



Office of the Secretary  
4050 Esplanade Way  
Tallahassee, FL 32399-0950  
850-488-2786

**Ron DeSantis, Governor**

---

**CONTRACT**  
**FOR**  
**MOBILE COMMUNICATION SERVICES**  
**CONTRACT NO: DMS-19/20-006C**  
**BETWEEN**  
**THE STATE OF FLORIDA**  
**DEPARTMENT OF MANAGEMENT SERVICES**  
**AND**  
**CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS**

# CONTRACT

## Table of Contents:

SECTION 1. CONTRACT TERM AND TERMINATION.....	3
SECTION 2. CONTRACT DOCUMENTS AND HIERACHY .....	4
SECTION 3. PAYMENT AND FEES .....	5
SECTION 4. CONTRACT ADMINISTRATION .....	7
SECTION 5. CONTRACT MANAGEMENT .....	9
SECTION 6. COMPLIANCE WITH LAWS.....	10
SECTION 7. WORKERS' COMPENSATION, GENERAL LIABILITY INSURANCE, INDEMNIFICATION, AND LIMITATION OF LIABILITY .....	12
SECTION 8. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY .....	14
SECTION 9. DATA SECURITY REQUIREMENTS .....	15
SECTION 10. GRATUITIES AND LOBBYING .....	18
SECTION 11. CONTRACT MONITORING .....	19
SECTION 12. CONTRACT AUDITS .....	20
SECTION 13. BACKGROUND SCREENING AND SECURITY.....	21
SECTION 14. COMMUNICATIONS AND CONFIDENTIALITY .....	23
SECTION 15. LICENSING .....	24
SECTION 16. PERFORMANCE BOND .....	25
SECTION 17. CUSTOMER OF RECORD.....	25
SECTION 18. SPECIFIC APPROPRIATION.....	25
SECTION 19. MISCELLANEOUS.....	26

## Exhibits:

- Attachment A – Definitions and Acronyms
- Attachment B – Final Statement of Work
- Attachment C – Final Service Level Agreements;
- Attachment D – Contractor's Pricing, including:
  - Exhibit 1 to Attachment D – Vendor's Services and Discounts Pricing
  - Exhibit 2 to Attachment D – Vendor's Device List
- Attachment E – Instructional Document for Request for Best and Final Offer to ITN DMS-19/20-006
- Attachment F – ITN DMS-19/20-006

## **CONTRACT**

This Contract is between the STATE OF FLORIDA, DEPARTMENT OF MANAGEMENT SERVICES (Department), an agency of the State of Florida with offices at 4050 Esplanade Way, Tallahassee, Florida 32399-0950, and Cellco Partnership d/b/a Verizon Wireless (Contractor) with offices at 4075 Esplanade Way, Suite 226, Tallahassee, FL 32399, each a "Party" and collectively referred to herein as the "Parties." The terms "Party" and "Parties" are defined as provided in this paragraph whether capitalized or not, unless stated otherwise.

The Parties enter into this Contract (Contract) in accordance with Chapters 282 and 287, Florida Statutes (F.S.), and with the negotiated terms and conditions of Invitation to Negotiate, DMS-19/20-006, Mobile Communication Services.

### **SECTION 1. CONTRACT TERM AND TERMINATION**

#### **1.1 Initial Term**

The initial term of the Contract will be five (5) years and will begin on the date the Contract is signed by all Parties.

#### **1.2 Renewal**

Upon written agreement, the Department and the Contractor may renew the Contract, in whole or in part, for up to five (5) renewal years in accordance with section 287.057(13), F.S., and Rule 60A-1.048, Florida Administrative Code (F.A.C.).

#### **1.3 Suspension of Work and Termination**

##### **1.3.1 Suspension of Work**

The Department may, at its sole discretion, suspend any or all activities under the Contract, at any time, when it is in the best interest of the State of Florida to do so. The Department may, at its sole discretion, suspend the Contract at any time, when in the best interest of the Department or Customer, as defined in Attachment A, Definitions and Acronyms, to do so. The Department will provide the Contractor written notice outlining the particulars of suspension and the effective date of the suspension. After receiving a suspension notice, the Contractor must comply with the notice and will cease the specified activities associated with the Contract. Notwithstanding the foregoing, the suspension of wireless services under the Contract is limited to two (2) ninety (90) day periods (a total of 180 days) per twelve (12) month period. Within ninety (90) days, or any longer period agreed to by the Contractor, the Department will either (1) issue a notice authorizing resumption of work, at which time activity will resume, or (2) terminate the Contract for convenience. If the Department fails to provide notice in accordance with this section, suspended lines will be automatically restored to active billing status on the 91<sup>st</sup> day following each suspension period. Suspension of work will not entitle the Contractor to any additional compensation. However, the Customer will remain responsible to compensate Contractor for services ordered and delivered under the terms of this Contract through the date of termination. For the avoidance of doubt, the Contractor will not be compensated for any suspended services during the time of suspension.

### **1.3.2 Termination for Convenience**

The Contract may be terminated by the Department in whole or in part at any time, when, at the sole discretion of the Department, it is deemed to be in the best interest of the State of Florida to do so. The Department shall provide Contractor thirty (30) days' advanced written notice of such termination. If the Contract is terminated before performance is completed, the Contractor will be paid only for that work satisfactorily performed, prior to the termination, for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Contract price as the amount of work satisfactorily performed. All work in progress will become the property of the Customer and will be turned over promptly by the Contractor.

### **1.3.3 Termination for Cause**

If the performance of the Contractor is not in compliance with the Contract requirements the Department may, at its sole discretion, (a) terminate the Contract pursuant to Rule 60A-1.006, F.A.C, by notifying the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified timeframe, which shall generally not be less than thirty (30) days from such notice, or (b) take other action deemed appropriate by the Department.

### **1.3.4 Termination Assistance**

In case of termination, whether for cause or for convenience, the Contractor will provide prompt and thorough transition assistance and cooperation, including as specified in Subsection 3.24, Transition for Future Iterations of this Service, of the Statement of Work (SOW).

## **SECTION 2. CONTRACT DOCUMENTS AND HIERACHY**

The Contract including any exhibits referred to herein, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral, with respect to such subject matter. The Contract consists of the documents listed below, and in the event any of these documents conflict, the conflict will be resolved in the following order of priority (highest to lowest):

1. This Final Contract document;
2. Attachment A – Definitions and Acronyms;
3. Attachment B – Final Statement of Work
4. Attachment C – Final Service Level Agreements;
5. Attachment D – Contractor's Pricing, which consists of:
  - a. Exhibit 1 – Vendor's Services and Discounts Pricing (i.e., End-User Price List)
  - b. Exhibit 2 – Vendor's Device List
6. Attachment E – Instructional Document for Request for Best and Final Offer to ITN DMS-19/20-006; and
7. Attachment F – ITN DMS-19/20-006.

In accordance with Rule 60A-1.002(7), F.A.C., Form PUR 1000, is included herein by reference but is superseded in its entirety by the Contract.

## **SECTION 3. PAYMENT AND FEES**

### **3.1 Price Adjustments**

Pricing may be updated in accordance with SOW Section 1.5, Update Process to End User Price Lists and Vendor's Equipment List.

### **3.2 Price Decreases**

During the term of the Contract (including renewal years), the Department encourages the Contractor to offer price decreases that are in line with increased efficiencies and added infrastructure enhancements. The Department reserves the right to further negotiate reduction in pricing for the renewal years. The following additional price decrease terms apply:

#### **3.2.1 Volume Discounts**

Contractor may offer additional discounts for one-time delivery of large single orders.

#### **3.2.2 Competitive Pricing**

The Parties agree to review on an annual basis the competitiveness of the prices stated in the Contractor's most recent EUPL for services, features and devices by comparing the combined pricing for all services, features and devices provided under this Contract to the combined pricing charged by Contractor to any similarly situated United States State government customer for a mix of services, features and devices substantially similar in scope and volume to those provided under this Contract, taking into account the particular characteristics of both contracts such as performance standards, pricing terms, and contract terms and conditions. If after review the Parties determine that such similarly situated customer of the Contractor is receiving services, features and devices from the Contractor at a combined price below the pricing on the Contractor's current EUPL, the Contractor shall submit an updated EUPL with revised lower pricing; except that Contractor will have no obligation to amend pricing to the extent that the combined price difference results from services, features and devices provided by third parties, unless and to the extent that Contractor can obtain reduced pricing from such third parties using reasonable efforts. In connection with the review described in this Section 3.2.2, Contractor has no obligation to provide DMS with Contractor's or its subcontractors' or suppliers' trade secrets or confidential information not otherwise required to be provided under this Contract.

#### **3.2.3 Sales Promotions**

In addition to decreasing prices for the balance of the Contract term due to a change in market conditions, Contractor may conduct sales promotions involving price reductions for a specified lesser period provided the Customer meets all qualifications of the promotion. Contractor must submit documentation to the Customer and to the Department identifying the proposed (1) starting and ending dates of the promotion, (2) commodities or contractual services involved, and (3) promotional prices.

### **3.3 Purchase Orders and Communication Service Authorizations**

A Customer may use Purchase Orders (POs) issued through MyFloridaMarketPlace (MFMP) or Purchase Orders issued through the Communications Services Authorization and Billing (CSAB) system (known as Communication Service Authorizations (CSAs) to buy commodities or services. The Department may also issue POs or CSAs on behalf of Customers. The Contractor must provide commodities or services pursuant to POs or CSAs. The PO or CSA period of performance survives the expiration of the Contract. All terms and conditions of the Contract will be incorporated into the PO or CSA and will survive the termination of the Contract. The duration of POs or CSAs must not exceed the expiration of the Contract by more than twelve (12) months, unless they have been entered into pursuant to an Extended Pricing Plan, in which case they may not exceed the expiration of the Contract by more than thirty-six (36) months. Extended Pricing Plans are discounted prices offered in exchange for a Customer's commitment to lease commodities or purchase contractual services for an extended time. Requested terms and conditions may be added to the PO, subject to negotiation between the Customer and Contractor.

### **3.4 Payment Invoicing**

Payment will be made in accordance with section 215.422, F.S. The Contractor will be paid upon submittal of an invoice to the Department, or Customer if direct billed, after delivery and acceptance of commodities or contractual services is confirmed and the invoice is accepted by the Customer. The Contractor shall submit invoices for fees or other compensation for services or expenses in sufficient detail for a proper pre-audit and post-audit, and electronic invoices should include the Contract number and the Contractor's Federal Employer Identification Number. The Department reserves the right to request additional documentation as needed, and Contractor will follow all invoice directives in the SOW and this Contract document.

Contractor shall identify/flag all State agency Customer accounts as "Government Accounts" for which service will not be interrupted due to an outstanding balance, disputed amount owed, or late payments due without prior receipt of a written notice of nonpayment, three (3) contact attempts, and a minimum sixty-one (61) day period after payment due date for State agency Customers to cure a payment default.

### **3.5 Travel**

Travel expenses are not reimbursable unless specifically authorized by the Customer in writing and, if authorized, may be reimbursed only in accordance with section 112.061, F.S.

### **3.6 Annual Appropriation**

Pursuant to section 287.0582, F.S., the Department's performance and obligation to pay under the Contract is contingent upon an annual appropriation by the Legislature.

### **3.7 MyFloridaMarketPlace Transaction Fee**

The State of Florida, through the Department, has instituted MFMP, a statewide eProcurement system. Pursuant to section 287.057(22), F.S., all payments issued by Customers to the Contractor for purchases of commodities or contractual services will be assessed a Transaction Fee as prescribed by Rule 60A-1.031, F.A.C., or as may otherwise be established by law, which the Contractor shall pay to the State.

For payments within the State of Florida accounting system (FLAIR or its successor), the Transaction Fee shall, when possible, be automatically deducted from payments to the

Contractor. If automatic deduction is not possible, the Contractor shall pay the Transaction Fee pursuant to subsection (2) of Rule 60A-1.031, F.A.C. By submission of these reports and corresponding payments, the Contractor certifies their correctness. All such reports and payments shall be subject to audit by the State of Florida or its designee.

The Contractor shall receive a credit for any Transaction Fee paid by the Contractor for the purchase of any item(s) if such item(s) are returned to the Contractor through no fault, act, or omission of the Contractor. Notwithstanding the foregoing, a Transaction Fee is non-refundable when an item is rejected or returned, or declined, due to the Contractor's failure to perform or comply with specifications or requirements of the agreement.

Failure to comply with these requirements shall constitute grounds for declaring the Contractor in breach. VENDORS DELINQUENT IN PAYING TRANSACTION FEES SHALL BE EXCLUDED FROM CONDUCTING FUTURE BUSINESS WITH THE STATE.

### **3.8 Taxes**

Taxes, customs, and tariffs on commodities or contractual services purchased under the Contract will not be assessed against the Customer unless authorized by Florida or Federal law. The Contractor is authorized to collect government-imposed taxes, surcharges, and fees.

### **3.9 Return of Funds**

Contractor will return any overpayments due to unearned funds or funds disallowed pursuant to the terms of the Contract that were disbursed to the Contractor by the Department or Customer. The Contractor must return any overpayment within two (2) billing cycles after either discovery by the Contractor, its independent auditor, or notification by the Department or Customer of the overpayment.

## **SECTION 4. CONTRACT ADMINISTRATION**

### **4.1 Department's Contract Administrator**

The Department's Contract Administrator, whose primary responsibility will be to maintain the Contract file, is as follows:

Caitlen Boles  
Departmental Purchasing  
Department of Management Services  
4050 Esplanade Way, Tallahassee, FL 32399  
Telephone: (850) 410-1423  
Email: Caitlen.Boles@dms.fl.gov

In the event that the Department changes the Department's Contract Administrator, the Department will notify the Contractor's Contract Manager in writing via email and document such in the Contract file. Such changes do not require a formal written amendment to the Contract.

#### **4.2 Department's Contract Manager**

The Department's Contract Manager, who is primarily responsible for enforcing the performance of the Contract terms and conditions and will serve as a liaison with the Contractor, will be as follows:

Jonathan Rakestraw  
Division of Telecommunications  
Department of Management Services  
4030 Esplanade Way, Tallahassee, FL 32399  
Telephone: (850) 921-0857  
Email: [jonathan.rakestraw@dms.fl.gov](mailto:jonathan.rakestraw@dms.fl.gov)

In the event that the Department changes the Department's Contract Manager, the Department will notify the Contractor in writing via email. Such changes do not require a formal written amendment to the Contract.

#### **4.3 Department's Product Manager**

The Department's Product Manager, who is primarily responsible for monitoring the performance of the Contract terms and conditions and will serve as a liaison with the Contractor, will be as follows:

Raghib Quereshi  
Division of Telecommunications  
Department of Management Services  
4030 Esplanade Way, Tallahassee, FL 32399  
Telephone: (850) 413-0319  
Email: [raghib.quereshi@dms.fl.gov](mailto:raghib.quereshi@dms.fl.gov)

In the event that the Department changes the Department's Product Manager, the Department will notify the Contractor in writing via email. Such changes do not require a formal written amendment to the Contract.

#### **4.4 Contractor's Contract Manager**

The Contractor's Contract Manager, who is primarily responsible for the Contractor's oversight of the Contract performance, will be as follows:

Miko Baldwin  
Cellco Partnership d/b/a Verizon Wireless  
10170 Junction Drive, 2<sup>nd</sup> Floor, Annapolis Junction, MD 20701  
Telephone: (240) 280-3563  
Email: [Miko.Baldwin@vzw.com](mailto:Miko.Baldwin@vzw.com)

In the event that the Contractor changes its Contract Manager, the Contractor will notify the Department's Contract Manager in writing via email. Such a change does not require a formal written amendment to the Contract.

#### **4.5 Contractor's Account Manager**

The Contractor's Account Manager, who will serve as a liaison with the Department's Contract Administrator, will be as follows:

Tom Madden  
Cellco Partnership d/b/a Verizon Wireless  
4075 Esplanade Way, Suite 275, Tallahassee, FL 32399  
Telephone: (850) 294-5171  
Email: [Tom.Madden@verizonwireless.com](mailto:Tom.Madden@verizonwireless.com)

In the event that the Contractor changes its Account Manager, the Contractor will notify the Department's Contract Manager in writing via email. Such changes do not require a formal written amendment to the Contract.

## **SECTION 5. CONTRACT MANAGEMENT**

### **5.1 Notices**

All notices required under the Contract must be delivered to the designated Contract Manager by certified mail, return receipt requested, reputable air courier service, email, or personal delivery, or as otherwise identified herein or by the Department.

### **5.2 Change Request**

The Department's Contract Manager may authorize operational changes to services and infrastructure that do not have a pricing impact (non-billable changes) via a written change request to the Contractor. Such authorized operational changes do not require a Contract amendment but will be memorialized in writing and placed in the Contract Managers' files. The Department reserves the right to make the final determination if a change request or Contract amendment is required. Any change that would allow the Contractor to offer less of any deliverable, including commodities, services, technology, or software, requires a Contract amendment. Equipment List and End User Price List updates must be made in accordance with SOW Section 1.5, End User Price Lists (EUPLs) and Vendor's Device List, and do not require an amendment or change request.

### **5.3 Diversity Reporting**

The State of Florida supports its diverse business community by creating opportunities for woman-, veteran-, and minority-owned small business enterprises to participate in procurements and contracts. The Department encourages supplier diversity through certification of woman-, veteran-, and minority-owned small business enterprises and provides advocacy, outreach, and networking through regional business events. For additional information, please contact the Office of Supplier Diversity (OSD) at [osdinfo@dms.myflorida.com](mailto:osdinfo@dms.myflorida.com).

Upon request, the Contractor will report to the Department its spend with business enterprises certified by the OSD. These reports must include the time period covered, the name and Federal Employer Identification Number of each business enterprise utilized during the period, commodities and contractual services provided by the business enterprise, and the amount paid to the business enterprise on behalf of each Customer purchasing under the Contract.

### **5.4 Designated Centralized Nonprofit Agency**

Subject to the agency determination and to the extent applicable as provided for in section 413.036, F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT

SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INSOFAR AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated centralized nonprofit agency and the commodities or contractual services it offers is available at [https://www.dms.myflorida.com/business\\_operations/state\\_purchasing/state\\_contracts\\_and\\_agreements/\(contractType\)/4577](https://www.dms.myflorida.com/business_operations/state_purchasing/state_contracts_and_agreements/(contractType)/4577).

## **5.5 PRIDE**

Subject to the agency determination and to the extent applicable as provided for in sections 946.515 and 287.042(1), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INSOFAR AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the commodities or contractual services it offers is available at <http://www.pride-enterprises.org>.

## **SECTION 6. COMPLIANCE WITH LAWS**

### **6.1 Conduct of Business**

The Contractor must comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, State, and local agencies having jurisdiction and authority. These may include, but are not limited to, Chapters 282 and 287, F.S., Subtitle 60FF, F.A.C., the Communications Assistance for Law Enforcement Act, the Payment Card Industry DSS, IRS Publication 1045, Section 274A of the Immigration and Nationality Act, the Americans with Disabilities Act, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status. The Contractor must comply with and must assist the Department and Customers with compliance with Subtitle 60FF, F.A.C., (and Subtitle 60GG, F.A.C., if applicable).

### **6.2 Dispute Resolution, Governing Law, and Venue**

Any dispute concerning performance of the Contract, which is not resolved by mutual agreement of the Parties, will be promptly submitted in writing to the other party in accordance with Contract Section 5.1, Notices. The Parties shall designate individuals

with authority to resolve the dispute, which for the Department, will be the Department's Contract Manager, and such individuals shall work diligently and in good faith to resolve the dispute within sixty (60) days. If the dispute cannot be resolved after sixty (60) days, the dispute shall be decided by the Department's Contract Manager, who will reduce the decision to writing and serve a copy on the Contractor. The decision of the Department's Contract Manager shall be final and conclusive. Exhaustion of this administrative remedy is an absolute condition precedent to the Contractor's ability to pursue legal action related to the Contract or any other form of dispute resolution.

The laws of the State of Florida govern the Contract. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Contract. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county within the State of Florida chosen by the Department.

### **6.3 Department of State, Registration**

Consistent with Chapters 605 through 623, F.S., the Contractor must provide the Department with conclusive evidence of a certificate of status, not subject to qualification, if a Florida business entity, or of a certificate of authorization if a foreign business entity.

### **6.4 Suspended, Convicted, and Discriminatory Vendor Lists**

In accordance with sections 287.042, 287.133, and 287.134, F.S., an entity or affiliate who is on the Suspended Vendor List, Convicted Vendor List, or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Contract. The Contractor must notify the Department if it or any of its suppliers, subcontractors, or consultants have been placed on the Suspended Vendor List, Convicted Vendor List, or the Discriminatory Vendor List during the term of the Contract.

### **6.5 Scrutinized Companies—Termination by the Department**

The Department may, at its option, terminate the Contract if the Contractor is found to have submitted a false certification as provided under section 287.135(5), F.S., or been placed on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or been engaged in business operations in Cuba or Syria, or to have been placed on the Scrutinized Companies that Boycott Israel List or is engaged in a boycott of Israel. Notwithstanding the foregoing, the Parties are aware of the Eleventh Circuit Court's decision in *Odbrecht Constr. v. Sec'y*, Fla. DOT, 715 F.3d 1268 (11<sup>th</sup> Cir. Fla. 2013), and agree that the provisions of sections 287.135(1)-(5), F.S., pertaining to a company engaged in business operations in Cuba or Syria shall not apply to this Contract unless and until the Eleventh Circuit Court's decision in *Odebrecht Constr. v. Sec'y*, Fla.DOT, 715 F.3d 1268 (11<sup>th</sup> Cir. Fla. 2013) is overturned.

### **6.6 Cooperation with Inspector General**

Pursuant to section 20.055(5), F.S., Contractor, and its subcontractors, if any, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor must provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information

may include, but will not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Contract. The Contractor agrees to reimburse the State of Florida for the reasonable costs of investigation incurred by the Inspector General or other authorized State of Florida official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State of Florida which results in the suspension or debarment of the Contractor. Such costs include, but will not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

#### **6.7 E-Verify**

The Contractor (and its subcontractors) have an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees. By executing this Contract, the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees. The Contractor must obtain an affidavit from its subcontractors in accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of the Contract. In order to implement this provision, the Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the DMS Contract Manager within five (5) days of Contract execution.

This section serves as notice to the Contractor regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and the Department's obligation to terminate the Contract if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. If terminated for such reason, the Contractor will not be eligible for award of a public contract for at least one (1) year after the date of such termination. The Department reserves the right to order the immediate termination of any contract between the Contractor and a subcontractor performing work on its behalf should the Department develop a good faith belief that the subcontractor has knowingly violated section 448.095(1), F.S.

### **SECTION 7. WORKERS' COMPENSATION, GENERAL LIABILITY INSURANCE, INDEMNIFICATION, AND LIMITATION OF LIABILITY**

#### **7.1 Workers' Compensation Insurance**

The Contractor shall maintain Workers' Compensation insurance in compliance with the statutory requirements of the state(s) of operation, as evidenced by a Certificate of Insurance satisfactory to the Department, for the protection of employees not otherwise protected. The Contractor must require all subcontractors to similarly maintain Workers' Compensation Insurance for all of the latter's employees.

#### **7.2 General Liability Insurance**

At all times during the duration of the Contract, the Contractor, at its sole expense, and its subcontractors, if any, shall carry insurance coverage of such types and with such terms and limits as may be reasonably associated with the Contract. All insurance shall be with insurers authorized to transact the applicable line of insurance business in the State of Florida. The Contractor shall provide the Department with Certificate(s) of Insurance evidencing that all appropriate coverage is in place and showing the Department to be an additional insured within thirty (30) days after Contract execution and on the Contract anniversary date each year of the Contract.

Upon receipt of notice from its insurer(s), the Contractor must submit via email, to the Department's Contract Manager, notice of any cancellation of any required insurance that is not replaced at least thirty (30) calendar days prior to cancellation. In the event of cancellation, the Contractor will be responsible for securing a replacement insurance policy in accordance with this section within thirty (30) Business Days after the final date of the cancelled policy.

### **7.3 Indemnification**

The Contractor agrees to indemnify, defend, and hold the Department, Customers, and the State of Florida, its officers, employees, and agents harmless from all third-party fines, claims, assessments, suits, judgments, or damages, including consequential, special, indirect, and punitive damages, including court costs and attorney's fees, arising from or relating to violation or infringement of a trademark, copyright, patent, trade secret or intellectual property right or out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Contract, as well as for any determination arising out of or related to the Contract that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Department.

However, the Contractor shall not indemnify for that portion of any loss or damages proximately caused by the negligent act or omission of the State, the Department, or a Customer, nor shall the foregoing indemnification obligations apply to a Customer's misuse or modification of Contractor's products or a Customer's operation or use of Contractor's products in a manner not contemplated by the Contract or the purchase order.

If any product is the subject of an infringement suit or in the Contractor's opinion is likely to become the subject of such a suit, the Contractor may at its sole expense procure for the Department and Customer the right to continue using the product or to modify it, in accordance with the Contract terms and conditions, to become non-infringing. If the Contractor is not reasonably able to modify or otherwise secure the Customer and Department the right to continue using the product, the Contractor shall remove the product and refund the Customer and Department the amounts paid in excess of a reasonable rental for past use. The Department and Customer shall not be liable for any royalties.

The Contractor's obligations under the preceding two paragraphs with respect to any legal action are contingent upon the Department or State or Customer giving the Contractor: (1) written notice of any action or threatened action, (2) the opportunity to take over and settle or defend any such action at Contractor's sole expense, and (3) assistance in defending the action at Contractor's sole expense.

The Contract does not constitute a waiver of sovereign immunity or consent by the Department or the State of Florida or its subdivisions to suit by third parties.

### **7.4 Limitation of Liability**

For all claims against the Contractor under any PO, CSA, or contract entered into under this Contract, and regardless of the basis on which the claim is made, the Contractor's liability under such a PO, CSA, or contract for direct damages shall be limited to the greater of \$100,000 or two (2) times the dollar amount of such PO, CSA, or contract.

Unless otherwise specifically enumerated in the Contract, no party shall be liable to another for special, indirect, punitive, or consequential damages, including lost data or records even if the party has been advised that such damages are possible. No party shall be liable for lost profits, lost revenue, or lost institutional operating savings.

The limitations of this section do not apply to the Contractor's obligations under section 7.3. Indemnification, and section 9.5, Other Indemnifications and Credit Monitoring, of the Contract.

## **SECTION 8. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY**

### **8.1 Public Records**

Solely for the purpose of this section, the Department's Contract Manager is the agency custodian of public records. If, under this Contract, the Contractor is providing services and is acting on behalf of the Department, as provided in section 119.0701, F.S., the Contractor shall:

1. Keep and maintain public records required by the Department to perform the service.
2. Upon request from the Department's custodian of public records, provide the Department with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.
3. Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the Contract term and following the completion of the Contract if the Contractor does not transfer the records to the Department.
4. Upon completion of the Contract, transfer, at no cost, to the Department all public records in possession of the Contractor or keep and maintain public records required by the Department to perform the service. If the Contractor transfers all public records to the Department upon completion of the Contract, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the Contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department.

**IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT THE TELEPHONE NUMBER, EMAIL ADDRESS AND MAILING ADDRESS PROVIDED FOR THE CONTRACT MANAGER.**

## **8.2 Protection of Trade Secrets or Confidential Information**

If the Contractor considers any portion of materials made or received in the course of performing the Contract (“contract-related materials”) to be trade secret under section 688.002 or 812.081, F.S., or any other applicable law, or otherwise confidential under Florida or federal law, the Contractor must clearly designate that portion of the materials as trade secret or otherwise confidential when submitted to the Department. The Contractor will be responsible for responding to and resolving all claims for access to contract-related materials it has designated trade secret or otherwise confidential.

If the Department is served with a request for discovery of contract-related materials designated by the Contractor as trade secret or otherwise confidential, the Contractor will be responsible for filing the appropriate motion or objection in response to the request for discovery. The Department will provide materials designated trade secret or otherwise confidential if the Contractor fails to take appropriate and timely action to protect the materials designated as trade secret or otherwise confidential.

The Contractor will protect, defend, indemnify, and hold harmless the Department for third-party claims, costs, fines, and attorney’s fees arising from or relating to its designation of contract-related materials as trade secret or otherwise confidential.

## **8.3 Document Management and Record Retention**

The Contractor must retain sufficient documentation to substantiate claims for payment under the Contract and all other records, electronic files, papers, and documents that were made in relation to the Contract, including those required by Section 6.6, Cooperation with Inspector General. Contractor must retain all documents related to the Contract for five (5) years after expiration of the Contract, or, if longer, the period required by the General Records Schedules maintained by the Florida Department of State available at:<http://dos.myflorida.com/library-archives/records-management/general-records-schedules/>.

## **8.4 Intellectual Property**

No provision of this Agreement shall be construed as vesting in the Department any control, ownership or rights in any facilities, operations or intellectual property of Contractor.

The Parties agree that this Contract does not contemplate any development work, e.g., of software or any other intellectual property, for or on behalf of Customer that requires additional IP ownership rights to vest in Customer.

In the event the Parties agree that the Contractor will perform custom development work for or on behalf of Customer, which development work warrants the license or assignment of additional IP rights to Customer, the Parties shall enter into a separate agreement setting forth the work to be completed, the fees to be paid, and the rights to be assigned.

## **SECTION 9. DATA SECURITY REQUIREMENTS**

### **9.1 Duty to Secure State Data**

The Contractor will implement and maintain best practices for technical and organizational controls to protect the security of State Data, including, but not limited to, keeping a secure area around any displayed or otherwise visible State Data and such data is stored and

secured when not in use. The Contractor will be responsible for ensuring that all Persons it contracts with to maintain, store, or process State Data on its behalf will comply with all data security requirements of this section. The Contractor will also comply with any other applicable State or federal rules and regulations regarding security of information. The State will remain the owner of all State Data and any other data made available by the State to the Contractor pursuant to this Contract.

Unless otherwise agreed in writing, the Contractor and its subcontractors will not perform any of the services under this Contract from outside of the United States.

Notwithstanding the previous statement, services under this Contract relating to help desk services, system maintenance, and order processing review may be performed outside of the United States. Access to data that is not classified as personal information pursuant to section 501.171, F.S., or data that is not classified as confidential or exempt pursuant to any other Florida or federal law is allowed from outside the United States under this Contract, provided that the access is provided in compliance with Chapter 60GG-2, F.A.C.

Except as provided above, the Contractor will not allow, through its action or inaction, any State Data to be sent by any medium, transmitted, or to be Accessed outside of the United States. The Contractor will not store any State Data outside of the United States.

The Contractor shall comply with section 501.171, F.S. The Parties agree that the Contractor shall provide the notifications required by sections 501.171(3) and (4), F.S. on behalf of the Department, in accordance with section 501.171(6)(b), F.S.

## **9.2 State Data Access**

The Contractor shall retain a list of all Persons, as defined in Attachment E – Definitions and Acronyms, with Access to State Data, including a statement confirming that each Person has passed the background screening required herein. This statement shall not include the substance of the screening results, only that the Person has passed the screening.

