total amount of charges, and billing month. **Attachment C, SLA-G2.** This report will substantiate quarterly payments remitted to the Department. In the event a discrepancy is cited, the Contractor will have thirty (30) days from the date of bill close to provide the Department with the data necessary to reconcile the discrepancy. In the event the Contractor cannot substantiate the cited discrepancy, the Contractor will be responsible for payment of the disputed amount within thirty (30) days. Online reporting and auditing via the Contractor's portal may be appropriate, if it meets the requirements of this subsection and the reporting can be exported and saved by the Department. The format of the report is subject to DMS final approval.

6.5 Quarterly Reporting of Direct-Billed Accounts

On a quarterly basis, the Contractor will provide the Department a Direct-Billed Quarterly Report that aggregates utilization monthly reporting. **Attachment C, SLA-G3**. The report requirements are as follows:

1. The report must be in an Excel format sent via e-mail of all direct-billed accounts, which will include the Customers' aggregate utilization (minutes, data, and text) and billed amount by device type and billing month.
2. The report must contain information sufficient for the Department to independently verify and validate by Customer the utilization and billed amount by device type and billed amount and the cost recovery due to the Department.
3. The aggregate utilization reporting will not identify CPNI, such as but not limited to account names, subscriber number, or End-user level information for direct-billed Customers.
4. Online reporting and auditing via the Contractor's portal may be appropriate if it meets the requirements of this subsection and the reporting can be exported and saved by the Department.
5. The format of the report is subject to DMS final approval.

6.6 Customers Liability

Direct-billed Customers are solely liable for any performance, duties, payments, and responsibilities generated by their use of this Contract, fiscal or otherwise. As stated in Rule 60FF-2.007(3), F.A.C., "the Department has no obligation to assume payable commitments on behalf of SUNCOM or SUNCOM [Customers] in instances where a vendor or SUNCOM Provider submitted an invoice directly to SUNCOM [Customers]."

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.