The Contractor shall follow and maintain its written security policy. The security policy or a high-level summary of the security policy subject to DMS acceptance is subject to disclosure within thirty-six (36) hours upon written demand by the Department or its designated agents or auditors and are subject to audit and screening. The security policy may be substituted with a high-level summary of the security policy. The high-level summary of the security policy is subject to DMS acceptance.

The Contractor shall document and record, with respect to each instance of Access to State Data:

1. To the extent known, the identity of all individual(s) who Accessed State Data in any way, whether those individuals are authorized Persons or not;
2. The duration of the individual(s)' Access, including the time and date at which the Access began and ended;
3. The identity, form, and extent of State Data Accessed, including, but not limited to, whether the individual Accessed partial or redacted versions of State Data, read-only versions of State Data, or editable versions of State Data; and

4. The nature of the Access, including whether the State Data was edited or shared with any other individual or entity during the duration of the Access, and, if so, the identity of the individual or entity.

The damages that would result from the Contractor's failure to compile, retain, and provide access to the written policy (or the aforementioned high-level summary) and information required in this subsection are by their nature impossible to ascertain presently and will be difficult to ascertain in the future. The issues involved in determining such damages will be numerous, complex, and unreasonably burdensome to prove. The Contractor therefore agrees to credit the Department the sum of \$5,000 for each breach of this subsection. The parties acknowledge that these credits are liquidated damages, exclusive of any other right to damages, not intended to be a penalty, and solely intended to compensate for unknown and unascertainable damages.

### **9.3 Violations of Data Security Requirements**

A "Security Breach" in this Section 9 means an unauthorized Access of State Data while it is within the Contractor's control. Good faith Access of State Data by a Person, as defined in Attachment E – Definitions and Acronyms, does not constitute a security breach, provided that the information is not used for a purpose unrelated to the furtherance of the Contract or subject to further unauthorized Access. However, unauthorized Access includes incidents where Persons with authorized Access for certain purposes otherwise gain Access for unauthorized purposes.

The Contractor agrees that a Security Breach, including any violations of Section 9.1, Duty to Secure State Data, will entitle the State to a credit commensurate with the Department and Customer's internal staffing and administrative costs associated with managing the Security Breach or violation of Section 9.1, Duty to Secure State Data, as determined by the Department. Such credits will not preclude the State from recovering other damages it may suffer as a result of the Security Breach or violation of Section 9.1, Duty to Secure State Data.

### **9.4 Notification Requirements**

In the event of a Security Breach, including any violations of Section 9.1, Duty to Secure State Data, or a credible allegation of a Security Breach or violation of Section 9.1, Duty to Secure State Data (as determined by the Contractor or the Department), the Contractor must notify the Department's Contract Manager and the affected Customer as expeditiously as practicable in writing or by phone, but in all instances no later than one (1) Business Day of confirmation of Security Breach impacting the Services or credible allegation .

Notification is required regardless of the number of persons or type of State Data affected or potentially affected. The notification must be clear and conspicuous and include a description of the following:

1. The incident in general terms;
2. The type of information, to the extent known or should have been known, that was subject to the violations of Section 9.1, Duty to Secure State Data, or credible allegation of Security Breach;
3. The type and number of entities and individuals who were, or potentially have been, affected by the incident, to the extent known or should have been known; and

4. The actions taken by the Contractor to protect the State Data from further unauthorized Access. However, the description of those actions in the notice may be general so as not to further increase the risk or severity of the Security Breach.

The Contractor must also as expeditiously as practicable, but no later than seventy-two (72) hours from the time of discovery, set up a conference call with the Department's Contract Manager. The conference call invitation must contain a brief description of the nature of the event. When possible, a thirty (30) minute notice will be given to allow Department personnel to be available for the call. If the designated time is not practical for the Department, an alternate time for the call will be scheduled. All available information about the Security Breach or suspected Security Breach must be shared on the call. The Contractor must answer all questions based on the information known at that time and answer additional questions as additional information becomes known. The Contractor must provide the Department with final documentation of the incident including all remedial actions of the Contractor.

#### **9.5 Other Indemnifications and Credit Monitoring**

The Contractor shall be fully liable for the actions of all Persons, as defined in Attachment E – Definitions and Acronyms, and shall fully defend, indemnify, and hold harmless the Department, Customers, the State of Florida, its officers, directors and employees from any third-party claims, suits, actions, damages, proceedings, and costs of every name and description, including attorney's fees, to the extent arising or resulting from a violation by the Contractor or a Person, as defined in Attachment E – Definitions and Acronyms, of Section 9, Data Security, and Section 13, Background Screening and Security, resulting in the Security Breach of State Data. The Contractor shall provide credit monitoring services at its own cost for those individuals affected or potentially affected or by a Security Breach caused by the Contractor's negligence or willful misconduct, or violation of this agreement of these sections by the Contractor or a Person, as defined in Attachment E – Definitions and Acronyms, for a twelve-month period of time following the Security Breach.

### **SECTION 10. GRATUITIES AND LOBBYING**

#### **10.1 Gratuities**

The Contractor will not, in connection with the Contract, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State of Florida officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State of Florida officer or employee.

#### **10.2 Lobbying**

Funds provided under this Contract shall not be used to violate the provisions of sections 11.062 and 216.347, F.S. Pursuant to section 287.058(6), F.S., the Contract does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Contract after Contract execution and during the Contract's term.

## **SECTION 11. CONTRACT MONITORING**

### **11.1 Performance Standards**

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Contract. The Department and the Customer will be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof as it relates to orders provided under this Contract. Coordination must be maintained by the Contractor with representatives of the Customer, the Department, or of other agencies involved in the Contract on behalf of the Department.

### **11.2 Performance Deficiencies and Service Level Agreements**

Service Level Agreements (SLAs) dictate the levels of service delivery for individual services. The parties acknowledge that these SLAs contain financial consequences, as required by section 287.058, F.S., are exclusive of any other right to damages, and are not intended to be a penalty. The Contractor therefore agrees to credit the Department consistently with the Contract, including as set forth in Attachment C - Service Level Agreements. Financial consequences that are due to a Customer after the completion of service, or exceed any payment due to the Contractor, shall be submitted by check rather than as a credit.

One, multiple, or recurring violations of a SLA may be considered a breach of the Contract and may result in a suspension or cancellation of PO(s) or CSA(s) pursuant to Section 1.3.3 of the Contract. The Department reserves the right to determine when violation(s) of SLAs constitute a breach of the Contract or will result in a suspension or cancellation of PO(s) or CSA(s). The Department's determination of a breach of the Contract or suspension or cancellation of PO(s) or CSA(s) will depend on the number and severity of the SLA violation(s), disruption to service, Contractor's response, and other factors.

In addition to the processes set forth in the Contract (e.g., SLAs), if the Department determines that there is a performance deficiency that requires correction by the Contractor, then the Department will notify the Contractor in writing. The correction must be made within a timeframe specified by the Department. The Contractor must provide the Department with a corrective action plan describing how the Contractor will address all performance deficiencies identified by the Department.

If the corrective action plan is unacceptable to the Department, or implementation of the plan fails to remedy the performance deficiencies, the Department will retain ten percent (10%) of the total invoice amount and may suspend or cancel PO(s) or CSA(s) or may suspend work or terminate the Contract as set forth in Section 1.3, Suspension of Work and Termination. The retainage will be withheld until the Contractor resolves the performance deficiencies. If the performance deficiencies are resolved, the Contractor may invoice the Department for the retained amount. If the Contractor fails to resolve the performance deficiencies, the retained amount will be forfeited in order to compensate the Department for the performance deficiencies and the Department may suspend or cancel PO(s) or CSA(s) or may terminate the Contract as set forth in Section 1.3, Suspension of Work and Termination.

### **11.3 Timely Performance**

The Contractor will promptly notify the Department or Customer upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion (or delivery) of any commodity or contractual service. The

Contractor will use commercially reasonable efforts to avoid or minimize any delays in performance and will inform the Department or Customer of the steps the Contractor is taking or will take to do so and the projected actual completion (or delivery) time. If the Contractor believes a delay in performance by the Department or Customer has caused or will cause the Contractor to be unable to perform its obligations on time, the Contractor will promptly so notify the Department or Customer and use commercially reasonable efforts to perform its obligations on time notwithstanding the Department or Customer's delay.

#### **11.4 Force Majeure, Notice of Delay, and No Damages for Delay**

The Contractor will not be responsible for delay resulting from its failure to perform if neither the fault nor the negligence of the Contractor or its employees or agents contributed to the delay and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the Contractor's control, or for any of the foregoing that affect subcontractors or suppliers if no alternate source of supply is available to the Contractor. In case of any delay the Contractor believes is excusable, the Contractor will notify the Department or Customer in writing of the delay or potential delay and describe the cause of the delay either (1) within ten (10) business days after the cause that creates or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result, or (2) if delay is not reasonably foreseeable, within five (5) business days after the date the Contractor first had reason to believe that a delay could result. The foregoing will constitute the Contractor's sole remedy or excuse with respect to delay. Providing notice in strict accordance with this paragraph is a condition precedent to such remedy. No claim for damages will be asserted by the Contractor. The Contractor will not be entitled to an increase in the Contract price or payment of any kind from the Department or Customer for direct, indirect, consequential, impact or other costs, expenses or damages, including but not limited to costs of acceleration or inefficiency, arising because of delay, disruption, interference, or hindrance from any cause whatsoever. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this paragraph, after the causes have ceased to exist the Contractor will perform at no increased cost, unless the Department or Customer determines, in its sole discretion, that the delay will significantly impair the value of the Contract to the State of Florida or to Customers, in which case the Department or Customer may (1) accept allocated performance or deliveries from the Contractor, provided that the Contractor grants the same level of preferential treatment that it would grant to similarly situated government Customers with respect to devices, or (2) purchase from other sources (without recourse to and by the Contractor for the related costs and expenses) to replace all or part of the commodity or contractual services that are the subject of the delay, which purchases may be deducted from the Contract quantity, or (3) terminate the Contract in whole or in part.

## **SECTION 12. CONTRACT AUDITS**

### **12.1 Performance or Compliance Audits**

The Department may conduct, or cause to have conducted, either or both performance and compliance audits of the Contractor and subcontractors as determined by the Department. The Department may conduct an audit and review copies of all the Contractor's and subcontractor's relevant data and records that directly relate to the Contract. The Parties shall agree in writing on the scope of the inquiry, timeframe, location (if an audit is to be conducted), and other terms and conditions before work to satisfy the inquiry is commenced. To the extent necessary to verify the Contractor's claims for

payment under the Contract, the Contractor's agreements or contracts with subcontractors, partners or agents of the Contractor, providing services directly under the Contract, may be inspected by the Department upon fifteen (15) days' written notice, during normal working hours and in accordance with the Contractor's facility access procedures where facility access is required. Release statements from its subcontractors, partners or agents providing services directly under this Contract are not required for the Department or its designee to conduct compliance and performance audits on any of the Contractor's contracts directly relating to the Contract. The State of Florida's Chief Financial Officer and the Office of the Auditor General also have authority to perform audits and inspections.

## **12.2 Payment Audit**

Records of costs incurred under terms of the Contract will be maintained in accordance with Subsection 8.3, Document Management and Record Retention. Records of costs incurred will include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work related to this Contract, and all other records of the Contractor and subcontractors considered necessary by the Department, State of Florida's Chief Financial Officer, or the Office of the Auditor General.

## **12.3 Document Inspection**

In accordance with section 216.1366, F.S., the Department is authorized to inspect the: (a) financial records, papers, and documents of Contractor that are directly related to the performance of Contract or the expenditure of state funds; and (b) programmatic records, papers, and documents of Contractor which the Department determines are necessary to monitor the performance of Contract or to ensure that the terms of the Contract are being met. Contractor shall provide such records, papers, and documents requested by the Department within ten (10) business days after the request is made.

## **SECTION 13. BACKGROUND SCREENING AND SECURITY**

All Contractor employees, subcontractors and agents performing work under the Contract must comply with all security and other requirements of the Department or the Customer.

### **13.1 Background Screening**

In addition to any background screening required by the Contractor as a condition of employment, the Contractor warrants that it will have conducted a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other person, hereinafter referred to as "Person" or "Persons," operating under its direction with Access to State Data or who enter either the premises or facilities where State Data is stored or accessible. Contractor is not required to conduct the aforementioned background screening of a Person if that Person does not have Access to State Data and if that Person, whenever on Customer premises or facilities, is escorted by Customer authorized personnel.

The Contractor warrants that all Persons will have passed the background screening described herein before they have Access to State Data or begin performing services under the Contract. The look-back period for such background screenings shall be for a minimum of six (6) years where six (6) years of historical information is available.

The minimum background check process will include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard:

1. Social Security Number Trace; and
2. Criminal Records (Federal, State, and County criminal felony and misdemeanor, national criminal database for all states which make such information available).

The Contractor agrees that each Person will be screened as a condition prior to performing services or having Access to State Data. The Contractor is responsible for any and all costs and expenses in obtaining and maintaining the criminal background screening information for each Person described above. The Contractor will maintain documentation of the screening in the Person's employment file or applicable Contractor system. The Contractor will abide by all applicable laws, rules, and regulations including, but not limited to, the Fair Credit Reporting Act and/ any equal opportunity laws, rules, regulations, or ordinances.

### **13.2 Disqualifying Offenses**

If at any time it is determined that a Person has a criminal misdemeanor or felony record, regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict), within the last six (6) years, where six (6) years of historical information is available, from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that Person from any position with Access to State Data or directly performing services under the Contract. The disqualifying offenses are as follows:

1. Computer related crimes
2. Information technology crimes;
3. Fraudulent practices;
4. False pretenses;
5. Fraud;
6. Credit card crimes;
7. Forgery;
8. Counterfeiting;
9. Violations involving checks or drafts;
10. Misuse of medical or personnel records; and
11. Felony theft.

If the Contractor finds a Disqualifying Offense for a Person within the last six (6) years where six (6) years of historical information is available from the date of the court's disposition, it may obtain information regarding the incident and determine whether that Person should continue providing services under the Contract or have Access to State Data. The Contractor will consider the following factors only in making the determination: i) nature and gravity of the offense, ii) the amount of time that lapsed since the offense, iii) the rehabilitation efforts of the Person, and iv) relevancy of the offense to the job duties of the Person. If the Contractor determines that the Person should be allowed Access to State Data, then Contractor shall maintain all criminal background screening information and the rationale for such Access in the Person's employment file. The Contractor will promptly notify the Department of any determinations made pursuant to this subsection.

The Department reserves the right to require removal of any Persons from performing work on the Contract for any reason.

### **13.2.1 Refresh Screening**

Contractor will ensure that all background screening of key staff will be refreshed every five (5) years from the time initially performed for each Person during the term of the Contract.

### **13.2.2 Self-Disclosure**

The Contractor shall ensure that all key staff have a responsibility to self-report within three (3) calendar days to the Contractor any updated court disposition regarding any disqualifying offense, regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict). The Contractor shall immediately reassess whether to disallow that Person Access to any State of Florida premises or from directly performing services under the Contract.

In addition, the Contractor shall ensure that all key staff have a responsibility to self-report to the Contractor within three (3) calendar days, any arrest for any Disqualifying Offense.

### **13.3 Department's Ability to Audit Screening Compliance and Inspect Locations**

The Department reserves the right to audit the Contractor's background screening process upon fifteen (15) days prior written notice to the Contractor during the term of the Contract. The parties shall agree in writing on the scope of the inquiry, timeframe, location (if an audit is to be conducted), and other terms and conditions before work to satisfy the inquiry is commenced. The Department will have the right to inspect the Contractor's working area, computer systems, and/or locations to ensure that Access to State Data is secure and that the background screening process is in compliance with the Contract and all applicable state and federal rules and regulations.

## **SECTION 14. COMMUNICATIONS AND CONFIDENTIALITY**

### **14.1 Public Statements**

The Contractor shall not, without first notifying the Department's Contract Manager and securing the Department's prior written consent, make public statements or publicly disseminate any information which concern the Contract or its subject matter, including, but not limited to:

1. disclose or permit disclosure of any data or information obtained or furnished in accordance with the Contract,
2. use any statement attributable to the Department or its employees,
3. mentioning the Contract in a press release or other promotional material, or
4. otherwise linking Contractor's name and either a description of the Contract or the name of the State, the Department or any Customer in any material published, either in print or electronically, to any entity that is not a party to Contract, except potential or actual authorized distributors, dealers, resellers, or service representative.

Public statements include press releases, publicity releases, promotions, marketing materials, corporate communications, or other similar communications. If provided, the Department's written consent shall not be construed to supersede or waive the Contract requirements imposed on the Contractor to maintain confidential information.

The Contractor will not use the State of Florida seal, name, or logo of the Department or State of Florida, or Contractor's relationship to the Department for any purpose without the prior written consent of the Department.

The Contractor may refer to the Contract as an experience citation with other customers without prior approval.

The Contractor shall have the following obligations with respect to the marketing of this Contract to any Customers:

1. To use its commercially reasonable efforts to further the promotion, advertising, and marketing of services available under this Contract; and
2. To use its commercially reasonable efforts to promote the equitable utilization of this Contract to Other Eligible Users to any other cooperative purchasing contract for similar services.

#### **14.2 Confidential Information**

The Contractor must maintain confidentiality of all confidential data, files, and records related to the services and commodities provided pursuant to the Contract and must comply with all applicable state and federal laws, including, but not limited to Chapter 119, F.S., and sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor must also comply with any applicable professional standards with respect to confidentiality of information.

### **SECTION 15. LICENSING**

All services shall include all required licenses for Customers to utilize the services at no additional cost to the Customer.

This section does not govern Contractor or third-party software (which includes applications and enhancement software) sold separately, which are not necessary to provide the WDS, WVS, or public safety services under this Contract (as examples device operating software or device firmware).

Any software (which includes applications and enhancement software) licensed separately by the Contractor or its third-party supplier to Customers for use will be governed by the written terms and conditions applicable to such software or application (e.g., End User License Agreements (EULAs)).

When Customers purchase any software (which includes applications and enhancement software) licensed separately, applicable terms and conditions (e.g., EULAs) will be provided to Customers and may be provided via URL or click-through at point of sale or upon login to the third-party software application. The Contract will take precedence over any and all EULA's conflicting terms. Any provisions in applicable terms and conditions that require the Department to indemnify the Contractor are inapplicable.

## **SECTION 16. PERFORMANCE BOND**

Within thirty (30) days of Contract execution, Contractor will deliver to the Department's Contract Manager a performance bond in the amount of \$500,000 (five hundred thousand). This shall also apply to any renewal years. The bond shall name the Department as the beneficiary and will be used to guarantee satisfactory performance by the Contractor throughout the term of the Contract.

1. The performance bond shall be maintained throughout the term of the Contract. The performance bond must be issued by an acceptable surety company, as determined by the Department, and which surety must be licensed to do business in the State of Florida. The insurer or bonding company shall pay losses suffered by the State of Florida directly to the Department.
2. The Contractor and insurer or bonding company shall provide the Department prior written notice or immediate notice upon knowledge of any attempt to cancel or to make any other material change in the status, coverage, or scope of the performance bond, or of the Contractor's failure to pay bond premiums.
3. The Department shall not be responsible for any premiums or assessments on or in relation to the performance bond.
4. The performance bond is to protect the Department and the State against any loss sustained through failure of the Contractor's performance in accordance with the Contract. No payments shall be made to the Contractor until the performance bond is in place and approved by the Department in writing.
5. Within thirty (30) days of Contract execution, and by Contract execution anniversary each year following, the Contractor shall provide the Department with a surety bond continuation certificate or other acceptable verification that the performance bond is valid and has been renewed for an additional year.
6. The performance bond provided under this section shall be used solely to the extent necessary to satisfy the damage claims made by the State of Florida pursuant to the terms of the Contract. In no event shall the performance bond be construed as a penalty bond.
7. No sooner than two (2) years after Contract execution, if it is in the best interest of the State of Florida, as determined by the Department, the Contractor's performance bond may be reduced for the remainder of the term. This reduction shall require an amendment to the Contract with the agreement of both parties.

## **SECTION 17. CUSTOMER OF RECORD**

The Department is considered the Customer of Record for all services for the purposes of the Federal Communications Commission and Customer Proprietary Network Information.

## **SECTION 18. SPECIFIC APPROPRIATION**

The following is the specific State fund from which the State will make payment under the first year of the Contract:

General Appropriations Act (Florida Law)  
2845 SPECIAL CATEGORIES

CENTREX AND SUNCOM PAYMENTS FROM COMMUNICATIONS WORKING  
CAPITAL TRUST FUND

**SECTION 19. MISCELLANEOUS**

**19.1 Warranty of Contractor's Ability to Perform**

The Contractor warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Contract obligations. The Contractor warrants that neither it nor any affiliate is currently on the Suspended Vendor List, Convicted Vendor List, Discriminatory Vendor List, or on any similar list maintained by any other state or the federal government.

The Contractor shall notify the Department of any regulatory or legal actions filed by any federal, state, or local government entity and any other litigation that is reasonably likely to have a material adverse impact on the Contractor's ability to perform under this Contract within thirty (30) days of the action being filed.

The Contractor must notify the Department of any legal actions filed against it for a breach of a contract that is of similar size and scope to this Contract within thirty (30) days of the action being filed, unless such legal action is withdrawn or dismissed within such thirty (30) day period. Failure to notify the Department of a legal action within thirty (30) days of the action will be grounds for termination for cause of the Contract.

The Contractor shall within five (5) calendar days notify the Department in writing if its ability to perform is compromised in any manner during the term of the Contract.

**19.2 Subcontractors, Affiliates, Partners, Teammates, Third-Party Vendors**

The Contractor is fully responsible for satisfactory completion of all subcontracted work, including work by affiliates, partners, teammates, and all other third-party vendors, in accordance with the terms and conditions of the Contract.

**19.3 Assignment**

The Contractor will not sell, assign, or transfer any of its rights, duties or obligations under the Contract without the prior written consent of the Department, which shall not be unreasonably withheld.

However, the Contractor may assign its right to receive payment under the Contract without the Department's consent upon written notice to the Department, with documentation supplied to the Department as required.

In the event of any permitted assignment, the Contractor remains secondarily liable for performance of the Contract, unless such responsibility is waived by the Department in writing. The Department may assign the Contract with prior written notice to the Contractor.

**19.4 Independent Contractor**

The Contractor is an independent contractor. The Contractor and its employees, agents, representatives, and subcontractors, affiliates, partners, teammates, and all other third-party vendors are not employees or agents of the Department and are not entitled to the benefits of State of Florida employees. The Department will not be bound by any acts or

conduct of the Contractor or its employees, agents, representatives, or subcontractors, affiliates, partners, teammates, and all other third-party vendors.

#### **19.5 Risk of Loss**

Matters of inspection and approval are addressed in section 215.422, F.S. Until acceptance, risk of loss or damage will remain with the Contractor. The Contractor will be responsible for filing, processing, and collecting all damage claims. To assist the Contractor with damage claims, the Customer will: record any evidence of visible damage on all copies of the delivering carrier's Bill of Lading; report damages to the carrier and the Contractor; and provide the Contractor with a copy of the carrier's Bill of Lading and damage inspection report. When a Customer or the Department rejects a commodity at Contractor's expense, it may be returned within thirty (30) days of receipt, and the risk of loss will remain with the Contractor.

For Contractor-installed in-building infrastructure owned by the Contractor (e.g., bidirectional amplifiers, including antennas and power), Contractor will remove the commodity (except for cabling) from the premises within thirty (30) days, after notification of rejection, removal fees may be applicable, and the risk of loss will remain with the Contractor.

For Contractor-installed in-building infrastructure, commodities not removed by the Contractor within thirty (30) days of receipt of notification will be deemed abandoned by the Contractor, and the Customer or the Department will have the right to dispose of it as its own property. Contractor will reimburse the Customer or the Department for costs and expenses incurred in storing or effecting removal or disposition of rejected commodities

#### **19.6 Safety Standards**

Performance of the Contract for all commodities or contractual services must comply with applicable requirements of the Occupational Safety and Health Act and other applicable State of Florida and federal requirements.

#### **19.7 Ombudsman**

A Vendor Ombudsman has been established within the Department of Financial Services. The duties of this office are found in section 215.422, F.S., which include disseminating information relative to prompt payment and assisting contractors in receiving their payments in a timely manner from a Customer. The Vendor Ombudsman may be contacted at (850) 413-5516.

#### **19.8 Time is of the Essence**

Time is of the essence regarding each and every obligation of the Contractor. Each obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

#### **19.9 Waiver**

The delay or failure by the Department or Customer to exercise or enforce any rights under the Contract will not constitute waiver of such rights.

#### **19.10 Modification and Severability**

With the exception of the process described in Section 5.2, Change Requests, this Contract may only be modified by a written agreement signed by the Department and the Contractor.

Should a court determine any provision of the Contract is invalid, the remaining provisions will not be affected, and the rights and obligations of the Parties will be construed and enforced as if the Contract did not contain the provision held invalid.

**SIGNATURE PAGE IMMEDIATELY FOLLOWS**

**SO AGREED** by the parties' authorized representatives on the dates noted below:

**FLORIDA DEPARTMENT OF MANAGEMENT SERVICES**

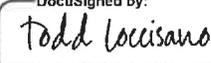


**J. Todd Inman, Secretary**

8/24/2021

**Date**

**CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS**

DocuSigned by:  
  
CD86E5219D09460...

**Signature**

Todd Loccisano  
VP - Commercial Deal Management (Wireless), Verizon Business Group

**Print Name and Title**

7/27/2021 | 9:59 AM MDT

**Date**



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

Ron DeSantis, Governor

**Contract No.: DMS-19/20-006C**  
**Attachment A – Definitions and Acronyms**

All personal pronouns used in the Contract, whether used in the masculine, feminine, or gender-neutral, shall include all other genders; the singular shall include the plural; and the plural shall include the singular. The following definitions and acronyms apply to the Contract in addition to the definitions in Chapter 287, Florida Statutes (F.S.), and Rule Chapter 60FF-1, Florida Administrative Code (F.A.C.). In the event of a conflict, the definitions provided in this document will prevail.

Access	When capitalized, this means review, inspect, transmit, approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any State Data, regardless of type, form, or nature of storage; Access to a computer system or network includes local and remote access.
Business Days	Monday, Tuesday, Wednesday, Thursday, and Friday, excluding weekends and State paid holidays as set forth in section 110.117, F.S.
Contractor	The Responsive and Responsible Respondent awarded this Contract pursuant to ITN DMS-19/20-006. This definition supersedes the definition in section 287.012(7), F.S.
CPNI	Customer Proprietary Network Information. The definition of CPNI is the Title 47 U.S. Code § 222(h) (2019) definition.
CRR	Cost Recovery Rate. The Department's monthly cost recovery charge applied to Customer invoices.
CSAB	Communications Service Authorization and Billing system. <a href="https://portal.suncom.myflorida.com/start/#/login">https://portal.suncom.myflorida.com/start/#/login</a>
Customers	The entities that are provided services under this Contract, including State agencies, which are required to use the SUNCOM Network, and other entities authorized to use the SUNCOM Network in accordance with Chapter 282, F.S.
End-user	The individual that utilizes the device that consumes the resources defined by the monthly plan. The End-user's employer is the Customer.
EUPL	End User Price List
HA/HR	Highly-available and Highly-reliable. Systems, services, and implementations designed to eliminate planned downtime and prevent unplanned downtime; methods utilize specific hardware, software, and processes; typically implemented in mission critical services.
IP	Internet Protocol
IPsec	An Internet Engineering Task Force standard. Text from RFC 4301 - IPsec creates a boundary, between unprotected and protected interfaces, for a host or a network. Traffic traversing the boundary is subject to the access controls specified by the user or administrator responsible for the IPsec configuration.

**Contract No.: DMS-19/20-006C**  
**Attachment A – Definitions and Acronyms**

IPsec Tunnel	Tunnels are a design technique utilized by telecommunications service providers to manage traffic. IPsec tunnels are used to create closed user groups to enforce segregation of traffic. IPsec tunnels are a specific type of tunnel which provides security services for IP packets through encryption, authentication, and protection against replay.
MFN	MyFloridaNet
OEU	Other Eligible Users. The entities provided services under this Contract that are not State agencies and are not required to use the SUNCOM Network but are otherwise authorized to use the SUNCOM Network in accordance with Chapter 282, F.S. These include, but are not limited to, political subdivisions of the State, including counties, municipalities, school districts, and water management districts. Also included are, private nonprofit elementary and secondary schools conditioned upon certain requirements, universities, libraries of community colleges, and nonprofit corporations.
Person	When capitalized in Sections 9 and 13 of the Final Contract, this means the Contractor's employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other person operating under the Contractor's direction with Access to State Data or who enters either the premises or facilities where State Data is stored or accessible.
Reply	A formal response to ITN No. DMS-19/20-006.
Respondent	An entity that submitted a Reply to ITN No. DMS-19/20-006.
SLA	Service Level Agreement
SLA Clock	Service Level Agreement Clock. The SLA clock refers to how a deliverable will be measured in terms of time for completion as stated in the particular SLA.
SNMP	Simple Network Management Protocol
State	The State of Florida
State Data	All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received by the Contractor in its performance under this Contract.
Subcontractor	A third party performing work under the Contract at the direction of the Contractor, including affiliates, partners, teammates, and all other third-party vendors.
VPN Concentrator	Virtual Private Network Concentrator. A device, or collection of devices, built to manage secure connections within or between infrastructures.
VRF	Virtual Routing and Forwarding
WDS	Wireless Data Service
WVS	Wireless Voice Service



Office of the Secretary  
4050 Esplanade Way  
Tallahassee, FL 32399-0950  
850-488-2786

**Ron DeSantis, Governor**

# Best and Final Offer

## 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	Mobile Communication Services Portfolio .....	6
1.2	MCS Objectives.....	7
1.3	MyFloridaNet .....	7
1.4	End User Price Lists and Vendor's Device List .....	7
1.5	Evolving Technology .....	11
2.	Contractor Staffing .....	14
2.1	Staffing Responsibilities .....	15
2.2	Key Staff Position - Account Manager.....	18
2.3	Key Staff Position - Project Manager.....	19
2.4	Key Staff Position - Business Operations Manager.....	19
2.5	Key Staff Position - Engineering and Design Manager .....	20
2.6	Key Staff Position - Operations and Security Manager .....	20
2.7	Customer Support Team .....	21
3.	Services and Devices for Mobile Communication Services .....	22
3.1	Wireless Voice Services .....	22
3.2	Wireless Data Service .....	22
3.3	Wireless Data Service - IP Addresses.....	23
3.4	Wireless Data Service – Access Circuit .....	23
3.5	Wireless Data Service - Closed User Groups .....	25
3.6	Wireless Data Service – Network-to-Network Interface Design .....	26

3.7 Wireless Data Service –Traffic Mapping into MyFloridaNet ..... 36

3.8 Wireless Data Service – Traffic Directly to the Internet ..... 37

3.9 Wireless Data Service - Test Plan ..... 39

3.10 State of Florida Coverage..... 39

3.11 Roaming ..... 40

3.12 Security..... 40

3.13 Reviews of the Contractor’s Service..... 43

3.14 Emergency Services..... 44

3.15 Contractor’s Service Delivery Costs ..... 45

3.16 Highly Available and Highly Reliable Design Characteristics ..... 46

3.17 Reports, Updates, and Notifications Requirements..... 47

3.18 Service Level Agreement Operational Process..... 48

3.19 Customer Support ..... 52

3.20 Contractor’s MCS Portal ..... 57

3.21 Devices..... 60

3.22 Cooperation with Other Contractors ..... 62

3.23 Customer Migration ..... 62

3.24 Transition for Future Iterations of this Service..... 64

3.25 Contractor Meetings with DMS ..... 66

3.26 Project Management ..... 68

3.27 Project Management - Services Infrastructure Checklist..... 72

4. Public Safety Service Plans and Devices..... 74

4.1	Deployable Technologies .....	74
4.2	Local Control .....	77
4.3	Local control portal .....	77
4.4	Public Safety Standards .....	80
4.5	Demonstration Devices .....	81
4.6	Public Safety Customer Support .....	81
4.7	Public Safety Reporting .....	83
4.8	Public Safety Marketing .....	84
5.	Business Operations .....	96
5.1	General Description of the SUNCOM Business Model.....	96
5.2	Communications Service Authorization and Billing Transaction Flowchart.....	96
5.3	Communications Service Authorization and Billing – Official Record.....	99
5.4	Communications Service Authorization and Billing - Interface with Contractor .....	99
5.5	Communications Service Authorization and Billing Service Catalog .....	100
5.6	Taxes and Government Sanctioned Fees .....	100
5.7	User Access Privileges for the Contractor .....	101
5.8	Work Orders .....	101
5.9	Inventory .....	102
5.10	Invoicing Requirements .....	102
5.11	Electronic Substantiating Detail File .....	102
5.12	Audit of Contractor Invoices .....	103
5.13	Mandatory Interface with the Contractor .....	103

5.14 Properly Authorized Work Orders..... 103

5.15 General Billing Requirements ..... 103

5.16 Billing Start ..... 103

6. Direct Ordering and Billing..... 104

6.1 Services and Devices Sold to Direct-Billed Customers ..... 104

6.2 Cost Recovery Rate ..... 104

6.3 Contract Association on Direct-Billed Accounts ..... 105

6.4 Monthly Reporting of Direct-Billed Accounts ..... 105

6.5 Quarterly Reporting of Direct-Billed Accounts ..... 106

6.6 Customers Liability ..... 106

# 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.

## 1.1 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.

## 1.2 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.

## 1.3 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](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.

## 1.4 End User Price Lists and Vendor's Device List

This subsection applies to both WVS and WDS.

### 1.4.1 EUPL and Vendor's Device List

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 Vendor's Device List should include all proposed devices, including, at a minimum, cellular phones, smartphones, tablets, broadband access devices (data-only), cellular mobile broadband devices (support for internet access), devices supporting secure access to MFN, and accessories. Devices may be shown with a variety of packages, with detailed pricing, and descriptions of associated services, devices and/or features. Any services, devices, and/or features provided at no cost should be identified as \$0.00. Vendor's Device List may also include Public Safety wearables and other Public Safety wireless enabled devices. All devices shall include an AC charger at no additional cost, however additional or replacement AC chargers may be offered with a cost associated. Contractor's may offer a price discount if a chargeable device is sold without an AC charger included.

For all items listed below, the Vendor's Device List should include: manufacturer and model, vendor's identification number (SKU), vendor's commercially advertised retail price as of the date the EUPL is submitted to the Department, State purchase price, and any promotional pricing, as well as the following device-specific information:

1. Smartphones
  - a. Operating system, camera, removable memory (if available), hearing aid compatibility, mode, and other features.
  - b. At least one (1) unlocked iPhone and one (1) unlocked Android smartphone.
2. Air Cards, USBs, and hotspots
  - a. Mode, compatibility with 4G LTE, compatibility with 5G, compatibility with Apple Operating Systems (iOS, Mac OS), compatibility with Microsoft Operating systems (Windows), external antenna, and other features.
3. Tablets
  - a. Operating system, camera, removable memory (if available), and other features.
4. Basic Phones.
  - a. At least one (1) basic phone that is available to Customers at no charge, other than the cost of the purchased service plan.
5. Accessories
  - a. May include phone cases, tablet cases, headphones and ear buds, chargers, screen protectors, foldable keyboards, belt clips, and hands-free kits.
6. Public Safety Wearables
  - a. Contractor's EUPL should state service prices as monthly recurring charges (MRC) or non-recurring charges (NRC).

The EUPL should include, as applicable, the following information for provided services and devices, at a minimum:

1. Non-pooled Plans
  - a. Pricing and details of all non-pooled plans, which may include:
    - i. Voice per minute rate plans: usage based, limited
    - ii. Unlimited plans: voice; voice and text; voice, text, and data; voice, data, messaging, and hotspot
    - iii. Messaging plans: limited and unlimited

- iv. Data only device plans: per megabyte data plan, data plan with tethering, data plan without tethering, and unlimited data
    - b. Relevant unit pricing, including price per minute, variation of price per minute for nights and weekends, monthly rollover of minutes or data.
    - c. Description of services included in the monthly recurring costs, including the number of messages (SMS/MMS), minutes (anytime, nights, or weekends), data limits, and included features, such as call waiting.
      - i. Detail how airtime and other measured usage are billed; for example, in full-minute increments, rounded up to the next full increment at the end of each call for billing purposes, unanswered outgoing calls incurring airtime.
      - ii. Description of billing for calls directly dialing or receiving from the same carrier.
      - iii. If the pricing changes for nights and weekends, describe the times the carrier deems are nights and weekends and any changes to charges during this time.
      - iv. Detail any prohibited activities, such as those prohibited for compliance with the law or to prevent interference with the network.
2. Pooled Plans
  - a. Pricing and details of all pooled plans, which may include:
    - i. Description of tiers, including the number of minutes included in the plans.
  - b. Relevant unit pricing, including price per minute, variation of price per minute for nights and weekends, monthly rollover of minutes or data.
  - c. Describe:
    - i. how the minutes are aggregated and credits are applied;
    - ii. how a Customer can have more than one pool;
    - iii. rollover minutes;
    - iv. pool limitations, e.g., limits to the number of users; and
    - v. included features, such as call waiting.
3. Push-to-Talk
  - a. Pricing and details of all push-to-talk plans, which may include:
    - i. Standalone push-to-talk and add-on push-to-talk plans.
    - ii. Relevant unit pricing including price per minute, variation of price per minute for nights and weekends, monthly rollover of minutes or data.
    - iii. Description of services included in the monthly recurring costs and included features
      1. Detail how measured usage is billed, for example, in full-minute increments, rounded up to the next full increment at the end of each call for billing purposes, or unanswered outgoing calls incurring airtime.
      2. If the pricing changes for nights and weekends, describe the times the carrier deems are nights and weekends and any changes to charges during this time.

3. Detail any prohibited activities, such as those prohibited for compliance with the law or to prevent interference with the network.
4. Machine-to-Machine
  - a. Pricing and details of all machine-to-machine and internet of things service plans which may include:
    - i. Description of tiers, including the usage caps of each tier. One (1) MB to twenty (20) GB requested, at minimum.
  - b. Relevant unit pricing, including price per minute, variation of price per MB for nights and weekends, and monthly rollover of minutes or data.
  - c. Description of services included in the monthly recurring costs and included features.
    - i. Detail how measured usage is billed.
    - ii. Detail any prohibited activities, such as those prohibited for compliance with the law or to prevent interference with the network.
5. Discounts
  - a. All proposed discounts off accessories and devices.
  - b. State what published price the discount percentage applies to (MSRP, vendor published catalog, etc.).
    - i. Describe any additional proposed discounts, such as 100% discount off activation fees.
    - ii. Specific pricing for devices should be listed in the Vendor's Device List.
6. Additional Features, Fees, and Other Items
  - a. The EUPL may describe and detail any additional offerings that are contemplated within the SOW.
    - i. These may include chargeable features, such as robo-call blocking, mobile device management, etc.
    - ii. The EUPL may also include tiered pricing.
  - b. There will be no activation fees for services and devices purchased off the Contract.
  - c. There are no termination fees for services purchased off of the Contract.
  - d. Rate plans shall be month to month, unless otherwise agreed in writing by the DMS Contract Manager.
  - e. In the event that a rate plan includes a device subsidy and the Customer terminates services early, the Contractor may bill the Customer for the unpaid portion of the subsidized amount on the Customer's invoice. For example, a device is offered at discounted price if purchased with a twenty-four (24) month rate plan. In the event a Customer purchases a subsidized device and the Customer terminates services early, or moves to a lesser price plan or disconnects the devices from the Contractor's network within twenty-four (24) months of the device activation, the Contractor may bill the Customer for the unpaid portion of the subsidized amount of the device.

#### 1.4.2 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 combined pricing is competitive to market rates offered under state government contracts similar in size, scope and terms, specifically that it is equal to or less than combined pricing for similar offerings in the State of Texas, State of California, and State of New York and excluding rates for commercial contracts;
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.
--

#### 1.5 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).

#### **Verizon's Evolving Technology**

Verizon acknowledges the importance of ensuring delivery of services and devices that keep pace with rapidly evolving technologies and related service plans for customers purchasing under the State of Florida contract for Mobile Communication Services. In order to achieve this end, your Government Account Manager will keep DMS's authorized POC abreast of developments made possible through technological advancements as they become commercially available. As new technology becomes commercially available, DMS may add new plans, features and equipment that take advantage of the technology's functionality. If new equipment is needed, then the State may order new equipment in accordance with the terms and conditions for equipment upgrades as outlined in your overarching contract. Please note that the purchase of new equipment may require an extension of applicable line terms.

Verizon acknowledges the requirements for updating Vendor's Device List and EUPL as detailed within SOW Subsection 1.5, End User Price Lists and Vendor's Device List. In order to ensure that we are offering the latest generation of devices and related service plans to DMS, Verizon can provide DMS with Quarterly Business Reviews (QBRs). These QBRs include, but are not limited to: a review of your recent account activity; cost saving opportunities and account optimization strategies; a discussion of new technologies, products and services; and any other items that you would like to discuss with us. From time-to-time your Government Account Manager may present new products, services, and offers outside of the QBR.

#### **Our Commitment to the Verizon Wireless Network**

Network leadership is the central element of our strategy, and we are continually investing in our network to extend our leadership. Since 2000, we have invested more than \$145 billion nationwide to build and enhance our wireless network, and continue to make significant network-related capital investments, including spectrum acquisitions.

We've deployed multiple LTE Advanced features on our network that already contribute to our unparalleled, award-winning network performance; and we've led the charge in harnessing unlicensed spectrum with our work on LTE-Unlicensed (LTE-U) (precursor to License Assisted Access [LAA]) and Citizens Band Radio Service (CBRS) @ 3.5 GHz. By design and with consistent investment over time, we are in a great position to continue to meet the needs of our customers with the nation's most reliable network, and to extend our lead over the competition.

We are focusing our capital spending on adding capacity and density to our 4G LTE network while also building our next generation 5G network. We are densifying our network by utilizing small cell technology, in-building solutions and distributed antenna systems. Network densification enables us to add capacity to address increasing mobile video consumption and the growing demand for Internet of Things (IoT) products and services on our 4G LTE and 5G networks.

Our thoughtful technology choices, well-rounded spectrum assets and excellence in execution position us for continued 4G distinction and 5G leadership. Verizon has multiple network-related projects underway or planned for the near future.

### **5G Technology**

Verizon is here. 5G will deliver enhanced fixed and mobile broadband, low-latency services and massive scale for IoT, which will transform all industries. 5G won't be a wireless "evolution," with better speeds and feeds, but a true revolution changing the way we work and interact: This means more connected services and devices, and higher broadband capacity that can benefit our entire society.

We started with America's most reliable network. Now, we're providing 5G Nationwide coverage for more than 200+ million people in 1,800+ cities. And, we have expanded our 5G Ultra Wideband, the fastest in the world\*, to select areas of 57 cities.

- 5G Ultra Wideband uses the high-band, ultra-wide millimeter wave spectrum to deliver 5G. These ultrafast speeds and reduced lag time (latency) can enable advancements in technology such as augmented and virtual reality, autonomous cars, connected cities and more.
- 5G Nationwide uses low-band spectrum enabled by dynamic spectrum sharing (DSS), which allows customers with 5G-enabled devices to use the high-frequency millimeter spectrum 5G Ultra Wideband network where it is available and fall back on the low-frequency 5G Nationwide network where it is not available.

With these 5G technologies, our network has the power to deliver on eight capabilities, or currencies: Peak data rates, mobile data volumes, mobility, number connected devices, energy efficiency, service deployment, reduced latency and improved reliability. Initially, customers should expect our 5G Nationwide network to perform similarly to our award winning 4G LTE network. Performance and coverage will continue to grow over time.

\*Global claim from May 2020, based on Opensignal independent analysis of mobile measurements recorded during the period January 31 – April 30, 2020. © 2020 Opensignal Limited

For Verizon, there are four critically important foundational elements that underpin the construction of our 5G network: Optical fiber, abundant Radio Frequency spectrum, Software-Defined Networks (SDN) and mobile-edge computing (MEC).

- **Fiber:** We are reinventing our network architecture around a common fiber platform that will support both our wireless and wireline businesses.
- **Spectrum:** In addition to our low and mid-band spectrum, we have spectrum licenses in the 28 and 39 Gigahertz (GHz) band, collectively called millimeter-wave spectrum, which is being used for our 5G-technology deployment.
- **Software-Defined Networks (SDN):** As organizations strive to stay ahead of the competition in an increasingly digital economy, we've expanded our offerings to help them accelerate their digital transformation to support future 5G capabilities. Verizon's Virtual Network Services will support 5G devices on software-defined wide area network (SD-WAN) platforms, making it easier to manage network traffic and application performance across a wide area network on both public and private networks. An extension of SDN is network slicing, the ability to partition the network into varying service levels of performance and offerings.
- **Mobile Edge Compute (MEC):** We will use multi-access edge computing to move intelligence to the edge of the network, to minimize latency, and to maximize network efficiency. We will also build in privacy measures that understand data context, including location.

Verizon's network legacy is rooted in being the first to deliver to customers the next-generation of wireless technology, nationwide, before any other carrier.

- On October 1, 2018, we launched the first commercial 5G network – our 5G Home Internet service for consumers – in parts of four cities on our 5G Ultra Wideband network; additional cities continue to be added
- In 2019, Verizon focused on dense, downtown areas and public spaces, and then rapidly expanded 5G availability
- Through October 2020, Verizon has launched our 5G Ultra Wideband mobile network in select areas of 57 cities as well as parts of 43 stadiums and arenas and 7 airports, with a goal of 60 cities by the end of 2020
- On October 13, 2020, Verizon launched its 5G Nationwide network enabled by DSS in 1,800+ cities

With 5G, we will continue to drive innovation across the technology landscape to bring new solutions to market for our customers.

Your Government Account Manager can provide additional network roadmap information through an Executive Briefing.

## 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 sixty (60) 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 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 one hundred and twenty (120) days of vacancy or within the timeframe established by the Department after a waiver of the one hundred and twenty (120) 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 reasonably 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.

### **Verizon's Florida Government Support**

Since 2004, Verizon has used a dedicated government sales and support model for all government sales in the state of Florida. The team is solely dedicated to state and local government and specifically trained in government contracting, ethics and compliance. This team provides local frontline sales and support to public safety, state, and local government as well as local EOC support during times of crisis. Today the team consists of over 40 employees living in Florida with a combined 240 years of experience supporting the State of Florida Department of Management Services Wireless Contracts with Verizon.

#### **Structure:**

Managing Partners (MP) are responsible for teams that are geographically dispersed between North, Central and South Florida. Each MP team consists of Government Major Account Managers (GMAM) and Senior Managers (SM) reporting directly to the MP while a team of Government Business Account Managers (GBAM) report directly to the Senior Manager with a dotted line to the MP. In addition, there are Government Business Account Specialists (GBAS) dedicated to each MP team for customer and team support. Additional support for the MP teams is provided by a team of Government Solutions Architects (GSA) that are geographically assigned to support the local teams, Global Enterprise Advisors dedicated to supporting billing and escalations issues within our larger accounts, Coordinator Business Operations (CBO) supporting the operations aspects of our current contract and a Client Partner (CP) which functions as the account and contract manager.

#### **Current Head Count**

- Managing Partners- 2
- Senior Managers-3
- Client Partner-1
- CBO-1
- GMAM-10
- GBAM-13
- GBAS-5
- GSA-4
- GEA-3

Verizon must retain discretion and control over assignment of account management, customer support or other such Verizon personnel. Our prospective employees are investigated and reviewed to determine whether they merit employment at the positions for which they applied. All such information remains confidential and shared with third parties only on a need to know basis. Our employees are covered by the Verizon Code of Conduct, which can be provided for your review upon request. At any time, you may provide feedback to us regarding the skills, qualifications and performance of any member of the account management team. We will make every effort to notify you of any changes in your account team.

In the event of any change to any member of your account management team, we will work with DMS towards achieving a smooth transition. Additional account support procedures are available in the event of personnel change. In addition, you can use escalation procedures as well as the cross-trained skills and experience of many account support personnel.

We may review any recommendations from you, as allowed by law, that will assist us in placing a Client Partner or Account Manager with the appropriate skills to support your account initiatives.

Although our goal is continuity of the Verizon account team, we cannot guarantee that changes in personnel and staffing assignments will not occur during the term of your contract. The structuring of the Business and Government Customer Operations organization enables all members of the Business and Government Customer Operations organization to be cross-trained on all accounts with the goal of each customer receiving the same comprehensive professional customer service.

## 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 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 or equivalent experience:

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. This is a required key staff position that must remain filled until the Contractor completes, and the Department accepts, the project closure documentation required by Statement of Work section 3.26.4.

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 or equivalent experience:

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 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, or at least two (2) years of equivalent work experience in lieu of a current project management certification.

### 2.4 Key Staff Position - Business Operations Manager

The Contractor shall assign a dedicated, but not necessarily exclusive, Business Operations Manager. 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 or equivalent experience:

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. 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 or equivalent experience:

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. Equivalent work experience of five (5) years is acceptable in lieu of a degree.
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. 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 or equivalent experience:

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 in lieu of a degree.
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, or a range of 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. For closed user groups the Contractor must configure 1) public IP addresses owned by the State and Other Eligible Users or 2) private IP addresses furnished by the State 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 in public user groups.
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.
--

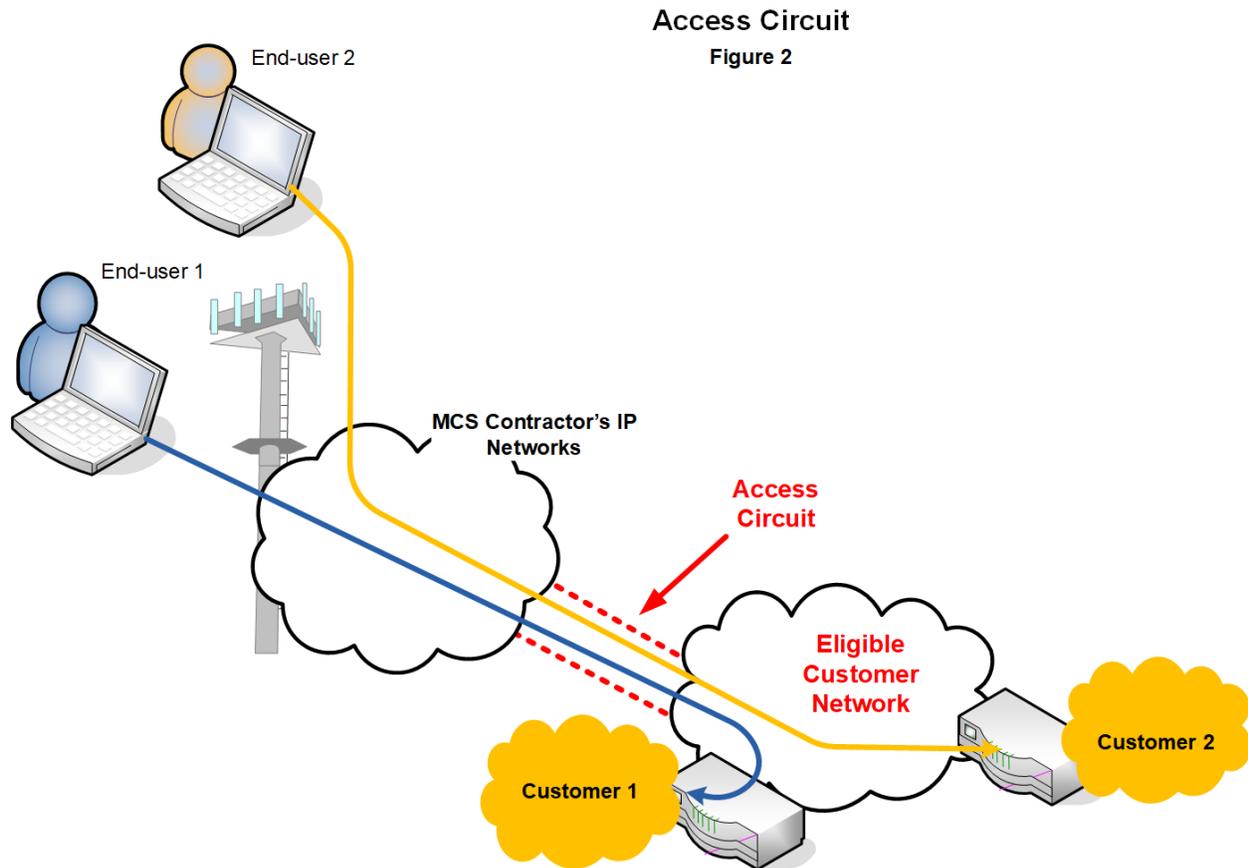
### 3.4 Wireless Data Service – Access Circuit

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. In accordance with SOW Section 3.15, Contractor will configure Contractor's end of the tunnels, and the Customer will be responsible for the Customer's end of the VPN.

**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.

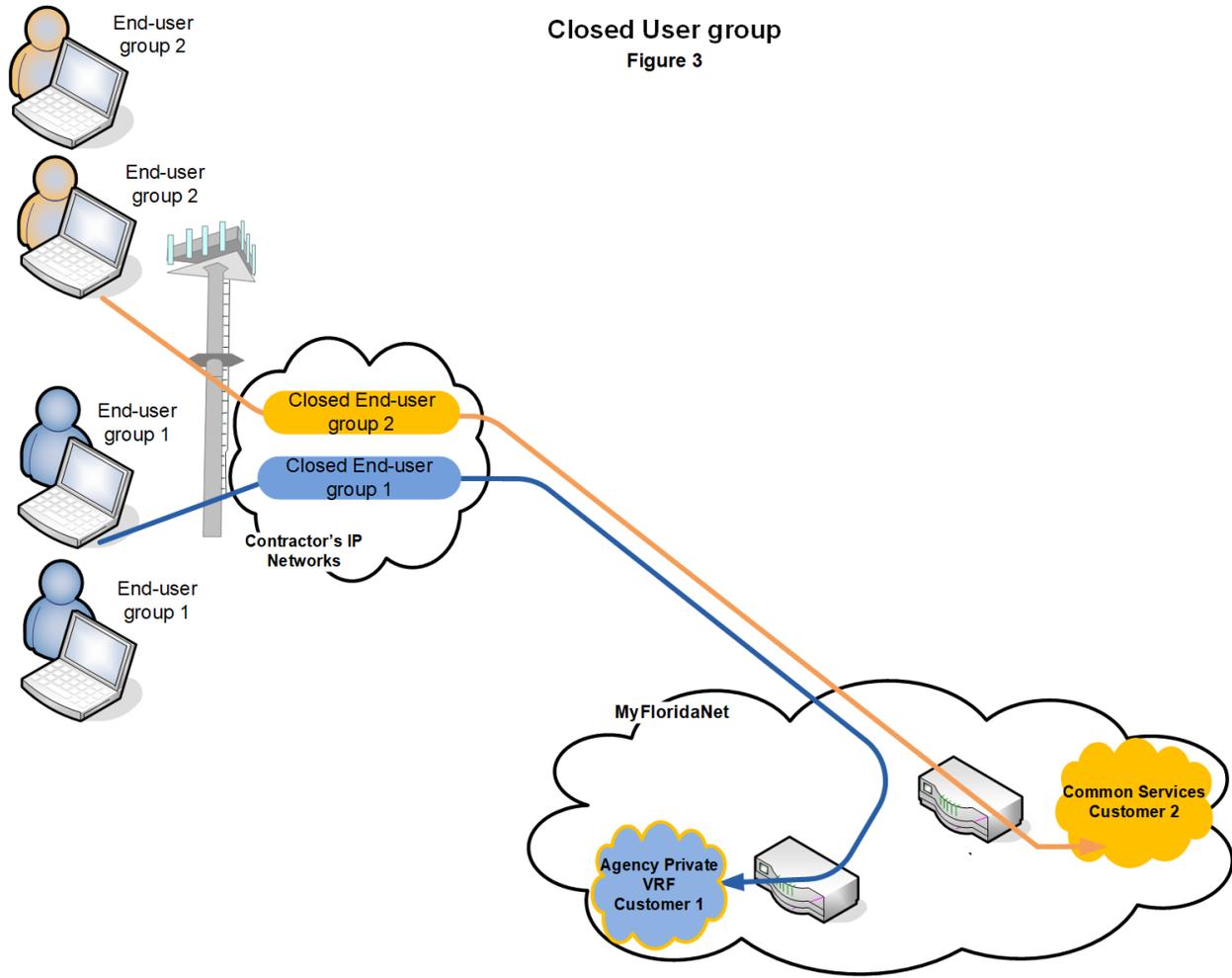
### 3.5 Wireless Data Service - Closed User Groups

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.



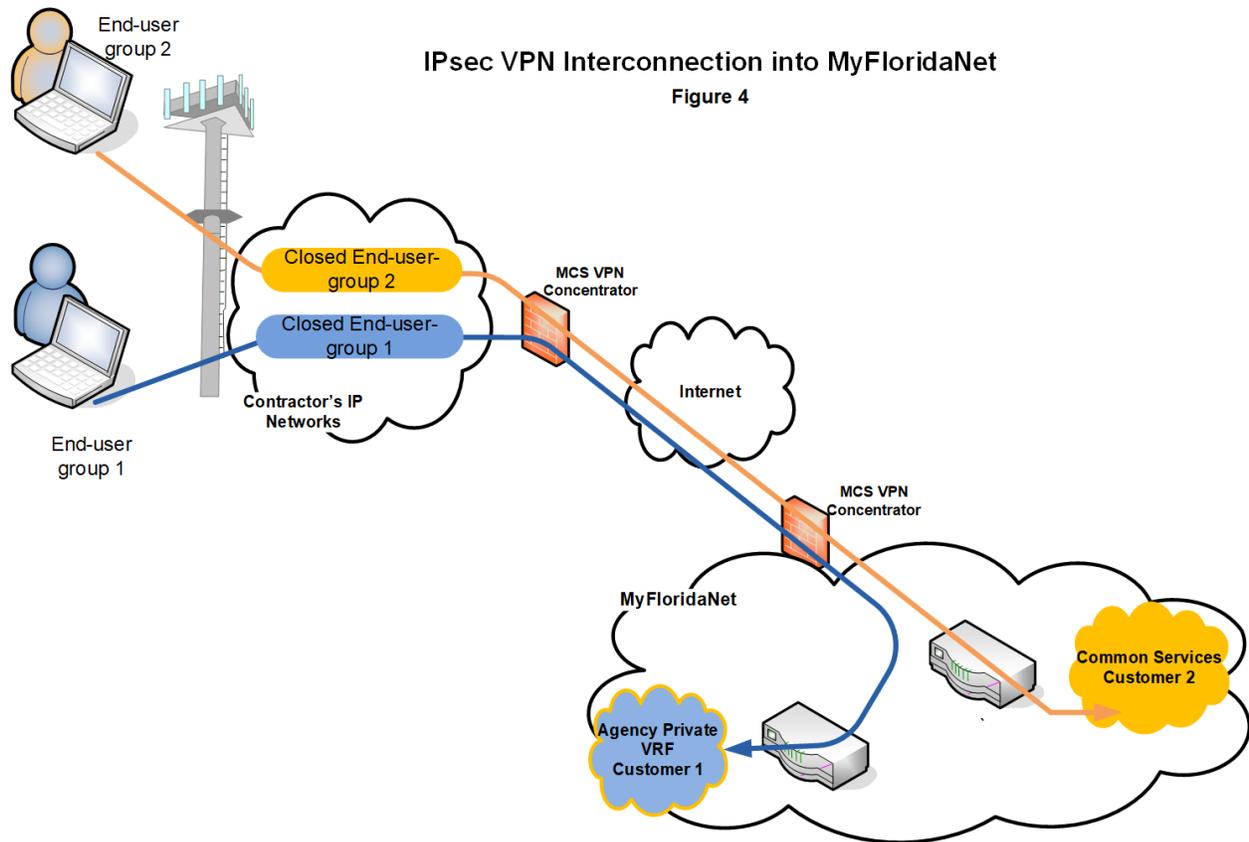
No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

### 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, or an alternate solution, as proposed by the Contractor and accepted by DMS through the Change Request process. 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 secondary MFN IPsec concentrator. Within Figure 4 above, this is shown as "MCS VPN Concentrator" directly adjacent to the MFN section. This is currently rented from and managed by the MFN contractor. 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 specific to the Contractor's owned network to network connections and devices. 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 (or an alternate solution, as proposed by the Contractor and accepted by DMS through the Change Request process) 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 fallback processes.
6. Describe how you will maintain the security of your MFN interconnection.
7. Respondents may also propose an alternative design.

#### **Advantages of Verizon Wireless Private Network**

Verizon has been providing a Network to Network Interface into the MFN Network utilizing our Private Network Platform, as highlighted below, since 2012. The solution provides redundant connectivity into the VZ Network with a primary connection in Charlotte, NC and redundant/failover connection in Nashville, TN. As of 2018 these connections terminate into the new MFN2 network in Tallahassee, FL as the primary with Miami, FL being the redundant/failover connection. During migration to the MFN2 network, failover was tested and proved successful as did the successful migration of several live Closed User Groups.

Verizon Wireless Private Network enables DMS to use the state existing MFN network routing schemes and network protocols to manage the state wireless devices via a secure link between the wireless environment and agency local area network (LAN).

Verizon Wireless Private Network (Private Network) is a comprehensive solution that joins wireless devices to the organization's internal IP network using a dedicated connection that isolates data from the public Internet. It extends a corporate IP network to wireless devices, while enabling your IT department to maintain the control and manageability that it needs. With Private Network, organizations can take charge of their evolving networks by:

- Avoiding the exposure of wireless devices and internal networks to the inherent risks of solicited public Internet traffic.
- Controlling which wireless devices can connect to the network.
- Controlling which network resources the wireless devices and machines can access.
- Leveraging the convenience of mobility and wireless technologies to introduce new opportunities.

With Private Network, organizations can add devices to their own internal networks, with their own IP addressing, to be managed by their own support personnel. This empowers them to make wireless solutions part of their infrastructure and extend their core-computing networks farther, faster and easier. Private Network is also compatible with Verizon Mobile Device Manager. And organizations can be confident knowing that their Private Network is backed by the coverage, speed and reliability of Verizon. We can help organizations make the most of wireless communications to securely and cost effectively power their networks.

#### **Enhanced Features of Private Network**

##### **Tiered Hierarchy**

Tiered Hierarchy design provides separate accounting/billing of data traffic for customers with multiple agencies, business units, departments or organizations whose data traffic traverses over a single Private Network. Billing can be separated for each agency, business

unit, and department or organization profile. It allows the financial cost to be attributed to the correct company or department.

#### **Dynamic Mobile Network Routing**

Dynamic Mobile Network Routing (DMNR) allows accessing IPv4 addresses of devices that are connected to wireless router for easier support and management. DMNR is a network-based mobile technology providing dynamic routing and support for mobile or stationary routers in primary wireless access or automatic wireless backup configurations using Mobile IPv4-based Network Mobility (NEMO) protocol, without the need for Generic Routing Encapsulation (GRE) tunnels or network address and port translation. This delivers the any-site-to-any-site connectivity wireline customers expect when solutions extend the corporate network (e.g., intranet).

#### **Service Based Access**

Service Based Access (SBA) is an optional configuration for Private Network that allows subscribers to have the same experience with assisted GPS (aGPS); Multi-Media Services (MMS); and Visual Voicemail as they have on the consumer network but with the added security of Private Network.

#### **Traffic Management**

Traffic Management is a Private Network feature, available only for Verizon's 4G LTE devices, that provides customers with a premium and differentiated network experience. Private Network Traffic Management uses Quality of Service (QoS) technology to enable application differentiation over the LTE Private Network using standards-based IP packet marking.

Private Network Traffic Management has a Monthly Access Fee per user according to the level of service selected. Private Network Traffic Management subscribers have access to two Classes of Services (CoS), Enhanced and Premium, to prioritize applications.

- **Enhanced:** Allows mapping of business applications up to a maximum of 2.0 Mbps Business Critical CoS, with the remaining best effort applications mapped into the Best Effort CoS utilizing the remaining available LTE bandwidth.
- **Premium:** Allows mapping of business critical applications up to a maximum of 12 Mbps Business Critical CoS, with the remaining best effort applications mapped into the Best Effort CoS utilizing the remaining available LTE bandwidth.

Private Network Traffic Management subscribers have the flexibility of mapping their business critical applications to the respective CoS.

Private Network Traffic Management (PNTM) capability is not available when roaming off the Verizon wireless network since the roaming partner's network cannot establish the dedicated bearer, i.e., channel created between the device and gateway for transporting IP packets, used for PNTM.

#### **International Roaming**

International Roaming enables Private Network customers to have connectivity for their devices (such as Smartphones, Tablets, Machine-to-Machine/Internet of Things) when leaving the Verizon wireless network footprint (a.k.a. "outbound roaming") on approved international roaming providers' networks, whose wireless technologies include GSM, UMTS, HSPA, or 4G LTE.

#### **Account Records Streaming**

Private Network supports the option to have a direct feed of accounting records (Start and Stop fields/attributes) sent from the Verizon Data Streaming Server (DSS) to a designated

customer accounting server at no additional cost. The customer will receive the raw data (without modification or customization) can be parsed per the customer's reporting needs. The customer's receiving server must be capable of receiving and acknowledging raw accounting information.

### **Split Data Routing**

Verizon Wireless Private Network customers looking for a more efficient way to route data traffic can do so with our split data routing solution. When you split the data flow, you can send secure private data one way and public traffic another. This separation reduces a customer's cost of managing in-house network capacity and firewall policies. Dual Access Point Name (APN) capability allows split data routing where the device uses multiple data connections – one to the Internet and another to Private Network.

### **How it Works**

The functionality is device-driven, where the APN Class 3 (VZWINTERNET) data traffic is associated with an Internet designation and the APN Class 6 (the APN associated with the customer's Private Network) data traffic is for the Private Network.

- Device establishes data connectivity for APN Class 3 and 6.
- Device routes data to the designated APN Class 3 or 6 Packet Data Network.
- Customers must ensure that device security is implemented to protect private data from Internet data and to preclude:
  - mixing data packets associated with the Internet and Private Network
  - Internet data from traversing Private Network and private data traffic from the Internet
  - any Internet threats (e.g. virus, malware) from corrupting private data
- Verizon will route Internet data to our Public gateway and private data to the Private Network gateway with the connection to the customer's network.

The wireless device selected must have the ability to:

- Support multiple APNs including APN Class 3 and Class 6.
- Route Internet designated data traffic using the APN Class 3 and data traffic categorized for the customer's Private Network using APN Class 6.
- Separate Internet and private data traffic to ensure Internet data uses APN Class 3 only and private data uses APN Class 6 only.

### **Split Data Routing with Multi-Party Billing**

Split Data Routing with Multi-Party Billing extends Verizon's billing and rating architecture to take a single MDN (Mobile Destination Number) and assign multiple financially responsible parties based on various service-based data streams from the same device.

- Only available on government-liable devices with Verizon's Private Network.
- Verizon bills enterprise for Mobile Private Network traffic and bills other enterprises/consumer for Internet traffic.

### **Verizon's Commitment to Industry Standards**

Verizon complies with industry, statutory and regulatory requirements regarding safeguards and controls of protected information: Federal Communications Commission (FCC), Department of Justice (DoJ), Sensitive Personal Information (SPI), Customer Proprietary Network Information (CPNI), Payment Card Industry (PCI) & Intellectual Property.

Established cellular industry and performance standards serve as the foundation for our engineering, design, operation and quality assurance programs. Verizon has created enterprise-wide policies that conform to the International Organization for Standardization (ISO) 27002.2005 and National Institute of Standards and Technology (NIST) standards for the protection of customer and employee information. These policies cover security issues, such as account management, password standards, server configuration and a wide range of security topics.

Verizon Wireless executives are active participants in national wireless industry associations and organizations focusing on the latest technology and public policy developments. They are invited regularly by these groups to take on leadership positions to lend their knowledge and expertise.

#### **DMS Private Network Design**

Today, Verizon Wireless uses VRF isolation to isolate closed user Groups and handoff traffic to the IPsec tunnels provisioned across the Internet.

The Verizon Wireless Private Network offering is built around isolating the SUNCOM Client IP traffic from all other Private Network and Consumer traffic. At all points between the mobile device and the MFN network the SUNCOM Client IP traffic is encapsulated in a tunnel, isolated in a dedicated VLAN, VRF, PVC, etc. There are no “backdoor” or alternate paths into or out of this isolated environment which would allow access from any other entities or devices.

It is a standard option to permit or deny traffic within and between different SUNCOM Closed user Groups. This can be done as granularly as needed such that Group A could be permitted to communicate with other Group A devices as well as Group B devices, whereas Group C could be blocked from talking to other Group C devices as well as Group A and Group B devices.

Verizon has created and maintained closed user groups. The closed user group is designed and configured so to isolate one closed user group’s IP traffic from all other. Each closed user group correlates to one unique NNI IPsec tunnel in such a manner, the tunnel traffic can be mapped into the appropriate MyFloridaNet MPLS VRF associated with the closed user group by the MFN Service Provider.

#### **Redundancy**

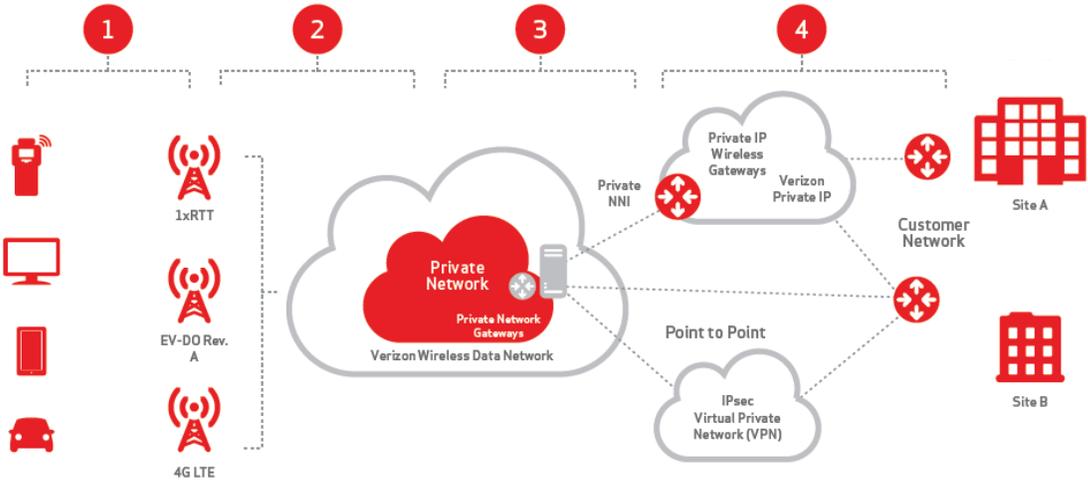
Network redundancy provides a backup path when the primary connection experiences a failure and can no longer support data traffic. Each Private Network is built with a primary and secondary gateway where the secondary gateway acts as a hot standby to provide support when the primary gateway has experienced a failure and can no longer operate. Once the primary gateway becomes operational, traffic will be redirected to the primary gateway, and the secondary gateway will go back into hot standby mode.

Connectivity redundancy provides a backup path when the primary connection between Verizon and the enterprise network experiences a failure that prevents traffic from moving over the connection. Verizon requires the connectivity redundancy.

#### **Verizon Wireless Private Network Security**

Data travels from wireless devices connected to the Radio Access Network, through the Private Network to a dedicated connection to the organization’s network. Each organization has its own Private Network whose traffic is kept isolated from the public Internet, avoiding unnecessary risk associated with unsolicited public Internet traffic. Only authorized subscribers may send and receive data.

With Private Network: 1) Devices are authenticated and authorized for each Private Network (only authorized data can traverse the designated network). 2) Data are routed per the customer-specific IP pools. 3) Dedicated Private Network Gateways are designated. 4) A direct connection is created between Private Network Gateways and the customer premises router. [See following diagram.]



**Connectivity Options**

With Private Network, you have the flexibility to connect in a way that makes the most sense for your network’s configuration.

- **Virtual private network (VPN).** You can use VPNs to create a secure tunnel between your internal network and the Verizon gateway. Because your IT staff is probably familiar with setting up and managing VPN environments, this can be a simple and effective solution. With this option, all traffic from the Private Network gateway router is encrypted and sent over the tunnel, through the public Internet, to your organization location. It is possible to encrypt the entire path by layering additional technologies.

IPsec Parameters		Verizon Private Network VPN Complies Y/N
IKA (SA)	Main Mode	Y
Encryption Strength	3DES	Y
Authentication	Pre-Shared Key	Y
Diffie-Hellmans (D-H) Groups	2 or 5 (group-5 preferred)	Y
Perfect Forward Secrecy	Pfs	Y

Data Integrity Hash Algorithm	SHA	Y
IPsec (SA)	Quick Mode	Y
Security Association (SA) Lifetime	86,400 seconds (maximum)	Y
Authentication Type	HMAC-SHA	Y
Security Association (SA) Lifetime	28,800 seconds (maximum)	Y
Simultaneous Active Tunnels	1,000 (minimum)	Y

- **Dedicated physical circuit [Point to Point].** A dedicated physical circuit can be installed at your location for the sole purpose of connecting to Verizon to complete the Private Network build-out. Because the circuit is dedicated, the entire bandwidth is available for use. No data traverses the public Internet, so the use of additional encryption technology is optional.
- **Verizon Private IP.** If your organization is already a Verizon Private IP customer, you can use that Private IP network to connect to the Verizon wireless network. This approach enables you to implement Private Network without affecting your existing network topology. If your organization is not a Private IP customer, Private Network and Verizon Private IP can be implemented together. Either way, you can combine the benefits of wireless with the benefits of a Multiprotocol Layer Switching (MPLS) network. When implemented with Verizon Private IP, all wireless data traffic can be routed directly to any location connected to Private IP. This simplifies network routing scenarios and provides redundancy for business continuity. Since both Private IP and Private Network are within the Verizon product portfolio, you have a single contact for product support. Customers also have access to additional hosted services from Verizon that could help drive increased return on investment and position your organization for the future.
- **Zero Tunnel Connectivity:** Zero Tunnel connectivity is designed for customers that require only mobile-to-mobile communication that does not require connectivity from the Private Network gateway to the customer premises (i.e., Private IP, dedicated circuit, VPN). Zero Tunnel configuration has no communication outside of the mobile IP pools and can be designed as a hub and spoke configuration where the central wireless device at the customer data center provides access to the customer-hosted applications to field/mobile devices.
- **Cloud Access:** Private Network can be constructed with connectivity to cloud service providers using Verizon's Secure Cloud Interconnect.

#### IP Addressing

Private Network supports Dynamic and Static IP addressing while offering a variety of IP addressing options that provide several levels of accessibility, protection and manageability. These options include enterprise-owned, private IP address assignment to the devices, essentially making the device a virtual extension of the wired enterprise network. This enables enterprise IT administrators to manage mobile stations and LAN devices using the same tools and techniques. For example, organizations can use the same firewall and routing schemes, and the IT administrators define which users get Internet access. This makes it easier for

enterprise IT administrators to manage and monitor network usage and enforce company IT policies.

As more and more devices are being activated using IP, the availability of IPv4 addresses is greatly diminishing. Since the world is running out of IPv4 addresses, IPv6 has become the new standard for IP addressing. Enterprise and Government customers are transitioning to IPv6 to continue to grow and enable new, innovative services to be developed because more devices can be connected. Private Network's initial release of IPv6 support offers Dynamic IP assignment. It offers capabilities to apply IPv6 addressing to the wireless device's packet data connection and to the connection used between the Verizon Wireless Data Network Private Network Gateway and customers premises.

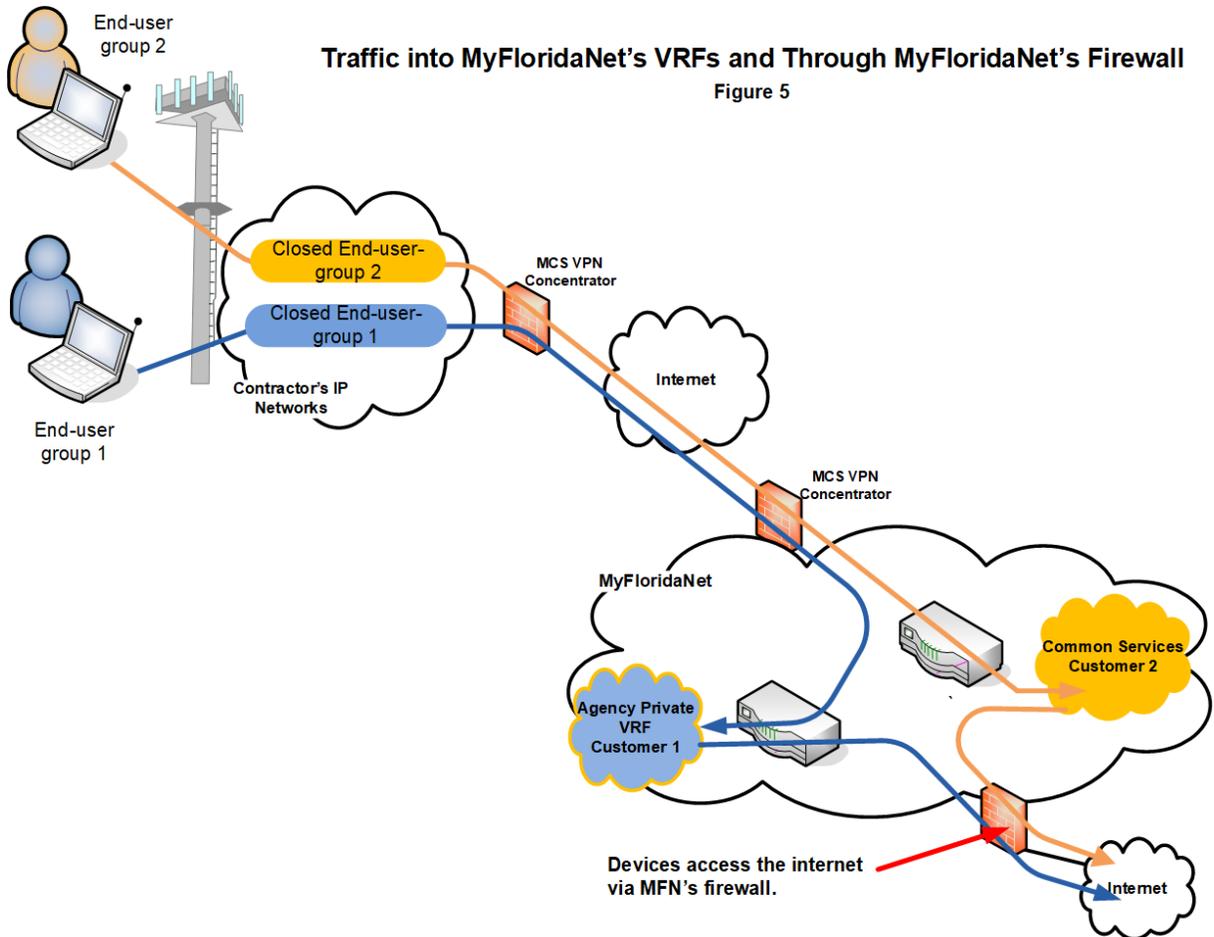
### 3.7 Wireless Data Service –Traffic Mapping into MyFloridaNet

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.



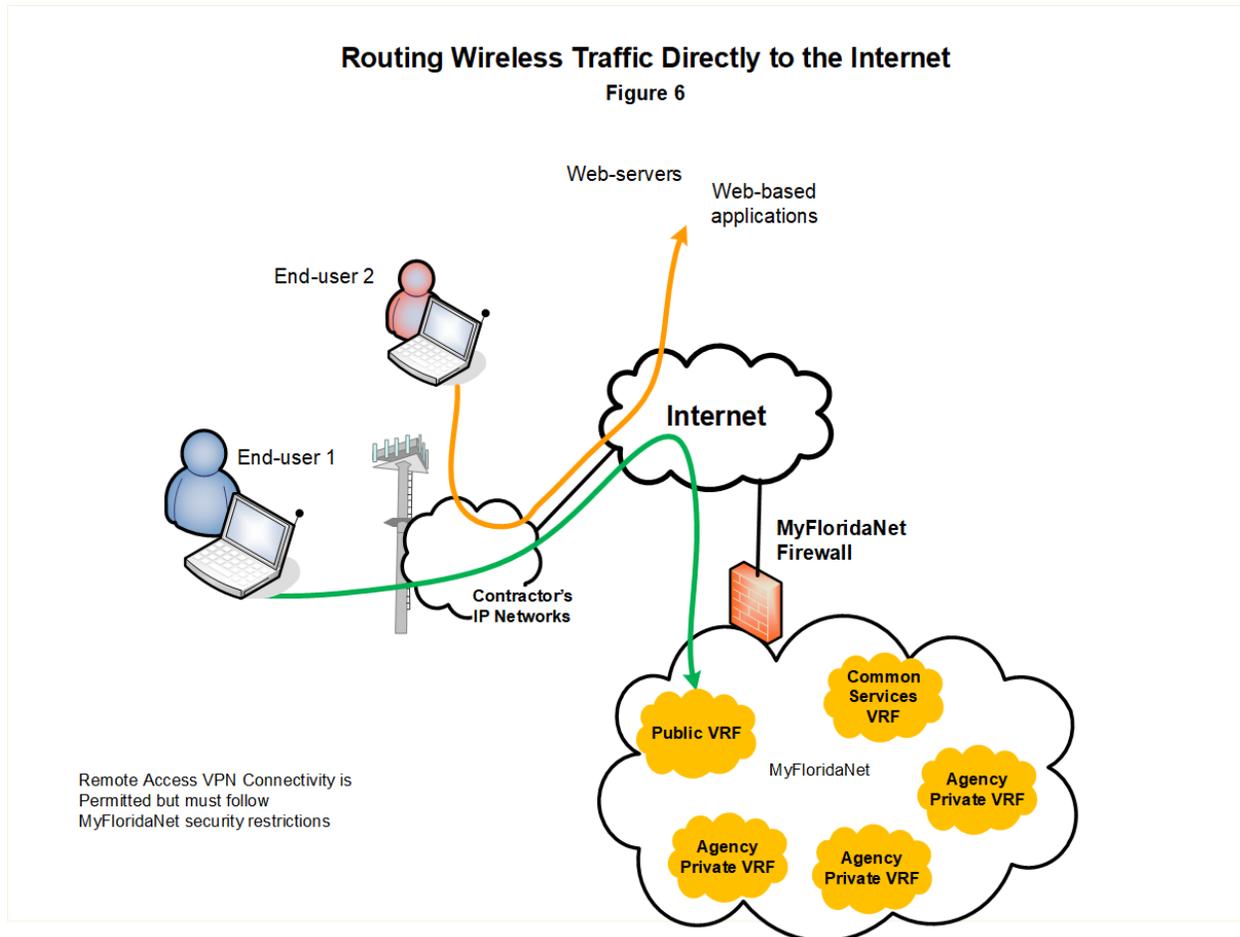
No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this subsection.

### 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.



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 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/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.

#### **Verizon Wireless Network Coverage**

Verizon Wireless operates the nation's most reliable wireless network, with more than 120.3 million wireless retail connections (September 30, 2020).

- Our 4G LTE network is available to more than 99 percent of the U.S. population and covers 326.1 million people over more than 2.6 million square miles.
- LTE Advanced - Verizon customers in more than 2,000 markets can access the benefits of carrier aggregation and those in 1,100 markets can access 4x4 MIMO (Multiple Input, Multiple Output) and 256 QAM (Quadrature Amplitude Modulation) in addition to carrier aggregation

Up-to-date coverage maps are made publically available online. Future plans for enhancement and expansion of Verizon's coverage areas are considered confidential and proprietary. Our online Coverage Locator tool depicts our wireless coverage area on a national map and enables you to zoom into any local area by entering that area's ZIP Code or the city and state information. The maps rendered show approximations, based on our internal data, of where coverage for various services is available.

- Our online domestic Coverage Locator tool can be accessed at:  
<https://verizon.com/coverage-map/>
- Our online international Coverage Locator tool can be accessed at:  
<https://verizon.cellmaps.com/>

We have also provided coverage maps below for DMS' convenience, review, and consideration listed as "Attachment A" in the 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

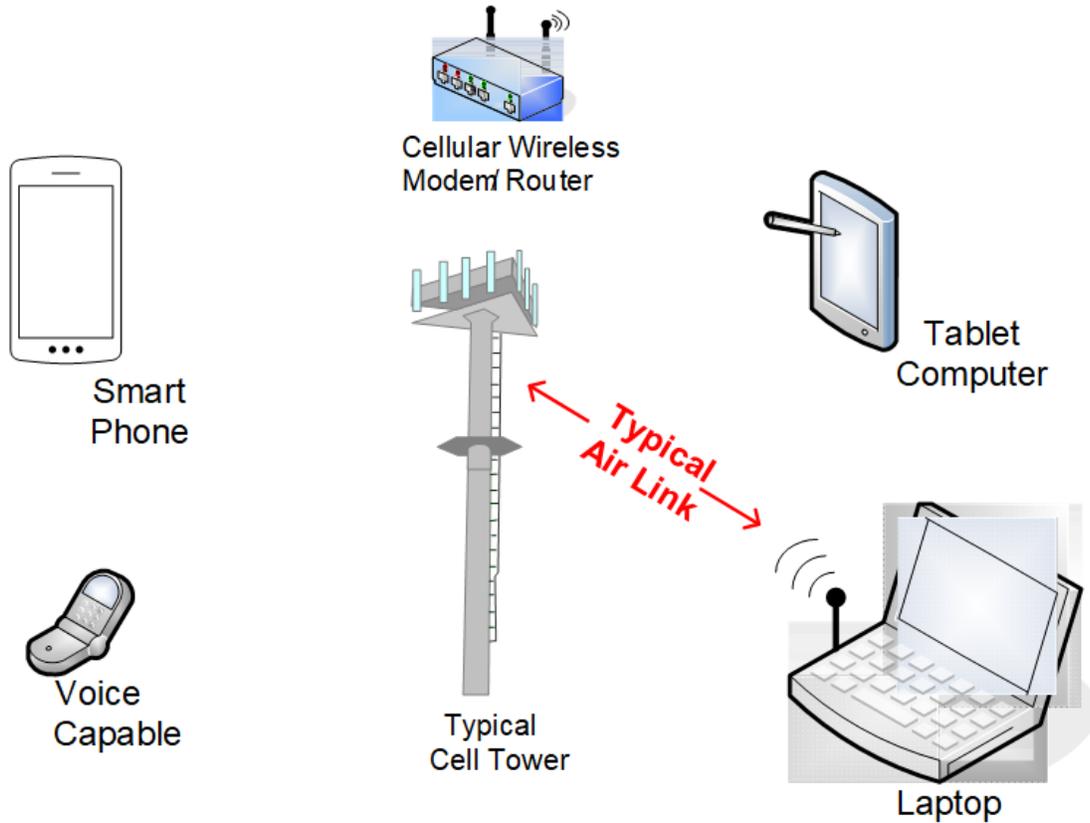
This subsection is applicable to both WVS and WDS.

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, or a generalized description deemed acceptable by the DMS Contract Manager, 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.

#### **Performance, Reliability, and Security**

DMS expects performance, reliability and security from your wireless network. The increasing numbers of factors that are beyond your control heighten that expectation. The security team at Verizon Wireless works tirelessly behind the scenes to keep the network running while monitoring, identifying and eliminating security threats and malicious attacks before they reach a single mobile device under your supervision.

Our reputation for reliability and peak performance depends on the security of our network. Our sophisticated security infrastructure utilizes firewalls, routers, monitoring systems, software, device standards and security expertise to keep mobile communications and data out of the hands of hackers and data thieves so you can keep your workforce productive, connected and mobile.

Data security is an integral part of our corporate strategy. Addressing security needs is paramount to delivering solutions that meet the demands of a mobile workforce. Verizon Wireless deploys a multipronged strategy for network security that combines the expertise and resources of our internal engineering teams, external software development partners and vendors of the various commercial applications and products we offer. Our security strategy includes:

- **Wireless Standards and Services:** Verizon operates CDMA, 4G LTE and 5G standards-based wireless access technologies, which offer robust security-based encoding, authentication and encryption. Wireless services are enabled and designed to enhance the mobile experience while maintaining security.

- **Policy and Governance:** Verizon has created enterprise-wide policies that conform to the ISO 27002.2005 and NIST standards for the protection of customer and employee information.
- **Vulnerability Management:** Verizon has implemented a four-stage (Discovery, Assessment, Remediation and Validation) vulnerability management model to guard against vulnerabilities.
- **Risk Management:** Verizon conducts penetration testing by both Verizon employees and contracted third-party entities; the results of the security risk assessment are used to decide whether or not to move forward with a commercial launch of the product.
- **Security Monitoring & Response:** Verizon has a dedicated team of certified security professionals (CISSP, GIAC) as part of the Network Cybersecurity Center (NCC) to ensure incidents are identified, the method by which the breach occurred, and to make all necessary changes to prevent a reoccurrence of that event. The NCC team is on-call on a 24/7 basis.
- **Physical Security:** Verizon has implemented partitioned access control systems by which access is granted based on individual needs. The wireless Network centers and cell sites are designed and equipped with intrusion detection and alarm systems and alarm conditions of all types including those from the access control systems (ACS) and the intrusion detection systems (IDS) are monitored and logged in at least three locations.

Verizon complies with industry, statutory and regulatory requirements regarding safeguards and controls of protected information: Federal Communications Commission (FCC), Department of Justice (DoJ), Sensitive Personal Information (SPI), Customer Proprietary Network Information (CPNI), Payment Card Industry (PCI) & Intellectual Property. See also attached information security document for detailed information regarding how Verizon's information security policies and practices will support the maintenance of security of DMS' MFN interconnection.

### 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 ship the specified quantity (up to 100 of each type (basic, Smartphone, MiFi, USB) requested) of activated wireless (WVS and WDS) devices within twenty-four (24) hours of receiving the ESF-2 request, and deliver within forty-eight (48) hours. 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.

#### **Resilient by Design**

Our wireless infrastructure is designed to provide customers with a resilient network that is fault-tolerant and cost effective. Verizon's two wireless Network Operations Centers (NOCs) serve as the hubs of our regional network operations. The NOCs are located in Bedminster, NJ, and Westlake, TX, and operate 24/7/365. The NOCs detect network failures, diagnose the failure, send out repair personnel and track the problem to conclusion. NOCs monitor cell sites, mobile switching centers, mobile data switching systems and transmission facilities for potential problems. If an outage occurs, a field engineer is dispatched as soon as possible to correct the problem and bring the cell site back on line.

Equipment electronically tracks system alarms and immediately reports them to our surveillance engineers to investigate and act on promptly. When an alarm is activated, the system gives detailed information, including cell location, the switch location, contact numbers for local commercial power companies, police and fire departments, and even driving directions to the cell site. The network management system also gives our network surveillance engineers the ability to perform remote diagnostic procedures and, in some cases, restoration of service.

#### **Network Surveillance and Alarm Monitoring**

We continuously monitor all of our data networks for congestion. We respond immediately to increased capacity needs where necessary and use internal statistical information, drive

testing and a third-party monitoring service to evaluate network performance. Peaks of concentrated traffic may, from time to time, cause heavy network usage; however, we engineer our systems to support a typical volume during the busiest hours of the day.

The Data Network Operations Center (DNOC) has procedures in place that are designed to troubleshoot and/or resolve problems that may arise. These include the following:

- Availability of a Data Help Desk and DNOC for problem resolution
- Prompt investigation of problems;
- Notification of key individuals, including wireless data engineers and technical experts, if necessary
- Establishment of estimated time frames for actions and resolution
- Upon resolution, notification to the customer

#### **Alarm Procedures**

##### **Business Hours (08:00 - 17:00)**

During business hours, surveillance engineers will alert regional network operations of critical alarm conditions. Regional operations will respond normally within one hour, providing the NOC of estimated time of arrival and service restoration. It will also notify the NOC of trouble resolution.

##### **After Hours (17:00- 08:00)**

After business hours, the NOC will initiate corrective actions on critical alarms. Failure to remotely diagnose and correct equipment problems will result in a page to regional "night watch" personnel. Regional operations will respond normally within one hour, providing the NOC of estimated time of arrival and service restoration. It will also notify the NOC of trouble resolution.

##### **Outage Notification**

Unscheduled outages will be reported immediately to an automated voicemail system that will notify appropriate Verizon personnel. System engineers will coordinate scheduled maintenance outages.

### 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. All reports are to be provided at the enterprise level (i.e., for all Customers that utilize this Contract) and shall exclude any information regarded as Customer Proprietary Network Information (CPNI). Should the Contractor provide the reports through a portal, dashboard or other self-managed web-based tool, the Department's access must allow enterprise reporting.

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. Notifications, SLA B7, B8, B9 (Subsection 3.19.4)
  - f. Weekly Transition Status Reports during Transition (Subsection 3.24)
  - g. Project Status Report, SLA-D3 (Subsection 3.26.2.3)
  - h. Incumbent Contractor Weekly Migration Report, SLA-D7 (Subsection 3.26.5)
  - i. Monthly Public Safety Service Plans and Devices Report, SLA-E1 (Section 4)
  - j. Direct-Billed Accounts Monthly Report, SLA-G2 (Subsection 6.4)
  - k. 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, for data and information that is available and accessible to Contractor which will be at no cost and include a report delivery timeframe within two (2) Business Days of receipt of request, unless due to the amount of data required, DMS grants a longer timeframe after discussion with the Contractor.

Given the statements in this subsection:

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

#### **Reports, Updates, and Notifications Requirements**

Verizon currently provides DMS with reporting and data for contract oversight: This reporting includes the requisite updates and notifications in accordance with the requirements of its existing contract with DMS-1011-008C. Upon contract award, Verizon will work with DMS to ensure mutually agreeable reporting and notification criteria as detailed in section 1a. through 1m. of the agreement are met or exceeded.

In addition, DMS can take advantage of the reporting available through Verizon's My Business online web portal to meet the requirements of 2a. through 2f. listed above as described in Section 3.20 of the SOW.

### **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 it is the last billing cycle of the service and credits exceed any payment due to the Contractor, 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

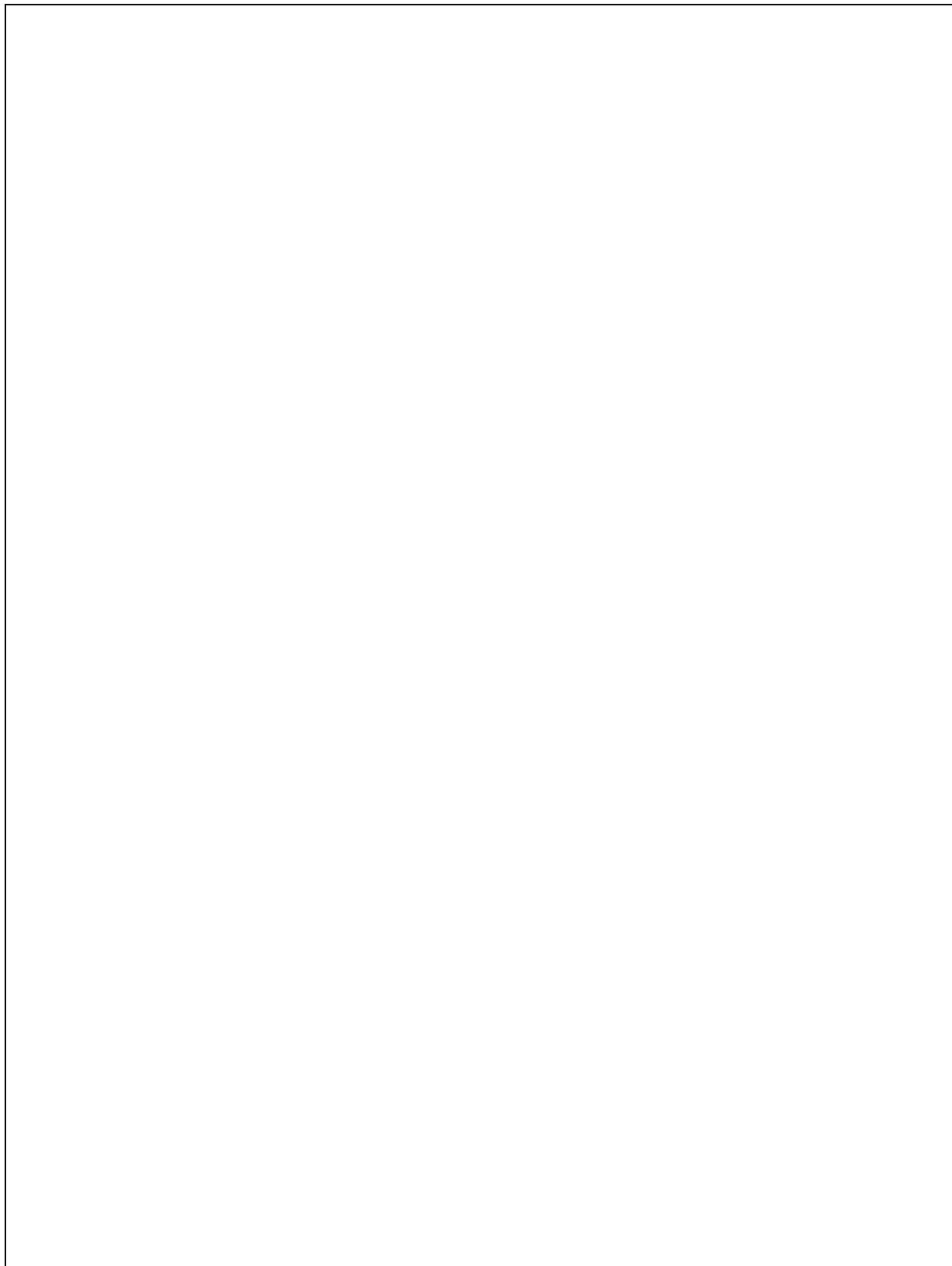
1. SLAs apply regardless of whether the violation was a result of human error, poor engineering design, tardy dispatch, dispatch without required repair or diagnostic tools, exceeding the scope of an approved maintenance change request that causes performance degradation (deterioration in quality, level, 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 Item 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. will be coordinated with the Contractor and 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. Electronic notifications are required in advance of planned maintenance during instances of significant service impact, including performance degradation, over a generalized area. **Attachment C, SLA-B7.**

Electronic notifications are required for emergency and unplanned outage activities when the activity may cause a significant service impact, including performance degradation, over a generalized area. Notifications must include an impact statement, date, time, reason for emergency or unplanned outage, and duration if available. The reason for emergency or unplanned outage and duration may be sent in a follow-up notification. Changes to the estimated duration should also be sent (if available).

**Attachment C, SLA-B8 and SLA-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.

### Customer Support

#### Monthly Escalation Reports

Verizon will support DMS with a monthly basis and detail the number of calls and emails related to requests for escalation assistance for technical and administrative support.

#### Quarterly Zero Usage Reports

Verizon will continue to provide a high-level summary of End-user devices that show no usage (i.e., zero minutes, zero texts, and zero data) quarterly. You can also obtain this report through Verizon's My Business online portal.

#### Escalation Process

Your authorized contact also has the option of contacting your Global Enterprise Advisor/Account Manager for assistance in managing your account.

Your first point of contact for trouble with your voice or data services is our Business and Government Customer Operations (BGCO) organization. Members of our BGCO teams can conduct rudimentary device and network troubleshooting. Concerns related to quality of service, such as the inability to make or receive calls, will be assigned the highest priority and receive prompt attention. A staff supervisor is available during the BGCO team's hours of operation.

In the event BGCO representatives cannot resolve a situation and escalation becomes necessary, the following account team members may be contacted.

Contact	Name	Phone Number
Client Partner - Public Sector, Verizon Business Group	Tom Madden	850.294.5171
Global Enterprise Advisor	Paris Perkins	1.800.757.0699 ext. 2103721

If the escalated situation is not effectively resolved or the process of resolution is not effectively initiated within 24 hours of the request, we suggest contacting the staff management level.

Contact	Name	Phone Number
Solutions Executive Federal	John Amorielle	843.670.6648
Senior Manager- Business Government Customer Operations	Andrew Cuozzo	443.820.4002

A highly sensitive situation that requires further escalation may require director level involvement. In those rare situations, we suggest you request a call back from the individuals below in the order in which they are listed.

<b>Contact</b>	<b>Name</b>	<b>Phone Number</b>
Director- Business and Government Customer Operations	Joseph Chuisano	410.694.3400

Complex situations may require research and may take longer to resolve. In these situations, we will research, resolve the issue and report back to the employee or authorized contact when the issue is resolved.

### **Notifications**

The Network Event Notification (NEN) Program is a courtesy service that provides notice to your organization about planned and unplanned network maintenance, including ongoing updates and issue resolution for affected services. Network event notifications are issued via email and the same information is maintained online through a self-serve NEN portal for up to four weeks. Your organization may choose to receive notices on unplanned and/or planned events.

### **Events That May Trigger Notification and Notification Process**

Network event notifications will issue to your organization's identified contacts, providing information about planned and unplanned maintenance events that may impact your service with us.

A planned network event is sent to your identified contact up to two weeks before any planned network maintenance.

An unplanned network event is sent when we receive confirmation there has been an unplanned disruption of service on the network. Events that may trigger automatic notification include a service condition that is significantly below our normal service operational thresholds. Because the service outage notification is sent when our systems identify a possible outage, your identified contact may receive the notification regardless of whether or not your end users are affected.

There are four types of unplanned network event notifications:

- Initial – Sent when the disruption is confirmed
- Update – Sent every half hour until the service is restored
- Restored – Sent when the issue is resolved and service is restored
- Informational – Sent when it has been determined that a brief service disruption occurred on the network, but was resolved before an alert was issued

If you receive a notification, there is no need to take any action. Our network engineers will be working to resolve the issue and you will receive an update when it is resolved.

Both planned and unplanned event notifications will include the following information:

- Start Date
- Start Time
- Severity Level [(High or Low for Planned), (High for Unplanned)]
- Affected Service (e.g., 4G LTE, Enterprise Messaging)
- Affected Location: ( e.g., Dallas, Texas)
- Affected Counties: (e.g., Freestone, Grayson, Kaufman, Fannin, Rockwall, Dallas, Henderson, Collin, Hunt, Ellis, Van Zandt, Navarro, Denton)
- Tracking Number: (e.g., 123456)

**Self-Service Portal**

The self-service NEN portal includes the same network event information as is contained in the notification emails. The information is presented in user friendly views with data maintained for up to four weeks.

You can access the NEN portal directly through Verizon's My Business online resource or via <https://m2m.verizonwireless.com/m2m/index.html#nenManageEnrollment>

**Enrollment by Services**

Your organization may choose to receive notifications when all or at least one of the following covered services is operating below normal thresholds:

- 1X
- 4G LTE
- 3G Network Extender
- 4G Network Extender
- HD Voice (formerly known as Advanced Calling)
- Call Processing
- Domestic Roaming-Data
- Domestic Roaming-Voice
- Enterprise Customer Mapping Solution
- Enterprise Messaging
- EV-DO
- Enhanced Virtual Private Network
- International Roaming Data-GSM
- International Roaming Voice-GSM
- IOT Grid Wide Utility Solutions
- Location-based Service
- LTE in Rural America
- Network API
- OTA 4G Device Management
- One Talk
- Push To Talk
- Push To Talk Plus
- Blackberry
- SMS & Voicemail Notification
- Static IP (Eules, TX)
- Static IP (Hickory Hills)
- Static IP (Plymouth Meeting)
- Static IP (Sunnyvale)
- ThingSpace Manage
- Usage Controls
- Verizon Digital Signage

- Verizon Messaging Gateway
- Voicemail & Notification
- Visual Voicemail
- Visual Voicemail - iPhone
- Voice Cypher
- Wi-Fi Calling

The following are for Private Network (you may select all or at least one option from the list below):

- Verizon Wireless Private Network - Aurora
- Verizon Wireless Private Network - Birmingham
- Verizon Wireless Private Network - Branchburg
- Verizon Wireless Private Network - Charlotte 1
- Verizon Wireless Private Network - Charlotte 2
- Verizon Wireless Private Network - Columbus
- Verizon Wireless Private Network - Eules 1
- Verizon Wireless Private Network - Eules 2
- Verizon Wireless Private Network - Hickory Hills
- Verizon Wireless Private Network - Las Vegas
- Verizon Wireless Private Network - Lodge (Detroit)
- Verizon Wireless Private Network - Omaha
- Verizon Wireless Private Network - Plymouth Meeting
- Verizon Wireless Private Network - Redmond Ridge
- Verizon Wireless Private Network - Rocklin
- Verizon Wireless Private Network - Westborough

The Network Notification Program is offered as a courtesy only. In no event shall the failure to provide outage notifications subject Verizon to penalties or damages of any kind. Verizon reserves the right to modify or discontinue outage notifications at any time.

#### **Support Team**

Our Business and Government Customer Operations (BGCO) teams are trained to address your inquiries related to our wireless services. They operate out of three full-service centers across the country:

- Hanover, MD, Mon - Fri, 8 AM - 7 PM ET
- Alpharetta, GA, Mon - Fri, 8 AM - 7 PM ET
- Salt Lake City, UT, Mon - Fri, 8 AM - 7 PM MT

The BGCO team assigned to your organization is determined by the geographical area of your headquarters location and can be reached toll-free at 800-922-0204.

In the event your employees seek assistance after your BGCO team's hours, our standard full-service wireless Customer Care team is available from 8 AM - 9 PM, Monday through Saturday, and 8 AM - 5 PM on Sunday, in each time zone. Customer Care can be reached toll free at 800-922-0204 and airtime-free at \*611 from the wireless device. These Customer Care representatives are not specifically trained to support our corporate accounts, but can address many of your employees' inquiries.

### 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. equipment definitions and specifications;
8. maintenance information;
9. product configuration options; and
10. may include other information as mutually agreed to and approved in writing by the DMS Product Manager, such as whitepapers and diagrams.

Given the statements in this subsection:

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

**Contractor's Portal**

Verizon's My Business online resource is a self-service tool that enables your organization to manage your wireless accounts. You can view and pay your bills, create business structures, view select reports and maintain your account. Additionally, your designated employees can purchase equipment, accessories and service using My Business' functionality.

With My Business you can:

- Receive online reporting in a consolidated manner or broken out by account or wireless number
- View individual phone information, such as airtime usage and call detail
- Modify mobile number information to allow for specific, customized analysis

My Business provides a wide variety of comprehensive standard wireless reports, such as:

- Charges Reports

- Additional Charges – details monthly access, equipment charges, service & feature charges and taxes
- Airtime Charges Detail – Details call usage and charges
- Airtime Charges Summary – A summary of all your charges including taxes, services & features, access, airtime, etc.
- Analyze Phone Charges – Detail view of charges and calls
- Analyze Roaming Charges – Detail view of roaming calls
- Most Expensive Calls - Calls with the highest charges
- Purchase – All purchase activity details and charges
- Usage Reports
  - Account Unbilled Usage – Current unbilled usage for the account
  - Billed Data Details – Data session details for multiple wireless numbers displayed simultaneously
  - Billed Messaging Details – Message details for multiple wireless numbers displayed simultaneously
  - Call Summary – Summary of voice usage and charges for each wireless number
  - Data Summary – Summary of data, messaging and purchase charges for each wireless number
  - Grand Total – Comprehensive Summary. Details total charges and total minutes.
  - International Travel Data High Alerts – A weekly list of high data usage alerts sent for current global data usage by wireless number.
- Other Reports
  - Active Features – List of all features currently on your lines of service
  - Billing Structure – Your organization’s My Business users and their access within the online resource structures
  - Business Account Analysis – View a summary of your organization’s discounts and the amount of money saved, upgrade status and overage charges
  - Company Users – Your organization’s My Business users and their permissions within the online resource
  - Customer Invoice Management – A report with your own defined hierarchy
  - Deactivated Phones – Wireless numbers that have been deactivated
  - Device – Comprehensive summary of devices and upgrade eligibility

You can add or remove fields from most existing standard reports. You can also create customized reports for the way your organization does business, including just the information you need – selecting from over 300 different reporting fields and order the fields in any sequence you want for your reports. You can save and schedule reports in advance, and receive an email when they are ready to be downloaded. You can also share saved reports with others in your organization or keep them private and change sharing status as needed.

#### **Raw Data Download**

Raw data download (RDD) is a representation of your Verizon wireless bills and does not include any reporting structures you design in My Business. The download provides a holistic view of all of your statement data, and it is delivered in a .zip file with four individual .txt files. The .txt files are:

- Account Summary - Represents the account summary section of a statement
- Account and Wireless Charges Detail Summary - Represents the wireless number charges section of a statement

- Account and Wireless Summary - Represents the wireless number summary section of a statement
- Wireless Usage Detail - Represents the usage section of a statement

RDD is available within approximately 10 business days of each completed bill cycle. While these reports will meet the vast majority of your requirements, additional non-standard reporting options may be available upon specific written request. Your Account Manager can provide further details.

### 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 will display automatically in the portal and may take up to one (1) Business Day to be fully processed in the billing system with the exception of:
  - a. devices that are out of stock or otherwise unavailable;
  - b. account changes involving number portability;
  - c. account changes with 1,000 lines of service or more should be made within three (3) Business Days.
4. Account changes made by phone or email should be processed within two (2) Business Day with the exception of:
  - a. devices that are out of stock or otherwise unavailable;
  - b. account changes involving number portability;
  - c. account changes with 1,000 lines of service or more should be made within three (3) Business Days.
5. 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.

6. 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.
7. The Contractor may invoice the Customer an expedite charge.
8. 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.
9. 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.
10. The Contractor shall not impose any restocking fee under any circumstance.
11. Device provisioning errors must be corrected by the Contractor.
12. The Contractor shall not provide salvaged, distressed, outdated, or discontinued merchandise.
13. 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.

#### **Verizon's Devices**

Verizon works with manufacturers to update devices software/firmware for up to two (2) years after initial launch. Updates are typically made available via an over-the air update. Customers can contact their Account Manager/Customer Service for manufacturer-website links. Assistance with choosing service/equipment is provided by Customer's Account Manager. Any device on our network goes through extensive testing to ensure the device delivers reliable wireless service at peak performance levels. If a device does not perform to our standards, it will not be approved for use on Verizon's wireless network. Equipment arrives preprogrammed, ready to activate. Customers receive email-notification if ordered equipment is unavailable. Customers can order equipment and make account changes in My Business online resource; changes are typically effective within 24-hours of submission; two (2) day shipping is provided free of charge upon receipt of order. Customer's Account Manager can coordinate rush/overnight delivery (charges may apply). Title and risk of loss pass to Customer and acceptance occurs upon receipt of equipment at address on the order. Verizon accepts returns/exchanges on all equipment purchased from us by government-liable end-users within thirty (30) days of purchase and credits the Customer for the full amount of the equipment; devices are shipped with receipt, return label, and container. No restocking fees. Verizon's technical support is available 24/7 to assist with provisioning.

Verizon will provide new devices for the initial purchase. Replacement devices may be Certified Like-New. Customers receive manufacturer's equipment warranty.

### 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.

#### **Cooperation with Other Contractors**

Verizon has worked closely with DMS and its contractor since 2004. Specifically with current and previous MFN contractors in establishing the current Network to Network Interface. Given the numerous initiatives associated with the State of Florida's Digital Transformation we fully expect to and welcome working with DMS and its contractors.

Our standard communications solutions use applications, technologies and devices of many third parties. Most of these are provided under the terms and conditions of the corporate account agreement. However, certain features, applications, and devices described in this proposal may be provided by independent vendor(s) and may be subject to acceptance of their applicable terms and conditions. Verizon works with multiple vendors and third-party solution providers to present our customers with such applications and solutions, and we assume no responsibility for these third-party providers as our personnel or agents. For certain third-party solutions, you may elect to have charges presented on your Verizon bill for your convenience. Verizon will collaboratively with other Contractors and subcontractors (SUNCOM service providers) throughout the term of any resulting contract.

### 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 3.26.5, Project Management – Implementation Plan and Customer Specific Migration Plans.
2. Assist as necessary to migrate existing MCS 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 provided that the existing device can be unlocked and is compatible with Contractor's network.
6. Coordinate and communicate with DMS and Customers throughout all aspects of the migration.
7. Complete the migration for State Agencies in one-hundred and twenty (120) calendar days. Complete the migration for OEUs in one-hundred and eighty (180) calendar days.
  - a. Migration commences with DMS acceptance of the Services Infrastructure Checklist and ends when all current MCS Customers are identified as either migrated or no longer receiving services from the Contractor.
  - b. Migration does not include new Customers (non-current MCS Customers), Customers changing their services after migration, or non-State agencies that opt to purchase under a different contract.

Given the statements in this subsection:

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

#### **Customer Migration**

Verizon will work with DMS to migrate services with as little interruption or degradation as possible. For existing Verizon wireless subscribers, there should be no interruption of services upon conversion. If porting from another carrier, there may be a brief lapse of service while the conversion is taking place.

The implementation process comprises several phases. Your organization may be assigned a dedicated Implementation Manager who will serve as a project manager and assist you in the development of a customized implementation plan based on your specific requirements to transition your employees to Verizon wireless service. The Implementation Manager will also coordinate with other Verizon teams so the plan is executed in a timely manner.

Throughout implementation, you will be provided with status updates to keep the process running smoothly and accurately. Implementation will typically take 90 days. Complex requests or specialized elements within your corporate contract may extend the timeframe. The following are some of the more critical steps that are generally included in our current implementation process:

- The implementation team is assigned and meets internally to review your requirements
- The implementation team coordinates a formal implementation kick-off conference call to introduce members to you

- The Implementation Manager and/or team meets with your organization to develop a comprehensive account management program by customizing processes and procedures to meet activation, equipment fulfillment and your ongoing support requirements. This program may include an online billing, ordering, and analysis tool, among other account management functions
- If you will be using a self-service portal, a Web-based demonstration may be conducted
- You will provide a list of all the confirmed mobile numbers eligible to participate in the new Verizon wireless corporate pricing program
- Migration, including numbers to be ported from other carriers, commences
- To facilitate migration of your employees who already have wireless lines with us, we will query our billing systems to identify those lines based on Federal Tax ID numbers, Dun & Bradstreet numbers, and internal coding
- The Implementation Manager will create or identify coding; and an account profile for your organization will be created
- Account documents will be distributed and reviewed to include processes and procedures specific to you and your account
- Employee program materials are created and marketing for the employee program begins (if applicable)

### 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 closes 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 Management Plan and Disaster Recovery Plan

1. The Contractor shall create a Project Management Plan (see **Attachment C, SLA-D1**). 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 plan listed below is an additional component of the Project Management Plan. However, the plan listed below is a deliverable separate from the Project Management Plan and subject to final acceptance by DMS.

2. Disaster Recovery Plan. (See **Attachment C, SLA-D2**.) 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 Management Plan and ends with DMS acceptance of a completed Services Infrastructure Checklist. The Project Status Report, described below, is a deliverable that must be submitted to, and accepted by, the DMS Project Manager.

1. Project Status Report. The Contractor shall create Project Status Reports. **Attachment C, SLA-D3**. 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. Project schedule.
  - b. A narrative description of significant project activities that have been conducted or are underway.
  - c. The progress-to-date on project activities.
  - d. An explanation of any tasks/activities that are behind-schedule and a plan to bring them current.
  - e. Notification of issues or risks that have been encountered and their resolution or plan for future resolution.
  - f. Upcoming deadlines.

### 3.26.3 Project Management - Guides

The Contractor shall create the following two (2) 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-D4**.

1. WDS and WVS Operations Guides. The Contractor shall create and maintain one (1) 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 one (1) 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-D5.**) 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-D6.**) The Implementation Plan must address all activities in the Project Implementation Phase, which starts after the acceptance of the Project Management Plan 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-D7.** The reporting, which shall exclude any information regarded as Customer Proprietary Network Information (CPNI), should detail the number of current MCS 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 current MCS 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 current MCS End-users are identified as either migrated or no longer receiving services from the Contractor or for non-State agencies having selected another contract vehicle.. The format, content, and level of detail must be approved by DMS.
2. Individual Customer-Specific Migration Plans. If requested by DMS, the Contractor must submit these plans in accordance with the requirements in this section to DMS and the Customer. **Attachment C, SLA-D8.** The Contractor will be responsible for creating

Individual Customer-Specific Migration Plans as a 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.

#### **Project Management - Implementation Plan and Customer Specific Migration Plans**

Given Verizon's incumbent role we will work with DMS to assess projects related to the MCS ITN that have already been implemented, tested and functional. Based on those assessments Verizon will develop a project plan following the methodology listed below.

The implementation process comprises several phases. Upon contract execution, DMS will be assigned a dedicated Implementation Manager who will serve as a project manager and assist you in the development of a customized Implementation Plan based on your specific requirements. The Implementation Plan with six (6) weeks after Contract execution. Failure to meet this objective will not result in penalties of any kind. The Implementation Manager will also coordinate with other Verizon teams so the plan is executed in a timely manner.

Throughout implementation, you will be provided with status updates to keep the process running smoothly and accurately. Implementation will typically take 90 days. Complex requests or specialized elements within your corporate contract may extend the timeframe.

The following are some of the more critical steps that are generally included in our current implementation process:

- The implementation team is assigned and meets internally to review your requirements
- The implementation team coordinates a formal implementation kick-off conference call to introduce members to you
- The Implementation Manager and/or team meets with your organization to develop a comprehensive account management program by customizing processes and procedures to meet activation, equipment fulfillment and your ongoing support requirements. This program may include an online billing, ordering, and analysis tool, among other account management functions

- If you will be using a self-service portal, a Web-based demonstration may be conducted
- You will provide a list of all the confirmed mobile numbers eligible to participate in the new Verizon wireless corporate pricing program
- Migration, including numbers to be ported from other carriers, commences
- To facilitate migration of your employees who already have wireless lines with us, we will query our billing systems to identify those lines based on Federal Tax ID numbers, Dun & Bradstreet numbers, and internal coding
- The Implementation Manager will create or identify coding; and an account profile for your organization will be created
- Account documents will be distributed and reviewed to include processes and procedures specific to you and your account
- Employee program materials are created and marketing for the employee program begins (if applicable)

### 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-D9.** 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.

<b>Infrastructure Checklist</b>	
<b>Section Reference</b>	<b>Requirement</b>
<b>SOW Section 2</b>	
<b>2.1 - 2.6</b>	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.
<b>2.7</b>	The Contractor has demonstrated that its Customer Support Team is staffed and trained.
<b>SOW Section 3</b>	
<b>3.12</b>	Security and fraud services are ready for production.
<b>3.13</b>	Processes related to test and demonstration accounts for WVS and WDS are final.
<b>3.14</b>	Emergency services programs are ready for production.
<b>3.16</b>	Design characteristics have been reviewed and are ready for production.
<b>3.17</b>	Reports and reporting options are ready for production.
<b>3.18</b>	SLA processes are ready for production.
<b>2.7 and 3.19</b>	The Customer Support Team is staffed and trained.
<b>3.20</b>	The Contractor's portal is operational.
<b>3.21</b>	The Contractor has provided the link to the manufacture's website. The Contractor has provided its EUPL and Vendor's Device List.
<b>3.26.1 (2)</b>	The Contractor has provided an acceptable Project Management Plan.
<b>3.26.1 (7)</b>	The Contractor has provided an acceptable Disaster Recovery Plan.
<b>3.26.3 (1)</b>	The Contractor has provided the WDS and WVS Operations Guides
<b>3.26.3(2)</b>	The Contractor has provided the WDS and WVS User Guides

<b>3.26.5(1)</b>	The Contractor has provided the Implementation Plan.
<b>SOW Section 4</b>	
<b>4</b>	Public safety services are ready for production.
<b>SOW Section 5</b>	
<b>5.4</b>	The Contractor is ready to implement transactions utilizing the DMS approved method of implementation in CSAB.
<b>5.7</b>	The Contractor has demonstrated the ability to provide CSAB billing account and user management activities.
<b>5.9</b>	The Contractor has demonstrated the ability to maintain a corresponding inventory.
<b>5.10</b>	The Contractor has demonstrated the ability to invoice DMS for all fulfilled orders.
<b>5.11</b>	The Contractor has demonstrated the ability to provide a detailed invoice substantiation file and do so in a mutually agreed upon secured delivery method.
<b>SOW Section 6</b>	
<b>6</b>	The Contractor has demonstrated the MFMP 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.

### **Verizon's Deployable Technologies**

We own a fleet of portable emergency equipment that can be regionally deployed quickly to keep customers connected or restore damaged connections as soon as possible. We tactically place network-deployable equipment throughout the country, so we're ready if primary connections get shut down.

We maintain **Cell on Wheels** (COWs), **Cell on Light Trucks** (COLTs) and **Generator on a Trailer** (GOATs<sup>1</sup>) that can be deployed to improve wireless coverage at large gatherings and special events. They are also utilized to quickly improve coverage and capacity when natural disasters or other unplanned events interrupt wireless service.

We also deploy **Wireless Emergency Communication Centers** (WECCs) into disaster zones, providing a safe place where impacted members of the community can charge their phones, make a free call, or access the Internet.

We have over 530 portable assets located across the country that enable our teams to enhance or restore network coverage and capacity in emergencies, and we maintain a fleet of over 800 portable generators nationwide. There are many types of assets and innovative solutions, such as:

---

<sup>1</sup>**GOATs** are mobile electrical generators, often attached to trailers or trucks, deployed to provide electrical power. GOATs can be used to power network services or emergency operations in the aftermath of disasters (e.g., tornados or hurricanes) that compromise the existing infrastructure.

- Repeater-on-a-Trailer (RAT)
- Tower-on-Wheels (TOW)
- HVAC on Roadside Equipment (HORSE)
- Repeater on a Trailer (RAT)
- Pico cell on a Trailer (SPOT)
- High altitude wireless kennehat aka tethered drone (HAWK)
- Cell Repeater on Wheels (CROW)

We also continue to design and deploy innovative portable solutions that provide our personnel, first responders, and our customers with options that extend wireless coverage into areas of need. Many of these solutions leverage technologies ranging from lightweight suitcase-sized cell sites, to trailer-based solutions, and drone assets.

The **Verizon Response Team (VRT)** is a nationwide program sponsored and managed by the National Government Sales & Operations team. When a natural disaster, crisis, or planned event occurs VRT responds to government and non-profit organizations and emergency management agencies that need our assistance. VRT provides the following support in the event of a crisis:

- Deployment of COW/COLT/crisis response vehicle
- Back-up phone coverage
- Equipment/Network support
- Assistance with search and rescue initiatives
- A live support line to request help 24/7
- Best-in-class customer support
- Routing of requests to the Verizon Security Assistance Team
- One phone number (800-981-9558) to call in a crisis situation.

This process links together management of crisis situations in one location for the entire Verizon wireless community. VRT aligns network, operations, legal and sales – allowing us to react quickly to a crisis situation. The benefits to our customers and to emergency management agencies are tremendous.

On the VRT Team, Verizon has assigned a dedicated Crisis Response Manager to the State of Florida. The State's Crisis Response Manager is listed as part of Verizon's escalation path for public safety network events and works with the State's account team to coordinate support, drills, and ongoing customer training as needed.

As part of our robust regional deployable strategy, Verizon performs Emergency Operations Center ("EOC") drills each year prior to hurricane season with refreshers as needed. We have staff at key Verizon EOC locations within the state who regularly maintain, fuel, and test Verizon's deployable assets to ensure that Verizon is ready to provide emergency support within the State of Florida at a moment's notice.

Verizon stands ready to help keep DMS and public safety agencies connected even in remote areas where voice and data network infrastructure is unavailable, or in disaster scenarios where networks could fail. Verizon will continue to 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.

## 4.2 Local Control

The Contractor should 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.

### **Verizon's Approach to Local Control**

For Verizon's qualified public safety users subscribing to Verizon's Public Safety Price Plans, priority and preemption is always on. Verizon provides priority and preemption to public safety entities during times of emergency as described below:

#### **Responder Private Core**

Responder Private Core is a dedicated network core that Verizon uses to enable certain other products such as Mission Critical Push to Talk and Private Network Traffic Management for traffic segmentation capabilities to support improved security, enhanced service management and control. It is connected to Verizon's Radio Access Network (RAN), which utilizes spectrum in various bands including 700 MHz, 800 MHz Cellular, 1.9 GHz PCS and 1.7/2.1 GHz Advanced Wireless Services (AWS) bands. Responder Private Core separates data traffic of public safety mobile users from commercial users across Verizon's 4G LTE network; however, it is not available on Verizon's 5G Nationwide and 5G Ultra Wideband networks. Public safety users will have their data immediately recognized as public safety with enhanced reliability through the network. Responder Private Core leverages leading edge networking technology to provide security, flexibility and reliability.

#### **Mobile Broadband Priority**

Mobile Broadband Priority provides public safety users priority service for data and voice transmissions. During times of heavy commercial network congestion, Mobile Broadband Priority users will receive priority over commercial users. Mobile Broadband Priority enables priority service for public safety officials using applications on smartphones or tablets, transmitting data from first responder vehicles or video from surveillance cameras. Mobile Broadband Priority is available at no additional charge to qualified public safety customers on the 4G LTE Network only. Mobile Broadband Priority access to the 5G Network is not currently available.

#### **Preemption**

Preemption provides prioritized access to network resources during times of network congestion. Verizon automatically reallocates network resources from commercial data/Internet users to first responders in the unlikely event network resources become congested. As part of the network access and registration process, first responders and public safety personnel are identified and given preemption designation. This helps to determine which users will receive allocated resources with preemption. Preemption is offered at no additional charge for qualified public safety customers on the 4G LTE Network only. Preemption is currently not available to the 5G Network.

Customers can use **Traffic Management**, a feature of **Private Network** service that transports a multitude of data applications, including Voice over IP (VoIP), video and best effort applications. When there is contention for network resources, mission critical applications (i.e., VoIP) are competing with best effort applications (i.e., email) for network resources, so customers' mission

critical applications may experience performance degradation (e.g., difficulty accessing Verizon's LTE network resources, variable download/upload speeds, etc.).

Traffic Management is a Private Network feature, available only for Verizon's 4G LTE devices, that provides customers a premium and differentiated network experience. Private Network Traffic Management enables application differentiation and QoS over the LTE Private Network using standards-based IP packet marking. Benefits include:

- Allows customers to prioritize business critical applications over best effort applications during congested / non-congested environments.
- Delivers more predictable application performance for subscribers using business critical applications during network congestion.
- Extends Wireline QoS policies over the LTE Private Network.
- Delivers end to end QoS when combined with Verizon's Private IP network solution.
- Provides access priority during network heavy utilization for eligible Public Safety accounts.

Private Network Traffic Management can be added to a LTE Private Network device for a monthly charge and is available on configurations using Verizon Private IP; Dedicated Physical Connection; and Zero Tunnel connectivity.

Private Network Traffic Management offers both Enhanced and Premium subscription options.

- **Enhanced:** Allows mapping of critical applications up to a maximum of 2.0 Mbps Mission Critical Class of Service (CoS), with the remaining best effort applications mapped into the Best Effort CoS utilizing the remaining available LTE bandwidth. Mission Critical traffic may not exceed 2 Mbps.
- **Premium:** Allows mapping of critical applications up to a maximum of 12 Mbps Mission Critical CoS, with the remaining best effort applications mapped into the Best Effort CoS utilizing the remaining available LTE bandwidth. Mission Critical traffic may not exceed 12 Mbps.

Verizon's public safety plans are not throttled during an emergency. Verizon welcomes a deeper discussion to understand how this technology may meet your public safety data needs.

### 4.3 Local control portal

In addition to the requirements of subsection 3.20 Contractor's MCS Portal, the Contractor should provide a public safety portal (dashboard). The information held in this dashboard, or within the Contractor's MCS Portal, 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.

**Non-mission critical public safety service plans shall provide the status of the Statewide network and alerts on outages through an alternative means.**

## Local Network Command and Network Reporting

Verizon's **Local Network Command** allows designated public safety entities/Incident Commanders, to view the network operational status in an incident area and respond in real-time, dynamically administering user groups and temporarily managing data traffic Quality of Service (QoS) on qualified Public Sector responder devices.

DMS would use its **My Business** online resource as a dashboard for all of their Verizon services and products - including public safety services and products.

All Customers can enroll their authorized contacts in Verizon's **Network Event Notification ("NEN") Program**. Verizon's NEN Program is a courtesy service that provides notice to Customers about planned and unplanned network maintenance, including ongoing updates and issue resolution for affected services. Network event notifications are issued via email and the same information is maintained online through a self-serve NEN portal for up to four weeks. Customers may choose to receive notices on unplanned and/or planned events.

### Events That May Trigger Notification and Notification Process

Network event notifications will issue to your organization's identified contacts, providing information about planned and unplanned maintenance events that may impact your service with us.

A planned network event is sent to your identified contact up to two weeks before any planned network maintenance.

An unplanned network event is sent when we receive confirmation there has been an unplanned disruption of service on the network. Events that may trigger automatic notification include a service condition that is significantly below our normal service operational thresholds. Because the service outage notification is sent when our systems identify a possible outage, your identified contact may receive the notification regardless of whether or not your end users are affected.

There are four types of unplanned network event notifications:

- Initial: Sent when the disruption is confirmed
- Update: Sent every half hour until the service is restored
- Restored: Sent when the issue is resolved and service is restored
- Informational: Sent when it has been determined that a brief service disruption occurred on the network, but was resolved before an alert was issued

If you receive a notification, there is no need to take any action. Our network engineers will be working to resolve the issue and you will receive an update when it is resolved. Both planned and unplanned event notifications will include the following information:

- Start Date
- Start Time
- Severity Level [(High or Low for Planned), (High for Unplanned)]
- Affected Service (e.g., 4G LTE, Enterprise Messaging)
- Affected Location: ( e.g., Tampa, Florida)
- Affected Counties: (e.g., Broward, Miami-Dade, Palm Beach, Brevard, Polk, Pinellas, Osceola, Hillsborough)
- Tracking Number: (e.g., 123456)

**Self-Service Portal**

The self-service NEN portal includes the same network event information as is contained in the notification emails. The information is presented in user-friendly views with data maintained for up to four weeks.

You can access the NEN portal directly through Verizon's My Business online resource or via a direct website link that can be provided upon enrollment.

**Enrollment by Services**

Event enrollment is available for covered services, which are continually being updated. Notifications issue when the selected service is operating below normal thresholds. NEN services may include 4G LTE, 5G Services (Network), Amazon Web Services (AWS) – Multi-Edge Compute, Call Processing, Enterprise Messaging, HD Voice, Internet of Things (IoT), Push To Talk Plus, Verizon Wireless Private Network and others.

To avoid being overwhelmed with unnecessary notifications, Customers should only sign up for notifications that are relevant to the solutions the Customer has deployed. The Network Notification Program is offered as a courtesy only. In no event shall the failure to provide outage notifications subject Verizon to penalties or damages of any kind. Verizon reserves the right to modify or discontinue outage notifications at any time.

#### 4.4 Public Safety Standards

Mission Critical public safety service plans and devices shall be in compliance with the relevant 3rd Generation Partnership Project Technical Specifications and the National Public Safety Telecommunications Council (NPSTC) standards for a mission critical service .

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.

Should the Contractor offer plans marketed towards the public safety community that are not in compliance with the relevant 3rd Generation Partnership Project Technical Specification or do not meet the necessary criteria to be deemed "Mission Critical," as defined by the National Public Safety Telecommunications Council (NPSTC), the Contractor's EUPL must clearly state, at the beginning of the plan description, "THIS PUBLIC SAFETY PLAN DOES NOT PROVIDE A MISSION CRITICAL SERVICE STANDARD." Failure to include this statement where applicable will result in the EUPL not being accepted by DMS.

**Verizon Response**

Clarification. The basis of Verizon's Responder Private Core is Verizon's Long Term Evolution (LTE) wireless network. LTE is a technology based on 3GPP standards. It supports advanced application usage and high-speed data services.

Established cellular industry and performance standards serve as the foundation for our engineering, design, operation and quality assurance programs. Verizon has created enterprise-wide policies that conform to the International Organization for Standardization (ISO) 27002.2005 and National Institute of Standards and Technology (NIST) standards for the protection of customer and employee information. These policies cover security issues, such as account management, password standards, server configuration and a wide range of security topics.

Many of the equipment manufacturers that we utilize are certified through ISO.

#### 4.5 Demonstration Devices

**DMS Demonstration Devices.** Upon DMS request, in addition to any other test devices required by this SOW, the Contractor shall provide up to ten (10) wireless demonstration public safety devices (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 thirty (30) Business Days. Any demonstration agreements, equipment, forms, and processes shall be provided, managed, and maintained by the Contractor, subject to the approval of DMS.

**Customer Demonstration Devices.** The number of demonstration public safety devices the Contractor elects to provide to Customers is at the discretion of the Contractor. The Contractor will coordinate directly with any other Customer regarding public safety service demonstration equipment, notifying the Department in advance of these activities.

##### **Demo Devices**

Currently, Verizon offers a program that enables new and existing customers to demo/trial various devices and services at no charge to the customer. The customer may trial up to three devices at a time.

Verizon will make demonstration equipment available to DMS for sixty (60) business days; and will make demonstration equipment available to Customers purchasing from the resulting agreement for thirty (30) days. With approval from our B2B Demo Support Team, time-periods may be extended and the number of devices available for demo may be increased. The B2B Demo Support Team may also approve trialing devices and services outside of the U.S.

#### 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 or as recognized by the First Responder Network Authority.

The Contractor should limit access to the Mission Critical public safety plans to only Customers that are Public Safety Entities. At a minimum, Public Safety Entities should include the following Customers, as categorized by the North American Industrial Classification System (NAICS) codes:

- 621910 Ambulance Service
- 922110 Courts
- 922120 Police Protection
- 922130 Legal Counsel and Prosecution
- 922140 Correctional Institutions
- 922150 Parole Offices and Probation Offices
- 922160 Fire Protection (except private)
- 922190 Other Justice, Public Order and Safety Activities
- 928110 National Security
- 921190 Other General Government Support
- 921110 Executive Offices
- 921150 American Indian/Alaska Native Tribal Governments
- 922190 Other Justice, Public Order and Safety Activities

Should the Contractor offer non-mission critical public safety service plans, the Contractor's EUPL must clearly state the eligible NAICS codes in the plan descriptions.

#### **Verizon's Public Safety Customer Support**

Residing within Verizon's Business and Government Customer Operations (BGCO) Technical Solution Center is a group of technical experts who provide **Wireless Enterprise Help Desk (WEHD)** support to Verizon's public safety customers. This U.S.-based helpdesk-to-help desk support team is available 24/7/365.

Customers will be provided with the WEHD support contact number if you subscribe to one of the advanced product types it supports, such as Public Safety Plans, Private Network, Enterprise Messaging, or an Internet of Things (IoT) solution [Intelligent Video, Asset Management, etc.]. Upon contact, one of our technical experts will conduct troubleshooting and recommend specific actions to help you achieve issue resolution. If the issue is related to Verizon's wireless network, then the BGCO will escalate and engage the appropriate network support teams.

Please note: The WEHD service should only be used for troubleshooting of government liable devices related to the advanced product or solutions that are supported by this group of technical experts. Issues with devices on employees' personal accounts or non WEHD-supported issues should be handled by calling our regular customer service number, 800-922-0204, and selecting the appropriate support option in the IVR.

#### **Public Safety Escalation Procedure**

Your first point of contact for trouble with your public safety services is our WEHD located within Verizon's Business and Government Customer Operations (BGCO) organization. Members of our WEHD teams can conduct device and network troubleshooting. Concerns related to quality of service, such as the

inability to make or receive calls, will be assigned the highest priority and receive prompt attention. A staff supervisor is available during the BGCO team's hours of operation.

In the event BGCO representatives cannot resolve a situation and escalation becomes necessary, the following account team members may be contacted.

Contact	Name	Phone Number/Email Address
Client Partner - Government	Tom Madden	850-294-5171 tom.madden@verizonwireless.com
Verizon Crisis Response Manager - Florida <sup>2</sup>	Jos Bowmaster	800-981-9558 (VRT Hotline) 603-953-5023 (m) joseph.bowmaster@verizon.com

If the escalated situation is not effectively resolved or the process of resolution is not effectively initiated within 24 hours of the request, we suggest contacting the staff management level.

Contact	Name	Phone Number/Email Address
Managing Partner - Government Sales South Florida	Beth Bailey	786-360-9408 beth.bailey@verizonwireless.com
Managing Partner - Government Sales North/Central Florida	Colin Denney	904-718-9797 colin.denney@verizonwireless.com

A highly sensitive situation that requires further escalation may require director level involvement. In those rare situations, we suggest you request a call back from the individuals below in the order in which they are listed.

Contact	Name	Phone Number/Email Address
Director - Government Sales	Kim Mirabella	813-326-0929 kim.mirabella@verizon.com

Complex situations may require research and may take longer to resolve. In these situations, we will research, resolve the issue and report back to the employee or authorized contact when the issue is resolved.

Verizon limits access to Public Safety Plans to customers who have a qualifying North American Industry Classification System ("NAICS") code; eligible public safety NAICS codes are described in further detail under Question 9, *Eligible Users*.

#### 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

<sup>2</sup> Customers may contact the State's Verizon Crisis Response Manager to immediately escalate network issues during emergency situations.

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.

**Verizon’s Public Safety Reporting**  
Acknowledged.

**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.

Given the statements in subsection:

Describe in detail the proposed offering for this subsection, addressing the minimum requirements listed in SOW, section 4, Public Safety Service Plans and Devices.

Verizon will work closely with the Department as required regarding the marketing and promotion of Verizon’s public safety offerings, service plans, and devices.

Please review the responses below for further detail regarding our proposed offering for this subsection.

Describe the Respondent’s proposed deployable technologies and how they will be utilized during an emergency or when requested by a public safety entity.

**Verizon Response**

See above response to Question 1 above which describes Verizon’s *Deployable Technologies*.

Since the beginning, Verizon has worked closely with first responders, our customers, and our communities to provide support and wireless solutions when they are needed most – during an emergency/extreme weather conditions. With threats of hurricanes, tornadoes, wildfires and other natural disasters always a possibility, customers rely on us to keep them connected and productive, especially when the unexpected happens.

We provide support in a variety of ways, often lending wireless voice and data devices to first responders and emergency personnel. We built a Public Safety Private Core to support public safety, especially during times of high data traffic. In addition, when disaster strikes, we coordinate with first responders and can mobilize charging stations, special equipment, emergency vehicles and more to support local, state and federal agencies across the U.S.

Being crisis-ready is paramount to Verizon, and we are committed to supporting those who need us most when they need us most. During an emergency, first responders rely on wireless service more than ever to coordinate efforts in the face of fires, floods, snow and wind storms, earthquakes, tornados, or hurricanes.

We've assisted first responders and citizens during some of our nation's most destructive disasters. We loaned more than 6,000 devices during 9/11, more than 3,000 during Hurricane Katrina and more than 2,500 during Hurricane Sandy. During 2018, we supported disasters including Hurricanes Gordon, Florence, and Michael; Mendocino and Camp wildfires in California, a gas pipe explosion in Massachusetts, volcano eruption in Hawaii, earthquake in Alaska, and winter storm Diego across the Southeast, among others. In total, we supported 75 disasters in 2018, helping more than 120 different public safety agencies and non-profit organizations. Last year we lent more than 2,300 phones and tablets and more than 2,700 data devices (Jetpacks, routers, network extenders) to keep first responders connected and communities safe.

Below are recent examples of how deployables have been utilized during an emergency or when requested by a public safety entity in the State of Florida:

- During SBLIV in Miami, FL the Verizon Response Team provided the FDLE with a cradlepoint router to assist their JOC in their Super Bowl operations.
- During SBLIV in Miami, FL the Verizon Response Team provided the state governors of Missouri and California Security Teams with their communication operations during game day operations.
- In response to the COVID-19 national pandemic, Verizon partnered with the Florida Department of Veterans Affairs to provide smartphones, tablets, and eFEMTOs to each of the veterans' homes so that they could communicate virtually and safely with their families.
- In response to the COVID-19 national pandemic, Verizon partnered with Brooks Rehab and provided their COVID treatment facility with Push-to-Talk basic phones to communicate with inside of their facility.
- In cooperation with the Salvation Army, Camp Keystone in Keystone Heights was identified as the primary backup location for the state of Florida Emergency Operations Center and the Verizon Response Team installed network coverage throughout the primary usage areas of the camp to ensure that in the event of a disaster, communications could be established and maintained both inside and outside the camp.
- During SBLV in Tampa, FL the Verizon Response Team provided the Tampa Fire Department with Push to Talk smartphones that the Tampa Fire Marshals utilized for their communication needs.
- During Hurricane Sally, the Verizon Response Team drove through the encroaching outer bands

- of the storm to the Escambia County Emergency Operations Center to install an eFEMTO device
- inside the building to improve 4G network coverage inside the building at the request of the
- Emergency Management staff, leaving just before nightfall.
- After Hurricane Sally made Landfall, the Verizon Response Team provided charging stations and
- battery packs for the community and public safety, as well as free wifi and EOC ESF2 support to counties impacted by the storm throughout the Florida panhandle.

Verizon's mobile assets and deployables can generally be deployed within the following time frames, failure to meet these time frames shall not result in any penalty of any kind to Verizon:

- Satellite Connection - within 8-16 hours
- Asset without available on-site fiber interconnect - within 24-48 hours
- Asset with available on-site fiber interconnect - within 8-16 hours
- SPOT - within 4-8 hours
- Verizon Florida Statewide Assets - within 72 hours
- Southeastern Regional Assets - within 96 hours
- National Assets - within 120 hours

Describe how service plans and devices are not throttled during an emergency.

#### **Verizon Response**

Customers on "custom public safety rate plans" are not subject to data speed reductions ("throttling") within a given billing cycle. Data usage for actively engaged and deployed fire, police, emergency medical technicians, emergency management agency, and assigned federal law enforcement users on this plan will not be subject to speed reductions regardless of data usage during any billing cycle. This service plan includes Mobile Broadband Priority and Preemption. Mobile Broadband Priority ensures customers can connect to the network with priority by leveraging a pool of radio resources dedicated to enable their connection. Mobile Broadband Priority identifies the user with an Access Priority setting, giving them higher priority for network access than lower Access Class users. Preemption automatically activates to provide approved personnel uninterrupted access to the network in those uncommon times when the network is fully utilized. 911 calls are never preempted.

Lines of service that are conditioned with specific Public Safety features are provisioned with QoS Network Enhancements. These Network Enhancement attributes affect the treatment of data for first responders and public safety customers by providing higher data priority and packet treatment, resulting in better throughput speeds at times of congestion.

Describe the Respondent's planned network hardening approach, including issues caused by power, hardware failures, topography, weather, and man-made incidents.

#### **Verizon Response**

The **Verizon Business Continuity and Disaster Recovery** program is just one part of our overall philosophy to provide high quality services for our customers. Our nationwide wireless network is at the core of our business, and we have invested more than \$159 billion since the company was formed – averaging over \$7.95 billion every year – to increase coverage and capacity and to add new services. Our Business Continuity and Disaster Recovery (BC/DR) program team is responsible for minimizing the impact of a disruption to our customers, employees, infrastructure and business operations. We accomplish this objective by focusing on the following activities:

- Identify critical functions, infrastructure and risks;

- Implement strategies to minimize the risk of a disruption;
- Develop Business Continuity and Disaster Recovery plans and Crisis Management Teams to recover operations in the event of a disruption;
- Maintain BC/DR plans, with updates completed at least annually;
- Test our plans, at least annually, to validate our response capabilities.

We continue to refine our response and recovery capabilities due to the increasing variety of services we provide and the ever-changing level of potential threats to these services.

The cross-functional Crisis Management Teams in place across our national footprint enhance coordination and response activities during crisis events. These teams provide a command-and-control structure that allows management to gather and report information about crisis events, for the teams to escalate decision-making as needed and to facilitate resource allocation.

BC/DR activities are visible across all major aspects of our company. We have developed numerous plans to recover critical functions. Business functions have implemented strategies and procedures that not only support routine operations, but also help the function continue to operate in the event of a disaster. Robust operational strategies are at the core of our ability to provide reliable and resilient services.

Our pro-active planning activities center on three of our major departments:

- Network Operations
- Information Technology
- Customer Service

#### **Network Operations – Our wireless network is resilient by design**

The Verizon Wireless network operations philosophy is driven by the desire to provide our customers with an extremely high level of service.

Verizon Wireless strives to deliver superior service based on our design philosophy, which includes redundancy on critical paths and components so that a potential failure of a network component does not significantly affect our customers. Our wireless services are provided through a large and sophisticated national network of 148 Mobile Switching Centers (MSCs) and Data Centers throughout our service areas. We will continue to invest in our network to support our customers.

The wireless voice and data switching networks are designed to provide continuous service to the customer. The communications between our internal switches and external networks such as the Public Switched Telephone Network (PSTN) and the Internet are also designed to reduce the possibility of interrupted communications. The use of battery and generator backup systems in critical locations also serves to minimize the risk of a disruption, if commercial power is lost.

Our design concept extends from our equipment and technology capabilities to our business procedures. These procedures include frequent and thorough preventive maintenance, real-time monitoring of all key system components, the 24/7/365 availability of trained maintenance personnel to repair or resolve critical failures should they arise, and wide deployment of these personnel and spare parts to permit rapid response and restoration of service.

Our most critical recovery assets are the thousands of highly-trained and experienced network technicians who have repeatedly proven their ability to respond, troubleshoot problems, and restore service to our customers during emergency situations.

#### **Monitoring, maintenance and restoration of wireless services**

Service protection and restoration strategies are an integral part of Verizon Wireless network management and operations.

We have two Wireless Network Management Centers (wNMCs), one located in New Jersey and another in Texas, that monitor all facilities, cell sites and switches across our nationwide network. These wNMCs are staffed 24/7/365 with experienced personnel who work closely with our regional field operations teams and with our vendors to coordinate and expedite the restoration of service in the event of outages. Each wNMC receives alarms or other indicators that help troubleshoot problems in the network, and that provide technicians with key information to analyze and maintain network integrity.

wNMC technicians work with the field operation managers, and personnel are dispatched to the affected site as needed. An inventory of standard spare parts and repair equipment is available to technicians in all of our central network locations. We also have standing agreements with our critical vendors to get 24/7 support from their engineering personnel and obtain replacement equipment if required.

#### **Strategy for continued service to Mobile Switching Centers**

MSCs are an important part of our national wireless network, and we continue to add them to our network as we grow. We have 148 MSCs strategically distributed across the country to meet the needs of our customers. Our teams monitor the loading of the switching and data systems to maintain an optimum capacity and service level. One goal of this is to reduce the impact of a disaster to any one MSC. Available capacity in neighboring MSCs could be utilized in the event of a serious disaster.

In addition to redundancy in the equipment and circuitry, each MSC is protected by automatic power backup systems, by automatic fire detection and suppression systems, and by physical security systems and alarms. MSC buildings have restricted access to prevent entry by unauthorized personnel. The building structure itself is designed to provide protection for the systems and services located inside.

In each MSC, network operations personnel routinely backup system data for the switch itself and the peripheral systems. Automated backup routines are supplemented with scheduled manual backup routines and off-site storage of critical data.

A disaster recovery plan has been developed for each MSC, which addresses the recovery of the systems, services and personnel. These plans are updated at least annually. Exercises are conducted at least annually to confirm that these plans can be implemented as expected and to continually increase the readiness of the network teams to respond to an actual disaster. These exercises focus on disasters that may impact us or our customers.

#### **Strategy for continued service to cell sites**

We have thousands of cell sites across our nationwide network to provide the desired level of customer service, both in terms of capacity and quality of service. Despite the large number of sites, the loss of a single cell site is still a serious situation. We take extra precautions to protect and keep cell sites operational.

Cell site operations are protected in many ways, including redundancy in the equipment, automatic power backup systems, automatic fire detection systems, and by physical security systems and alarms. Through arrangements with our vendors, any major components of a cell site, up to and including the building and tower, becomes an immediate priority restoration effort on the part of both Verizon Wireless and our vendors.

Cell site equipment has sophisticated diagnostics that can instantly determine if a problem occurs at the site. These diagnostic alarms are transmitted to the MSC, which is monitored by regional field operations teams, and the wNMC. Cell sites are outfitted with backup batteries, and in most cases backup generators in case of commercial power loss.

We maintain and utilize portable cell sites referred to as Cells-on-Wheels (COWs) and Cell-on-Light-Trucks (COLTs), which are fully functional generator-powered cell sites that can replace or enhance network coverage and capacity in a given area. They can accommodate both voice and data services, and can be used for emergency situations. For example, they can be used to enhance communications between firefighters when they are fighting a fire in a remote wilderness area. These portable cell sites are strategically located throughout our network coverage areas and may be deployed to an area that is affected by a weather-related or other disaster.

#### **Backup power strategy for the wireless network**

Verizon Wireless purchases power from electric companies for the day-to-day power requirements of our network infrastructure. If commercial power is lost, we have implemented backup power systems for all of the critical equipment and infrastructure in our wireless network.

This is accomplished by installing large banks of backup batteries in our MSCs and Data Centers, and these are supported by permanent backup generators. We have arrangements with our fuel suppliers to refill our fuel tanks as needed, allowing our systems to operate until commercial power is restored.

The cell sites are also equipped with batteries, and most sites also have permanent generators which turn-on automatically if commercial power is lost. The company also owns a large supply of portable generators that can be deployed to provide emergency power during extended power outages to those cell sites without permanent generators.

Our MSC, Data Center, and cell site generators are tested regularly to ensure that they are functioning properly. Both the batteries and generators are regularly put through rigorous load tests to ensure that they can support the needs of the network in the event of a commercial power disruption.

#### **Circuit diversity strategy for the wireless network**

Our wireless network comprises numerous components that are connected using a mixture of fiber optic and high bandwidth telecommunication circuits. We support many of our critical network locations with diverse circuits, network technologies, and alternate local telecom carriers. The impact of a severed fiber optic cable or a faulty data circuit is minimized by this diversity in our telecommunications connectivity.

#### **Information Technology – Disaster Recovery Planning**

The Information Technology (IT) team for Verizon Wireless manages the technology that supports internal business functions. For example this technology helps internal users respond to customer needs, streamline internal and external communications, and automate many of our high volume activities. Many of these technologies are integral to our daily operations.

Our IT Disaster Recovery team focuses its efforts on mission critical applications and systems, many of which support customer transactions. System engineers for these applications and their supporting technologies emphasize redundancy, geographic diversity, and heightened security to safeguard these systems from an unexpected interruption or disaster.

#### **Data Center Strategy**

Mission critical applications are maintained in a secure data center environment. Our major data centers are protected by automatic fire detection and suppression systems, and by physical security systems and alarms. The data centers have strictly limited access to prevent entry by unauthorized

personnel. Only a small number of authorized employees are permitted to access these data centers, and the buildings are monitored by security guards and camera systems to provide a high level of protection to the systems and services located there.

All data centers are backed up by both battery and permanent generator systems which are designed to support the data center for extended timeframes in the event commercial power is disrupted. These systems are tested regularly to ensure that they will provide power when needed.

#### **Data Backup Strategy**

In each of the Data Centers that house mission critical applications, a significant amount of resources are put into our data back-up and restoration capabilities. Ensuring the availability and security of critical historic data is part of daily operations, and our back-up procedures include internal and off-site rotation of electronic files.

#### **Recovery Plans and Tests**

The IT Disaster Recovery team develops tests and maintains disaster recovery plans for mission critical applications in the data centers. Exercises are scheduled at least annually to confirm that the applications can be restored properly, that all interfaces are accessible, and timeframes are met. Surprise simulation drills are also conducted to enhance the preparedness of the recovery teams.

#### **Customer Service – Answering the call for operational resilience**

Providing industry leading customer service is an important way for us to understand our customer's expectations, assist with questions, and ensure satisfaction with the services we provide. We continue to invest in our ability to provide excellent customer service, whether the customer contacts us during routine operations or in the midst of a hurricane.

Our customer service operations are designed to be resilient. The contact centers are equipped to adapt to changes in customer call volumes, call types, or other circumstances so that they meet service quality targets. Customers are also provided with many different ways to interact with us. For example, customers can gather information about their accounts using our website and other self-service tools if these are most convenient for them.

#### **Call routing between multiple locations**

Our customer service team operates multiple contact centers located across the United States. Our teams can redirect calls between these locations to provide the best service possible and to optimize the skills of our personnel. This operational strategy is a valuable asset during times of crisis, since it helps minimize the customer impact from a disaster that may affect one location. For example, if one contact center needs to close due to a threatening major storm in the area, that center can redirect its calls to an alternate center in an unaffected part of the country. Our national operations infrastructure is a benefit for our customers since it limits the likelihood that any one event will cause a significant impact to our customer service operations.

#### **Contact center infrastructure**

We pay particular attention to the design of our contact centers, not only to make them a safe and enjoyable workplace for our employees, but also to minimize the risk of a disruption. These efforts include special security access to the building, including security guards, camera systems, and lighting systems. The communications equipment is maintained in a secure and environmentally controlled computer room, which is supported by both backup batteries and generator power.

#### **Recovery Plans and Tests**

Our customer care teams work closely to monitor service levels, and the need to redirect calls to an alternate contact center. We have documented many of these routing patterns in our recovery plans to

streamline our ability to activate the technology in the event of an interruption, and to send calls to the teams that are best equipped to help the customer.

Describe the corporate commitment to providing DMS the necessary Customer Support Team staffing (resources) for escalations to address real-time public safety network problems and public safety Customer and End-user issues.

**Verizon Response**

Protecting the public and our nation takes deep commitment, endless preparation and tireless service. First responders need a network provider that understands the challenges they face and works as tirelessly as they do to help solve problems and create safer communities.

Verizon has been supporting first responders for over 28 years. We're committed to helping public safety organizations execute their missions safely.

As described above, our support teams are committed to helping keep your agency ready for whatever problems stand in your way, offering:

**24/7 customer support**

- Local account teams provide dedicated account and technical support built on long-standing customer relationships
- Special support teams are deployed specifically to serve the needs of large public safety agencies

**Support before disaster strikes**

- Preparation is the cornerstone of our commitment to first responders
- We never stop preparing our network and support teams to help your agency whenever you
- need us

**Support after disaster strikes**

- Our dedicated Verizon Response Team (VRT) helps keep first responders ready to protect their communities during disasters
- Our business continuity teams help restore the network to your community after a disaster
- In 2019, the VRT had 405 emergency deployments and loaned 5,318 devices to enable business continuity and disaster recovery
- In 2020, our VRT had over 2000 engagements, over 1200 deployments and we loaned over 5400 devices.; As of February 9, 2021, the VRT has had 83 deployments and loaned 607 devices to enable business continuity and disaster recovery.

Describe the corporate commitment to providing DMS the information it requires for notifications on significant public safety performance impacts.

**Verizon Response**

Responding to emergencies, disasters and incidents requires your best coordination and communication. The last thing you should be worrying about is your choice of network. You need to focus on your mission, not your connectivity. You need to know that your network will be reliable, today and tomorrow. As described above, Verizon's Network Event Notification Program provides DMC with timely notification of events that may impact public safety performance.

Describe the use of an escalation procedure related to real-time public safety network problems and public safety Customer and End-user issues.

**Verizon Response**

As described above public safety Customers and End-users can contact Verizon’s dedicated help-desk for troubleshooting real-time public safety network problems and other issues. Verizon is committed to ensuring Customers and End-users have a clear path of escalation and have provided points of contact who can review and escalate public safety issues.

Describe the Respondent’s dedicated customer service, including helpdesk support and ongoing LTE training offered to public safety entities for the integration of LTE into State public safety communications.

**Verizon Response**

Verizon’s dedicated customer service, including escalation path, and helpdesk support. Your Verizon account team can create a training program with your assistance and guidance. This training program could include on-site training at locations across the country, online training is also available by device/application on Verizon’s website, and webinars as needed to ensure your employees are comfortable with their new devices and services.

On mutually agreed upon days and times, a Verizon account team member can be assigned to your organization’s location for additional support and training of your Corporate Subscribers at no additional charge. If equipment is delivered by a Verizon representative, the account team member can review the basic features of the device, as well as any service features you may be receiving. Alternatively, if equipment is shipped to your organization, your employees always have the ability to contact their account team member in order to receive additional information on any features or services.

Your employees can learn about device hardware, software applications, email setup and Smartphone maintenance on their own schedule through our Online Learning Center sessions. There are recorded and/or live sessions available presented via Adobe Connect software In addition to an ongoing training program, Verizon’s Account Team will keep DMS abreast of developments made possible through technological advancements as they become commercially available for the integration of LTE into State public safety communications.

Submit a defined list of eligible users that are public service entities, and describe how the Respondent will restrict access to their public safety service plans.

**Verizon Response**

Verizon identifies eligible public safety users by their NAICS Code. Eligible Public Safety NAICS Codes are listed below. Only entities that fall under these classification codes will be allowed to activate devices on a Verizon public safety plan or service. Verizon further separates these entities that qualify for public safety plans or services by placing these entities in a public safety root profile. Entities not in a public safety profile cannot activate public safety services without an approved exemption from the Verizon State and Local contracts team. In addition entities not in a public safety root profile will not have the ability to see public safety plans or services in our online portals.

**Eligible Public Safety NAICS Codes**

485111 Mixed Mode Transit Systems (Rail & Buses)	922190 Other Justice, Public Order, and Safety Activities
--	---

485112 Commuter Rail Systems	923120 Administration of Public Health Programs
621910 Ambulance Services	928110 National Security
922110 Courts	926120 Regulation and Administration of Transportation Programs
922120 Police Protection	926150 Regulation, Licensing, and Inspection of Commercial Sectors
922130 Legal Counsel and Prosecution	926130 Regulation and Administration of Comms, Electric, Gas, Utilities
922140 Correctional Institutions	921150 American Indian and Alaska Native Tribal Governments
922150 Parole Offices and Probation Offices	921190 Other General Government Support
922160 Fire Protection (except private)	921110 Executive Offices

Describe the Respondent's geographic coverage, both current coverage as of the time of Response, and also planned coverage during the term of the Contract. This should be accompanied by:

a. Detailed coverage maps

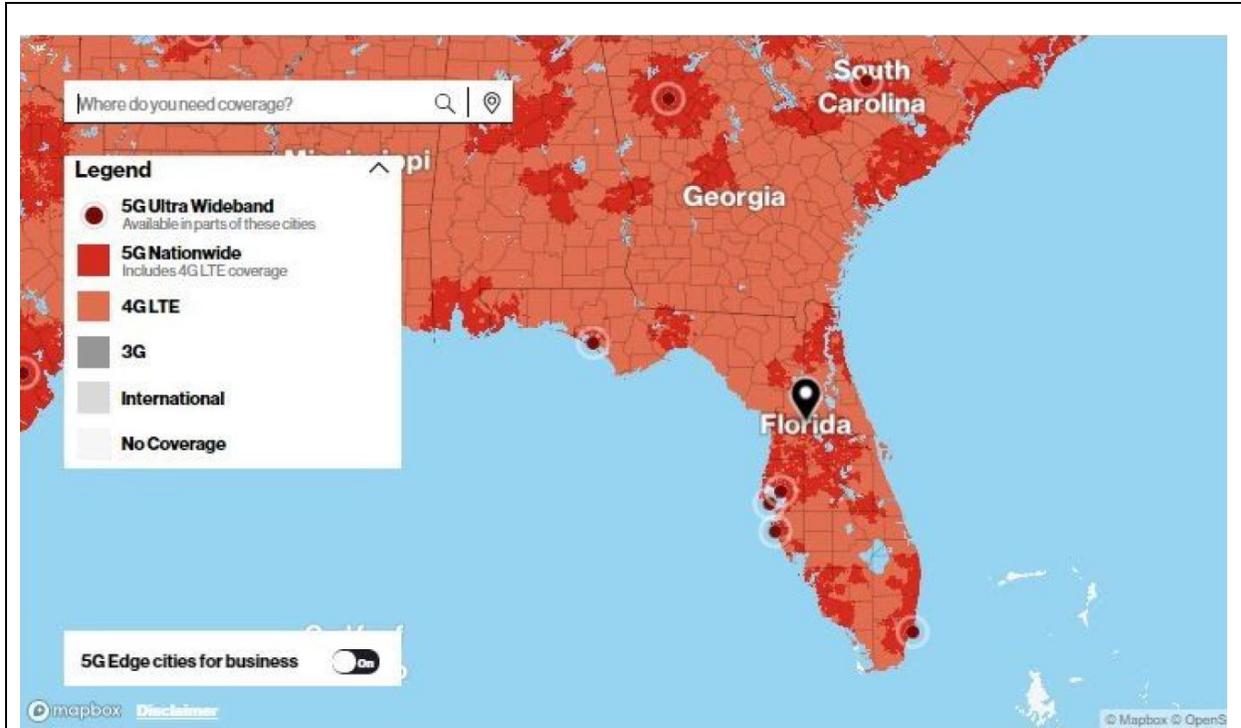
i. Provide detailed in-network voice, high speed (third generation -3G & fourth generation -4G, next generation such as 5G) and low speed (second generation -2G) data coverage maps for Florida (covered directly or through identified roaming agreements partnership).

**Verizon Response**

Our online Coverage Locator tool depicts our wireless coverage area on a national map and enables you to zoom into any local area by entering that area's ZIP Code or the city and state information. The maps rendered show approximations, based on our internal data, of where coverage for various services is available.

Our online domestic Coverage Locator tool can be accessed on Verizon's website.

A coverage map has been provided below for your review and consideration.



- ii. Provide a service area coverage map for Push-to-Talk (PTT). In addition, PTT protocols in use are to be identified. If some areas of the State have newer, higher performance or more capable PTT, those areas should be identified. If multiple types of PTT are supported, identify the technology and areas covered.

#### **Verizon Response**

Verizon's PTT and Mission critical PTT solutions use Verizon's award winning 4G LTE network to deliver seamless communications between PTT Responder users and it is available everywhere Verizon 4G LTE coverage is available. A detailed coverage map has been provided as a response to the above requirement which reflects Verizon's coverage in the State of Florida.

Describe how Mission critical Push-to-Talk (PTT) devices and services shall meet the "mission critical" definition as defined by the National Public Safety Telecommunications Council (NPSTC), as described SOW section 4.8, "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."

#### **Verizon Response**

Verizon's Mission critical PTT solutions are based on the MCPTT 3rd Generation Partnership Project (3GPP) standards compliant application designed to support public safety users' communication

needs.<sup>3</sup> It delivers Land Mobile Radio (LMR)-like functionality using Push to Talk services over LTE and new advanced functionality such as video and data services intended to enhance the experience and capability of public safety users to manage emergency situations beyond simple push-to-talk communications. Push to Talk Responder provides seamless communications between PTT Responder users and traditional public safety Land Mobile Radio (“LMR”) networks via interoperability. By implementing a LMR Gateway as part of the overall Push to Talk Responder solution, mobile device users are able to communicate securely with devices on your agency’s private LMR network.

Describe the Respondent’s approach to ensuring quality of service, priority and preemption as indicated in the 3GPP standards; the level of priority given to public safety entities and the methodology behind administering the level of priority; and the Respondent’s approach to ensuring public safety service plans and devices meet the public safety standards as described SOW section 4.4, “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.”

#### **Verizon Response**

Verizon’s public safety solutions are network integrated solutions with dedicated QoS Class Identifier (QCI) as required by the 3rd Generation Partnership Project (3GPP) standards to ensure voice and data are allocated the appropriate Quality of Service on the Verizon LTE network, combined with other advanced LTE network features such as Priority and Preemption, they provide priority on-demand communications to Public Safety users in times of network congestion.

Mobile Broadband Priority allows customers to connect to the network with priority by leveraging a pool of radio resources dedicated to enable their connection. Mobile Broadband Priority identifies the user with an Access Priority setting, giving them higher priority for network access than lower Access Class users.

Preemption automatically activates to provide approved personnel uninterrupted access to the network in those uncommon times when the network is fully utilized. 911 calls are never preempted.

Describe the local control portal, as described in SOW section 4.3.

#### **Verizon Response**

Verizon’s **Local Network Command** is a tool that provides on-demand local control of pre-selected users’ network quality of service on a temporary basis. Local Network Command provides qualified agencies the capability to pre-select users to be temporarily uplifted on-demand during an incident. Local Network Command users get a temporary uplift of their QoS for data service for the duration of the incident. This uplift increases the priority treatment of data sessions through the Verizon network. The tool also provides the location of those users uplifted in a map for the duration of the incident. Once an agency has been approved to get the service, the agency needs to pre-select the users that will be up-lifted at the time of an incident and create authorized users to access the Local Network

---

<sup>3</sup> Clarification. Established cellular industry and performance standards serve as the foundation for our engineering, design, operation and quality assurance programs. Verizon confirms that we are continually working to adhere and perform to 3GPP standards at all times.

Command Portal to be designated as Incident Commanders. Incident Commanders are authorized users that have access to the Local Network Command tool and have the capability to create and close incidents on the Local Network Command portal.

In order to up-lift end-users service at the time of the incident, the incident commander must create an incident using the Local Network Command (LNC) tool and select the LNC enabled lines that will be up-lifted. Incident Commanders can select individual lines or a pre-defined group to be uplifted.

Once a user profile is uplifted, the user profile will temporarily get an updated Quality of Service (QoS) for data traffic on the Verizon network for the duration of the incident.

After the incident has been completed or the time allotted for the incident has expired, all the participant end-user profiles will be set back to their original default profile.

## 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.

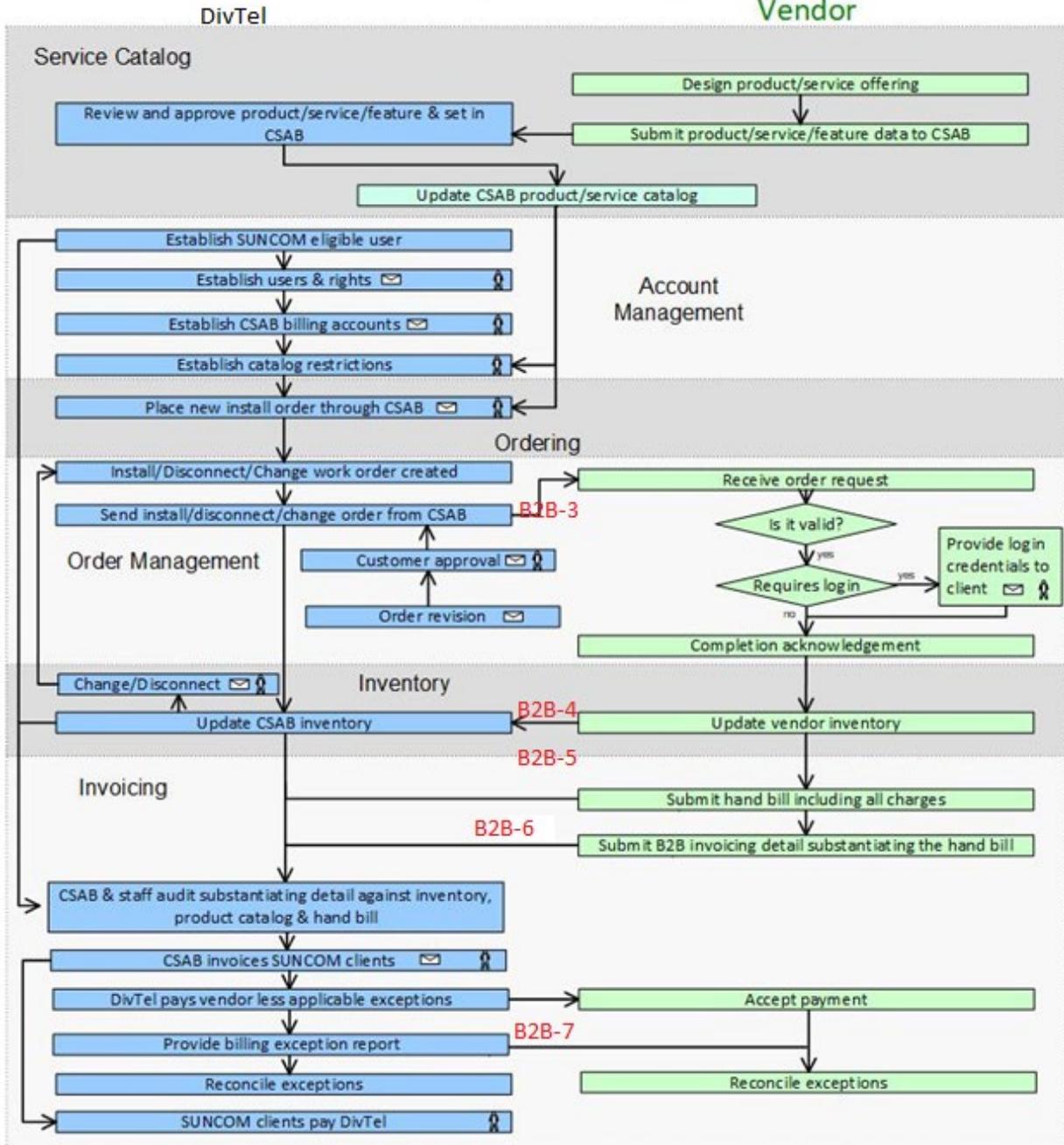
For DMS-billed MCS accounts, the Contractor will bill DMS monthly for services rendered to all Customers and provide DMS with substantiating details in electronic files (for example, comma delimited). The Contractor will include in the substantiating detail charges with unique identifiers for each transaction (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 may 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 DMS preferred method is API; however, this is not mandatory. 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 may 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. 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 MCS services in the CSAB Service Catalog:

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. A description of 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.

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 within two (2) billing cycles after the credit has been determined. **Attachment C, SLA-F2**. Both the handbill and electronic files for the CSAB portion must be received no later than the 10<sup>th</sup> calendar day of each month, unless otherwise agreed with DMS in writing.

## 5.11 Electronic Substantiating Detail File

The invoice substantiation file consists of electronic detail listing all billable services and activities with the CSAB Inventory ID 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 usage for each billing period (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 two (2) billing cycles from receipt of dispute. If Contractor has not resolved audit exceptions within two (2) billing cycles, 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 1<sup>st</sup> and run through the end of the month based on the completion date, unless otherwise agreed by DMS in writing. 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 catalog for Customers. The MFMP 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]."

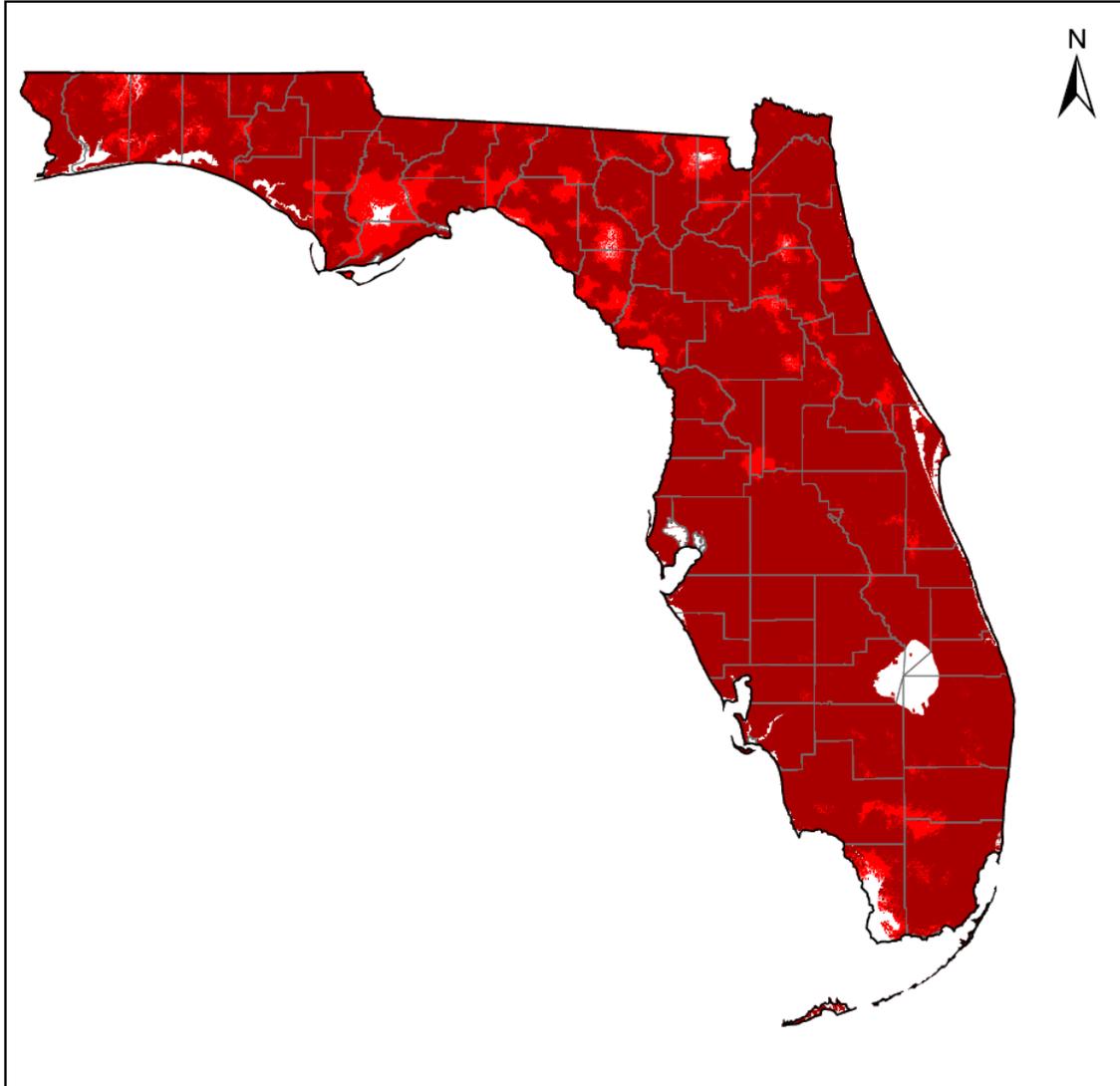
No response required. By submitting a Reply, Respondent has read, understands, and will comply with the statements contained in this section.

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.**

# Attachment A



## Verizon Wireless 4G LTE Coverage - Florida

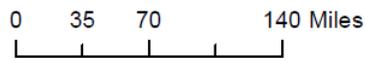


Map Created on 11/24/2020

This map is not a guarantee of coverage and may contain areas with no service.  
 4G LTE Core Area - Access to the 4G LTE network within the Core area.  
 4G LTE Border Area - Access to the 4G LTE network within the Border area; certain conditions may cause your service to connect to 3G in this area.  
 This map shows approximately where rates and coverage apply based on our internal data. Wireless service is subject to network and transmission limitations, including cell site unavailability, particularly near boundaries and in remote areas. Customer equipment, weather, topography and other environmental considerations associated with radio technology also affect service and service may vary significantly within buildings. With "all-digital" devices you can only make and receive calls when digital service is available. When digital service is not available your device will not operate or be able to make 911 calls. Check the roam indicator on your phone to determine actual areas where service rates apply.

**4G LTE Coverage**

- 120 dB RLOPL
- 133 dB RLOPL
- COUNTY



## Verizon's Experience Reply

Verizon Wireless ("Verizon") has the most reliable network utilized by public safety across the country. Our premier network is available in more than 500 markets and covers about 98% of the United States population with 2.4 million square miles of 4G long term evolution ("LTE") network coverage and capacity. Over our advanced 100% fiber optic network, we provide Voice over LTE Wireless Priority Services, enhanced private network traffic management, and Push-To-Talk Plus with Land Mobile Radio interoperability. In sum, we deliver the best in class LTE network for public safety today.

Verizon has many years of experience providing wireless communication services to public sector clients within the State of Florida. Additionally, we have provided point of contact information for agencies that have agreed to act as references for our wireless services. These agencies will determine what information they will share with you when contacted by the State.

We estimate our market share for 2019 to be 37.8% of the U.S. wireless retail subscriber base [includes postpaid and prepaid subscribers; calculation based on top four carrier-reported numbers]. At the end of the third quarter of 2020, the total number of the population covered within our licensed U.S. territories was 329.1 million. Our 4G LTE network is available to more than 99 percent of the U.S. population and covers 326.1 million people over more than 2.6 million square miles. For additional information, please see the attached coverage map(s) in Section # or visit [www.verizon.com/coverage-map](http://www.verizon.com/coverage-map)

It is important to look at coverage in terms of network reliability and the number of people who have wireless coverage within a given geographical area rather than the number of cell sites. Because of the improved spectral efficiency of the Orthogonal Frequency Division Multiple Access (OFDMA) technology used in 4G LTE network, we can serve a large population within a geographical area with higher voice quality and data speeds with a reduced number of resources. Our choice of the 700 MHz frequency as the basis of our 4G LTE network results in a longer range from the base station. The superior characteristics of the 700 MHz frequency range coupled with the use of MIMO (Multiple Input/Multiple Output) antennae will maximize the use of our existing network infrastructure while delivering high-speed, feature-rich services to our customers.

### Customized Approach

Our robust network partner eco-system allows us to provide the right solution for the unique challenges that our first responders encounter daily. Today, we are solving first responder challenges: situational awareness, intelligent tracking and transport, energy management and community engagement.

Our approach is performance based to achieve the best possible solution while ensuring that our government customers have the network, features, functionality, and reliability that they deserve. The current industry available technological options would be available to the State of Florida ("the State"). It is important to note that Verizon is committed to providing the services that Florida requires now and into the future.

We believe in competition, thereby allowing industry and the marketplace to help establish the solution that can meet the objectives of the State including a technological architecture that would be cost effective, reliable, secure, and delivers the coverage and capacity needed by the State's users. Please also refer to Verizon's Public Safety FAQs included with this response for additional information.

We understand your concerns over cost, network reliability, security, coverage, and expertise in supporting Florida wireless mobile telecommunication services. Verizon Wireless has years of experience designing, implementing, and operating a wireless network in Florida and across the US. In a marketplace where some of our competitors ask customers to compromise on network quality, we, at Verizon, are united in our belief that "better matters" and confident of the unique role we play in delivering all the benefits of the digital world to our customers.

Our wireless devices, services and solutions easily integrate into existing IT environments, enabling organizations to use many of the applications and technologies they already have in place. Combining our solutions with existing technologies gives your end-users access to the applications they use the most, – enabling them to remain productive and efficient whether in the office or on the go. By combining a variety of devices, wireless access options and applications, Verizon can build wireless solutions to help public safety run more smoothly and efficiently.

**Verizon's Public Safety Core**

Verizon has built and operates its own Public Safety core dedicated to public safety communications. The network core manages and directs all communications functions, like network access and call routing. The dedicated public safety core operates separately from our commercial core and provides first responders with access to the company's 2.4 million square mile 4G LTE network. We make priority access and preemption services available to public safety when necessary and at no charge. In addition, we have invested in new mission-critical 4G LTE voice communications to complement existing services such as Push-to-Talk Plus ("PTT Plus"). PTT Plus already includes interoperability with existing Land Mobile Radio networks.

**Our Commitment to Quality**

Our commitment to quality is evident in our ongoing investment in the expansion and enhancement of our network. We have invested more than \$122 billion nationwide since 2000 to build and enhance our wireless network, and consistently earn top rankings from independent consumer reporting and testing institutions for network quality and performance.

We strive to operate our wireless network at optimal performance levels so that we can continue our record of providing the most reliable nationwide wireless network. We continually test and evaluate network performance, and when service anomalies are detected, we take immediate steps to resolve or remediate the situation. Our maintenance organization staff members are distributed in centers across the country and have areas of expertise and responsibility, such as microwave, switch, cellular radio, power. They are also cross-trained to handle a wide variety of system maintenance issues - all in an effort to maintain service reliability. Our success in these efforts is evidenced by the fact that fewer than 2 percent of the calls placed on our wireless network are dropped or fail to initially connect - even during the busiest hours of the day - as well as by our continual subscriber growth.

**Network Performance**

Recognizing that reliable wireless service is critical to your business, Verizon has established extensive preventive maintenance measures, network monitoring and system backup capabilities. These measures, coupled with our internal performance processes, enable us to provide our customers with levels of wireless service reliability that distinguish us from other national wireless carriers.

Two common service metrics used by the wireless industry to measure network performance are accessibility (ineffective attempts (IA) for voice calls or setup failures for data sessions) and retainability (lost calls [LC] for voice and dropped connections for data). Accessibility measures when a subscriber attempts to place a call or establish a data session and fails, and retainability measures calls or data sessions that are in progress but communication is interrupted by no overt act of the subscriber. While the industry uses these measures broadly to index call quality, we use one of the most stringent methods of applying these measurements. All reasons excluding landline network congestion are considered in arriving at the percentage figure that measures our wireless IAs.

We have experienced great long-term success in attaining the goal of keeping the aggregate percentage of accessibility or retainability failures below two percent across all of our markets. While our competitors may report percentages that are similar to ours, the methods of measurement by which they arrive at this network performance result may vary from the stringent methods we apply. When measured on a monthly average across the entire Verizon-owned and -operated network, our wireless network service level goals are:

- Cell availability (total Verizon wireless network):
  - Cell availability is greater than or equal to 99.9% every month of calendar year
  
- Data:
  - Dropped connections (total Verizon wireless network): Less than or equal to 2 percent, reported nationally as a monthly average
  - Setup failures (total Verizon wireless network): Less than or equal to 2 percent, reported nationally as a monthly average
- Voice:
  - Lost calls (total Verizon wireless network): Less than or equal to 2 percent, reported nationally as a monthly average
  - Ineffective attempts (total Verizon wireless network): Less than or equal to 2 percent, reported nationally as a monthly average

Independent third party engineers conduct approximately eight million tests annually of our network, along with

other national wireless carriers' networks, while traveling almost 500,000 miles across all 50 states and the top 125 urban markets. The tests are a combination of voice, data and text in order to mimic real world users' experience.

Each test is analyzed as for the ability to access the network and complete the given task. For voice calls, they are classified as either a successful call, an ineffective attempt (a call that is blocked) or a lost call (a call that connects, but drops). Data testing includes large file downloads, uploads and smaller file downloads. The results are then published and analyzed by Verizon engineers to analyze all failures.

Voice network reliability test results have consistently shown that the number of ineffective attempts for our national network, in major metropolitan centers and some remote areas, is lower than for any other national carrier. Test results also indicate that voice calls that connect on our network are more likely to stay connected for the duration of the call. Similarly, the data network reliability test results establish that we have the nation's most reliable wireless 4G LTE network, successfully setting up a higher percentage of data sessions than any other national carrier, and successfully completing a higher percentage of tasks during those sessions.

In addition to the strenuous third party drive collection, Verizon also leverages many other data sets to ensure that the network continues to perform at the highest level. This includes additional third party information as well as internal Network KPIs that are constantly monitoring the performance of the network.

### **Business Continuity**

Verizon has taken many steps to prevent outages from affecting our wireless customers. Our emergency response capabilities have been tested and proven during many difficult situations including wildfires, tornadoes, flooding and hurricanes.

### **Our Network**

Our reliable network is a combination of strong technology and capable employees. Network operations teams across the country conduct exercises each year to confirm team members have access to contacts, systems, tools, and suppliers to resolve the impact if any disruption occurs. These teams are empowered to identify and implement ways to make our network stronger, more efficient, and available for our customers when they need it, even during natural disasters. Thanks to these efforts and ongoing preparations and investments, our network has stayed strong – even through the natural disasters of past years – while other communication networks often were adversely impacted or failed.

We provide voice and data service through a sophisticated wireless network consisting of dozens of switching systems and thousands of base stations throughout our cellular footprint. Many critical network systems are located in geographically diverse locations. The most critical systems provide un-interrupted service to customers, even if one location is damaged. These systems are designed to automatically fail-over to an alternate location with minimal, if any, impact to customers. These systems are tested at least annually as part of the Business Continuity/Disaster Recovery program, and in many cases are tested more frequently to maintain reliable service.

Many critical circuits in our network infrastructure are provisioned with special priority. This is intended to ensure that in the event of a disruption, these circuits are repaired as quickly as possible. The costs for this service are just one part of our significant ongoing investment in network reliability.

### **Mobile Switching Center (MSC)**

The loss of a MSC is one of the most serious of possible scenarios. Each MSC is protected by automatic power backup systems, by automatic fire-suppression systems, and by physical security systems and alarms. In each MSC, network operations personnel routinely backup system data for the switch itself and the peripheral systems. Automated backup routines are supplemented with scheduled manual backup routines and off-site storage of critical data.

### **Cell Site**

We have thousands of cell sites across our nationwide network to provide the desired level of service, both in terms of capacity and quality of service. We continue to increase the density of our cell sites, often through small-cell locations, which can provide overlapping coverage and reduce impact to our customers if an individual cell site is damaged or disrupted. Despite the large number of sites, we still take the loss of a single cell site seriously. Cell sites are protected by automatic fire detection systems, by physical security systems and alarms, and most have automatic power backup systems, including batteries and generators. Through arrangements with our suppliers, any major components of a cell site, up to and including the building and tower, become an immediate priority restoration effort on the part of both Verizon and our suppliers.

**Service Protection and Restoration Strategies**

Service protection and restoration strategies are an integral part of our wireless network management. MSCs, Network Data Centers, and cell sites are automatically and continuously monitored for numerous factors, from call processing to room temperature. All MSCs and cell sites have battery backup and most cell sites have permanent generators. We also maintain and utilize a fleet of dozens of Cell on Wheels (COWs) and Cell on Light Trucks (COLTs), and Generator on a Trailer (GOATs) that can be rolled into hard-hit locations or areas that need extra network capacity. In addition, we also maintain towers on wheels and portable generators. We have implemented Telecommunication Service Priority (TSP) capabilities on critical backhaul circuits, which provide priority service restoration if a circuit is disrupted.

**Monitoring and Alarm Systems**

We have two geographically diverse Network Operations Centers (NOCs) that monitor all facilities, cell sites and switches across our nationwide network. These NOCs are staffed 24x7 with experienced personnel who work closely with the regional field operations teams and with suppliers to coordinate and expedite the restoration of service in the event of outages. We have set up alarms for critical components at the cell sites and the MSCs. These send prioritized alarms and detailed data to the MSCs and NOCs. The detail includes identification of any malfunctioning module and the component responsible. Alarms are coded with varying degrees of priority, so that minor problems do not obscure critical problems from a technician's attention. The code also helps the technician determine how quickly the problem must be addressed.

**Response Time**

In the event of an alarm or other failure indicator, our personnel will be dispatched to the cell site, MSC, or Data Center with a standard set of spare parts and repair equipment, in addition to other parts and equipment that are indicated by the nature of the alarm and failure. Maintenance personnel provide ongoing support for our equipment and facilities to minimize the possibility of disruptions and to verify proper performance. We work closely with our suppliers to see that we have access to their engineering personnel and replacement equipment when required. We also have the ability to dynamically reroute traffic over our backbone network to address switch, microwave, interconnection problems, or capacity issues.

**Respondents Experience**

While Verizon Wireless is truly a 21st century company, the mergers that formed Verizon were many years in the making, involving companies with roots that can be traced to the beginnings of the telecommunications industry in the late 19th century.

Verizon Wireless has been in business since 2000; however, the companies that merged to form Verizon Wireless had been in business for an average of 15 years. Verizon Wireless has more than 120.3 million wireless retail connections (September 30, 2020). We provide wireless service to organizations of all sizes including small businesses, Fortune 500 corporations, including federal, state and local governments. We also have considerable experience providing service to entities with subscriber lines in excess of 10,000.

Additionally, we have included point of contact information for entities that have agreed to act as references for our wireless services. These entities will determine what information they will share with you when contacted by DMS. Please refer to completed Form 6 - Business Experience included in this response.

**Software Support: Third Party Solutions**

We offer an array of mobile business solutions from our strategic technology partners (Third-Party Solution), giving organizations access to some of the industry's most innovative products and services, with the added benefit of enabling customers to consolidate their mobility spend on a single bill.

**Enterprise Management Solutions****IBM MaaS360 with Watson**

IBM MaaS360 with Watson is a trusted enterprise mobility management (EMM) solution that makes working in a mobile world simpler and more secure. It uses powerful mobile device management with comprehensive, integrated protection to enable applications, content, email and devices, without compromising the user experience, data security or privacy. IBM MaaS360 is the first EMM to integrate Machine-Based Learning/Artificial Intelligence into the EMM suites via Watson.

IBM MaaS360 with Watson delivers insights and analytics to make it faster, easier and more effective to manage and secure endpoints, their apps, data and content.

**MobileIron**

MobileIron provides Enterprise Mobility Management (EMM) security and solutions for Mobile Application Management (MAM), Mobile Content Management (MCM) and Mobile Device Management (MDM), meeting the needs of small, medium or large enterprise customers. MobileIron EMM:

**Security Management Solutions****Asavie Moda**

Asavie Moda is a mobility service that optimizes employee productivity and gives businesses control and visibility to ensure a safe mobile internet experience. It is a network-based solution that enables businesses to manage security and productivity along with rich reporting insights on all their mobile devices.

**Lookout Mobile Endpoint Security**

Lookout Mobile Endpoint Security helps organizations prevent data loss and leakage via mobile devices by delivering advanced security and comprehensive policy-based protection against the spectrum of mobile risk.

Lookout empowers your organization to adopt secure mobility across personal and corporate owned devices without compromising productivity, employee privacy or user experience.

**NetMotion Software**

NetMotion's software solutions improve the performance, visibility and security of your mobile enterprise. NetMotion software gives your IT team the tools to monitor and dynamically make decisions using real-time data and analytics. NetMotion software has helpful management features

**Samsung Knox**

The Samsung Knox is a defense-grade security platform built into the latest mobile devices. This enterprise solution allows companies to secure, manage and customize their Samsung devices using one platform. It offers a cloud-based platform that enables users to remotely set corporate device policies and security measures, configure apps and user access, and activate/deactivate devices. Knox Workspace.

**Collaboration and Productivity Solutions****BlueJeans**

The BlueJeans video collaboration platform helps you modernize today's meetings to better meet the needs of today's workforce. It gives employees video conferencing solutions that enable them to virtually meet and communicate at a moment's notice with teammates, partners and customers. Moreover, BlueJeans' Smart Meetings technology includes in-app intelligence to capture the most important discussion points, assign action items, and quickly replay meeting highlights to help bolster the effectiveness of each meeting.

BlueJeans empowers fast and easy face-to-face communications, using video conferencing solutions to help bring people closer together for more effective collaboration. The platform combines high-quality audio, HD video and web-conferencing capabilities for cloud-based meetings or large interactive events. The BlueJeans video conferencing platform features a number of tools that help make it easier for workforces to communicate and collaborate virtually anywhere and anytime – simply, easily and securely.

**doForms**

doForms is a mobile data collection platform that provides a paperless solution for business customers. With easy form customization, doForms captures information such as GPS location, job dispatch and scheduling, mobile payment and inventory management with barcode scanning options. doForms has pre-built vertical-based solutions for healthcare, field services, transportation and retail.

**GoCanvas**

GoCanvas is a platform for creating and editing your own mobile app (forms) which enable users to capture information electronically on a smartphone, tablet or PC and send it to customers, colleagues or partners in seconds. GoCanvas facilitates the elimination of paper forms and increases productivity through mobile apps on just about any mobile device. GoCanvas App Store houses over 20,000 free mobile form templates including invoices, checklists, inspection apps, other common business documents and apps for specific verticals including Construction, Retail, Distribution, Healthcare and Professional Services. Businesses can customize existing applications or create their own. GoCanvas also enables you to generate high quality, professional PDF files to automatically send to your customers.

**Intrepid Networks**

Intrepid Networks' integrated mobile platforms are designed for Law Enforcement, Emergency Management, EMS, Fire and Rescue teams, as well as any team requiring coordination between disparate team members. The Intrepid Response package provides the entire team with a real-time, easily accessible, common operational picture. Providing next-gen situational awareness is what makes Intrepid Network's suite of products the ultimate resource for coordination beyond visual range while providing greater front-line intelligence. Intrepid's situational awareness apps can also fit a number of private sector business critical security needs. For example, they can be used for event management and crowd control at major sporting events, dignitary visits or other events that have integrated response teams who need to know what's happening at any given time. These teams also want to know where each team member is located and be able to share vital information as needed. Private and corporate security organizations can also benefit from similar requirements. Other private sector uses include infrastructure protection, where teams are assigned as security or emergency responders to protect important buildings and structures, such as hospitals, nuclear reactors and oil refineries.

### **Verizon Mobile Device Management**

Verizon Mobile Device Management (MDM) is a Verizon-branded management portal that integrates Verizon differentiated services into a unified and intuitive customer experience. Verizon's MDM solution features Enterprise Firmware Over the Air (FOTA) Management, Device Diagnostics for Verizon Wireless customers, Broadband Mobile Hotspot Management, and Unified Endpoint Management.

Verizon's Business and Government Customer Operations (BGCO) teams handle support for ordering licenses and billing. However, Verizon Wireless is not the licensor of the mobile business solution. Customers obtain any license directly from the applicable Third-Party Solution provider. Customer support for Third-Party Solutions may be obtained directly from the Third-Party Solution provider or by calling Verizon Wireless technical support. The BGCO provides basic Tier 1 support, which may include set up and how to use, before advising customers to contact the Third-Party Solution provider directly. BGCO support can be reached at 800-922-0204. If the BGCO determines that an inquiry is not one concerning Equipment or Wireless Service, BGCO support may transfer the service request to appropriate Third-Party Solution representatives.

### **Device Support**

#### **Device Training**

Your employees can learn about device hardware, software applications, email setup and Smartphone maintenance on their own schedule through our Online Learning Center sessions. There are recorded and/or live sessions available presented via Adobe Connect software. The Online Learning Center can be accessed at <https://www.verizon.com/support/simulators/>.

### **Device Warranty**

As part of the wireless device equipment package, your employee will receive the manufacturer's equipment warranty, typically one year in length.

Whether or not a new device is defective out of the box, your corporate-liable end users may return wireless equipment purchased from us for any reason within 30 days of the original date of purchase.

#### **31 Days to 12 Months**

If a device is found to be defective more than 30 days but less than 12 months after the purchase date, and the malfunctioning device is still within the manufacturer's warranty period, you may obtain a Certified Like-New Replacement device in exchange for the defective unit at no charge. The remaining unused term of the original manufacturer equipment warranty or a total of 90 calendar days, whichever is greater, will transfer to the exchanged unit.

#### **13 Months to 23 Months**

If the defective device is beyond the manufacturer's warranty period, we will offer a Certified Pre-Owned device for purchase.

#### **24 Months or More**

If a device is found to be defective 24 months or more after the purchase date, and is not covered by an equipment protection program, unless otherwise provided in your agreement, your Government Subscribers will be eligible to upgrade at your discounted corporate equipment price at the end of a two-year agreement.

Several equipment protection programs are available for an additional monthly fee.

### **Staffing and Support**

**Key Staff Positions**

As an incumbent service provider to the State, Verizon's experienced account support team understands the State's unique requirements and provides an experienced team (inclusive of local staff) to proactively meet its needs and address any issues or concerns which may arise.

The following table describes the key staff qualifications of the support team for State of Florida:

<b>Position</b>	<b>Typical Verizon Experience</b>	<b>Role</b>	<b>Minimum State of Florida Qualifications</b>
Account Manager	5+ years	Responsible for sales and customer support to government accounts within the State of Florida. Expertise includes consultative support, sales presentations, training, problem resolution, and calling plan analysis.  Ensures the appropriate amount of staff at any given time from the Customer Support team. Available twenty-four (24) hours a day, 365 days of the year.	A minimum three (3) years' experience working with government clients in a government account management or sales role.  A knowledge of government business practices, including State practices and practices of Customers and public Safety Services.  At least three (3) years' work experience in the telecommunications industry.  Strong verbal and written communication skills, including the ability to communicate effectively at all levels of an organization.
Project Manager*  *To be determined based on assessment and/or evaluation of currently implemented solutions. This role to be reviewed and discussed during the contract negotiation phase.	TBD	Oversight and responsibility for all assigned projects under the DMS contract. Act as point of contact for DMS to coordinate all implementation and migration. Manage and direct the planning of the staff and resources in support of assigned projects under the DMS contract.	Responsible for every aspect of all projects related to the DMS Contract.  Lead and direct teams to deliver projects within the constraints of schedule, budget, and resources.  Demonstrated knowledge and experience to appropriately apply a project management methodology to projects.  Experience using Microsoft Project and the ability to keep all projects updated frequently and accurately.  A current Project Management Professional certification from the Project Management Institute, Scrum Master Certification from

## Attachment B - Final Statement of Work

			Scrum Alliance, CompTIA Project+ certification from CompTIA, a Lean Six Sigma certification, or other equivalent project management certification approved in writing by DMS
Business Operations Manager	3+ years	Oversight of business operations, including billing, ordering, and related business operational procedures under the DMS contract. Communicate DMS concerns to the appropriate Verizon management personnel. Authorized to effect business operational procedures and related outcomes in support of the DMS contract.	A minimum of three (3) years' experience working with government clients. Knowledge of government business practices, including State practices and practices of Customers. Strong verbal and written communication skills, including the ability to communicate effectively at all levels of an organization
Global Enterprise Advisor	2-4 years	Manages day-to-day account activity, complete account-specific projects, monitor accounts receivables, and, as needed, conduct bill reviews with authorized contacts to promote accurate billing. Can also provide personalized support for billing escalations and non-standard requests.	
Engineering and Design Manager*  *This role to be reviewed and discussed during the contract negotiation phase based on DMS' forecasted needs for dedicated support.	3+ years	Point of contact for all engineering and design issues. Responsible for directing all aspects of engineering and design concerns for the services. Authority to direct staff. Available twenty-four (24) hours a day, 365 days of the year to manage and oversee restoration of services and to address the State's requests.	A minimum of three (3) years' experience leading an engineering team responsible for services similar in size and scope to services available under MCS. A Bachelor of Science degree or higher in an engineering discipline. Equivalent foreign degrees are also acceptable. Five (5) years or more of engineering work experience.

## Attachment B - Final Statement of Work

<p>Operations and Security Manager</p> <p>*This role to be reviewed and discussed during the contract negotiation phase based on DMS' forecasted needs for dedicated support.</p>	5+ years	<p>Serve as the engineer capable of communicating with other engineers as needed to resolve day-to-day issues with DMS and engineers from other Contractors providing telecommunications to the State and, if applicable, subcontractors. Point of contact for the day-to-day networking, service, and security issues, typically those involving real-time concerns. Available twenty-four (24) hours a day, 365 days of the year as needed to manage operational and security concerns and to address the State's request</p>	<p>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.</p> <p>Experience with business continuity and disaster recovery, including experience in development of disaster recovery plans.</p> <p>Experience with information security architecture and security tools.</p> <p>Knowledge of telecommunications industry best practices for service performance and security and applicable laws and regulations as they relate to security.</p> <p>Knowledge of current technologies and processes used to establish and maintain networks with respect to security of MCS.</p> <p>May also be a Certified Information Security Manager, a Certified Information Systems Security Professional, or hold another current industry-recognized security certification.</p>
<p>Technical Specialist</p>	3-5 years	<p>Essential knowledge of cellular networking, switch operations, and data applications. Investigate, diagnose, and resolve customer inquiries. Troubleshoot roaming issues, support 800 line specialists, Company Stores, and roaming partners.</p>	

CSAB Administrator	3 years	Approves and monitors CSAB access privileges for Manages closeout and past orders. Reviews inventory data for Verizon services. Monitors other access as approved by DMS	
Customer Service Representative	4 years	Implement voice and data applications and resolve daily operational issues including training. Support of projects, implementations as well as operational changes.	
Technical Support	5 years	Team with specialized knowledge of cellular networking, switch operations, especially focused on data applications and solutions. Investigate, diagnose, and resolve customer inquiries beyond basic billing/device concerns. Coordinates trouble resolution with Verizon Network Repair Bureau, suppliers and wireless solution partners.	

Verizon must retain discretion and control over assignment of account management, customer support or other such Verizon personnel. Our prospective employees are investigated and reviewed to determine whether they merit employment at the positions for which they applied. All such information remains confidential and shared with third parties only on a need to know basis. Our employees are covered by the Verizon Code of Conduct, which can be provided for your review upon request. At any time, you may provide feedback to us regarding the skills, qualifications and performance of any member of the account management team. We will make every effort to notify you of any changes in your account team.

In the event of any change to any member of your account management team, we will work with the DMS towards achieving a smooth transition. Additional account support procedures are available in the event of personnel change. In addition, you can use escalation procedures as well as the cross-trained skills and experience of many account support personnel.

We may review any recommendations from you, as allowed by law, that will assist us in placing a Client Partner or Account Manager with the appropriate skills to support your account initiatives.

Although our goal is continuity of the Verizon account team, we cannot guarantee that changes in personnel and staffing assignments will not occur during the term of your contract. The structuring of the Business and Government Customer Operations organization enables all members of the Business and Government Customer Operations organization to be cross-trained on all accounts with the goal of each customer receiving the same comprehensive professional customer service.

#### **Account Team**

As an incumbent service provider to the State, Verizon provides an experienced account support team, inclusive of local staff to proactively address any issues or concerns which may arise.

#### **The Verizon Account Team**

Since 2004, Verizon has used a dedicated government sales and support model for all government sales in the state of Florida. The team is solely dedicated to state and local government and specifically trained in government contracting, ethics and compliance. This team provides local frontline sales and support to public safety, state, and local government as well as local EOC support during times of crisis. Today the team consists of over 40 employees living in Florida with a combined 240 years of experience supporting the State of Florida Department of Management Services Wireless Contracts with Verizon.

#### **Account Manager: Tom Madden, Government Client Partner, Public Sector, Verizon Business Group,**

As an incumbent Service Provider to the State Verizon's proposed Account Manager, Tom Madden, has served in this required key staff position and is well versed in DMS' requirements. Tom's credentials and 25 years experience meet or exceed all of DMS' requisite qualifications. Upon contract award, Tom will continue to fulfil the role of DMS' primary point of contact and full-time Account Manager for all MCS services provided under the resulting new Contract

The Account Manager for DMS under the State contract will serve as senior manager and primary contact, with responsibility for all day-to-day MCS issues, and the coordination and resolution of all MCS activities. These duties may include but are not limited to; overseeing account activity, discussing wireless communications objectives, as well as addressing any issues or concerns with the appropriate level of management (as necessary) working in concert with the rest of your support team. The Account Manager will continue to serve as the lead on account development, training, demonstrations, product updates, pricing, and statewide contract management. The Account Manager (or designated backup(s)) will be available twenty-four (24) hours a day, 365 days of the year to support the State's needs. Please refer to the resumes included with this response for further details.

#### **Saikham Baccam, Coordinator – Business Operations / Direct Account Support Rep**

Verizon Business Operations manager Saikham Baccam, Coordinator – Business Operations / Direct Account Support Rep is responsible for sales and customer support for government accounts within an assigned geographic territory. Expertise includes consultative support, sales presentations, training, problem resolution, and calling plan analysis. Provides follow-up training for new customers, handles equipment issues, performs rate plan analysis, explains billing and interacts with the Government support center on customer service issues. Please refer to his resume included below for additional detail.

#### **Customer Support Team**

The Business Government Customer Operations ("BGCO") team assigned to the State of Florida is determined by the geographical area of your headquarters location and can be reached toll-free at 800-922-0204. In the event your employees seek assistance after your BGCO team's hours, our standard full-service wireless Customer Care team is available from 8 AM - 9 PM, Monday through Saturday, and 8 AM - 5 PM on Sunday, in each time zone. Customer Care can be reached toll free at 800-922-0204 and airtime-free at \*611 from the wireless device. These Customer Care representatives are not specifically trained to support our government accounts, but can address many of your employees' inquiries.

If you are experiencing a technical issue with your service or equipment, our wireless technical support staff is available 24/7, 365 days of the year and can be reached toll free at 800-922-0204. Your authorized contact also has the option of contacting your Global Enterprise Advisor/Account Manager for assistance in managing your account. Please refer to the table above for additional information regarding the qualifications and experience of the team assigned to support the DMS contract.

#### **End User Training and Support**

Your Verizon account team can create a training program with your assistance and guidance. This training program could include on-site training at locations across the country, online training currently available by device/application at [www.verizonwireless.com](http://www.verizonwireless.com) and webinars as needed to ensure your employees are comfortable with their new devices and services.

On mutually agreed upon days and times, a Verizon account team member can be assigned to your organization's location for additional support and training of your Government Subscribers at no additional charge. If equipment is delivered by a Verizon representative, the account team member can review the basic features of the device, as well as any service features you may be receiving. Alternatively, if equipment is shipped to your organization, your

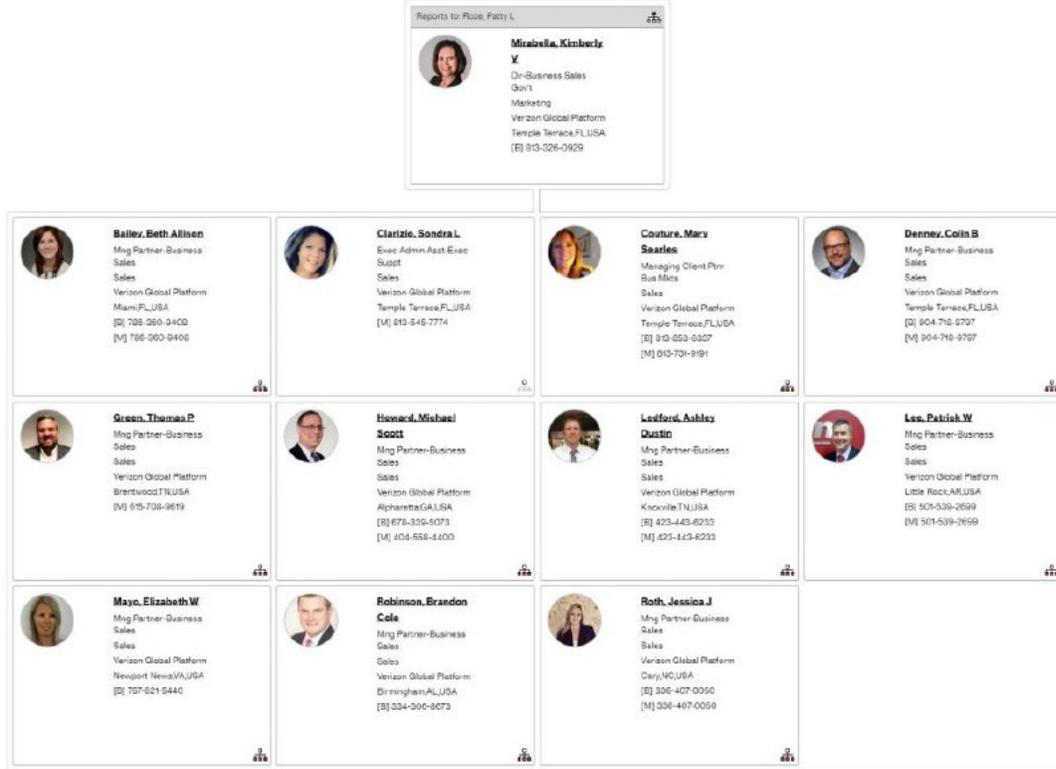
employees always have the ability to contact their account team member in order to receive additional information on any features or services.

Please note, your employees can learn about device hardware, software applications, email setup and Smartphone maintenance on their own schedule through our Online Learning Center sessions. There are recorded and/or live sessions available presented via Adobe Connect software. The Online Learning Center can be accessed at

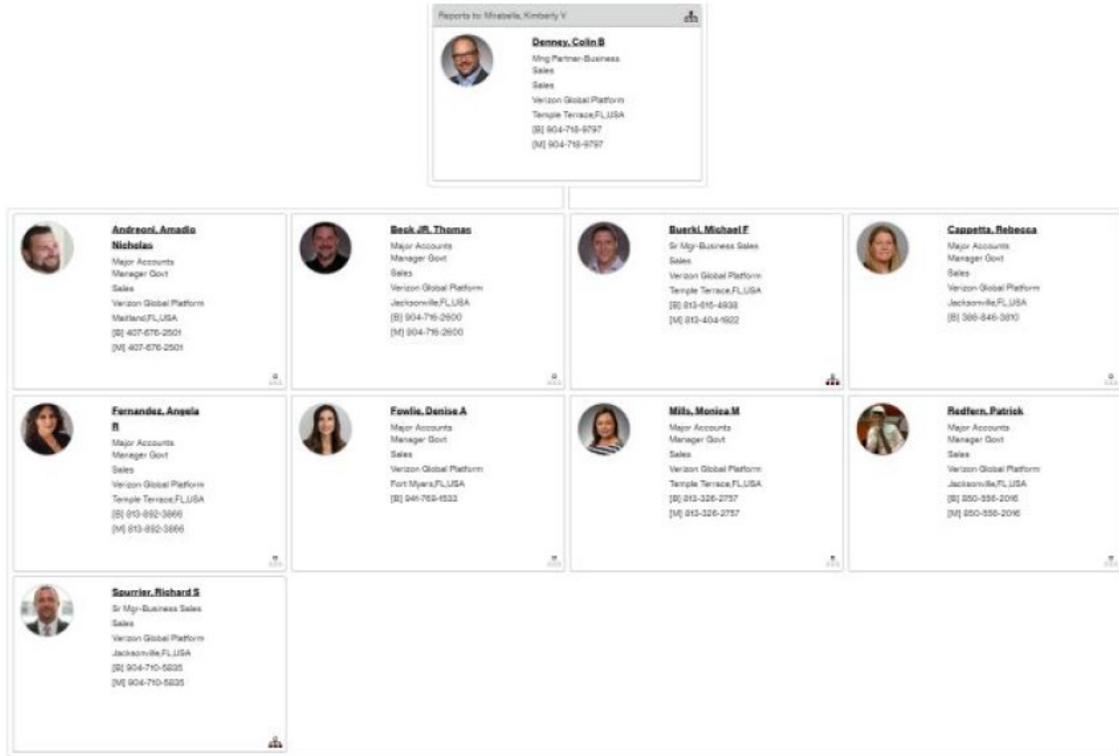
<https://www.verizon.com/support/simulators/> .

### Organizational Charts

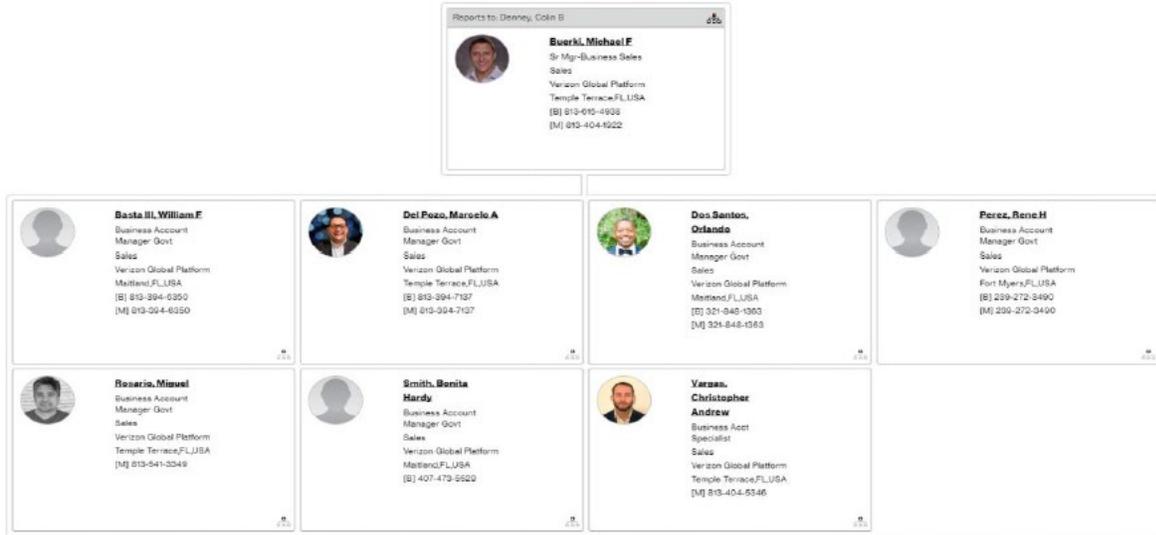
#### Leadership SouthEast Region Government Sales Support



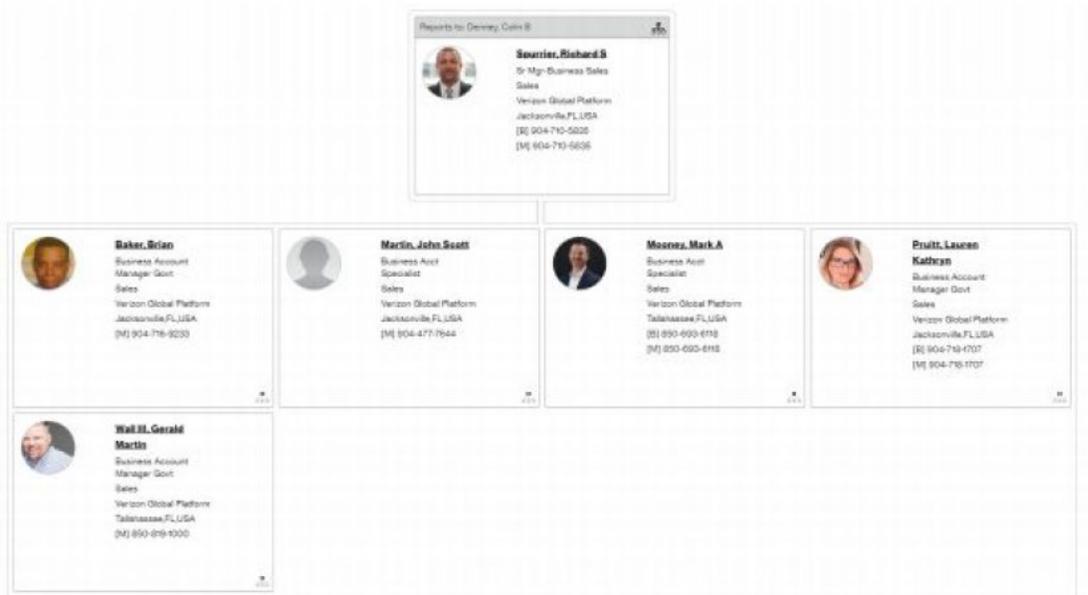
### North/Central Florida Government Sales Support



### North/Central Florida Government Sales Support



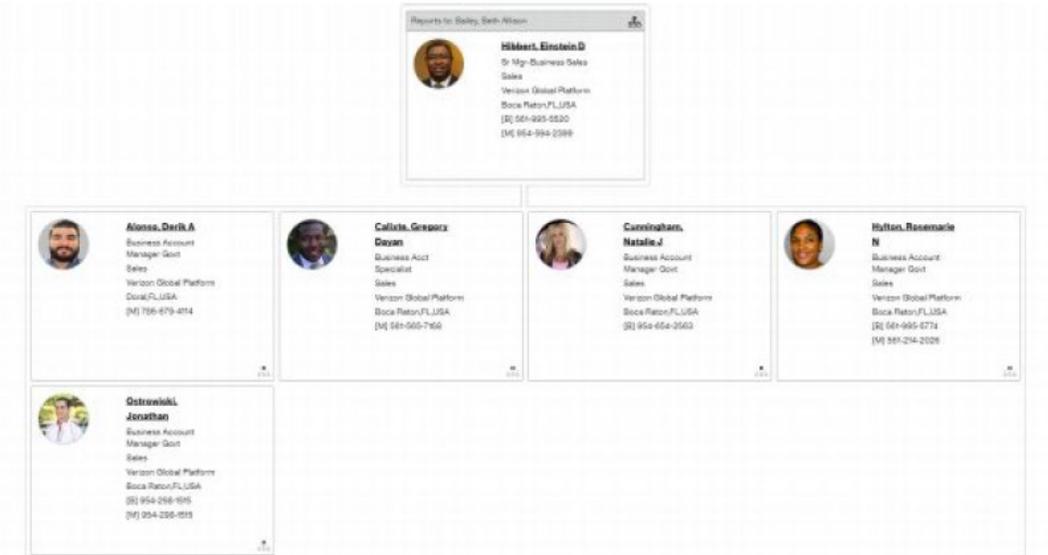
North/Central Florida Government Sales Support



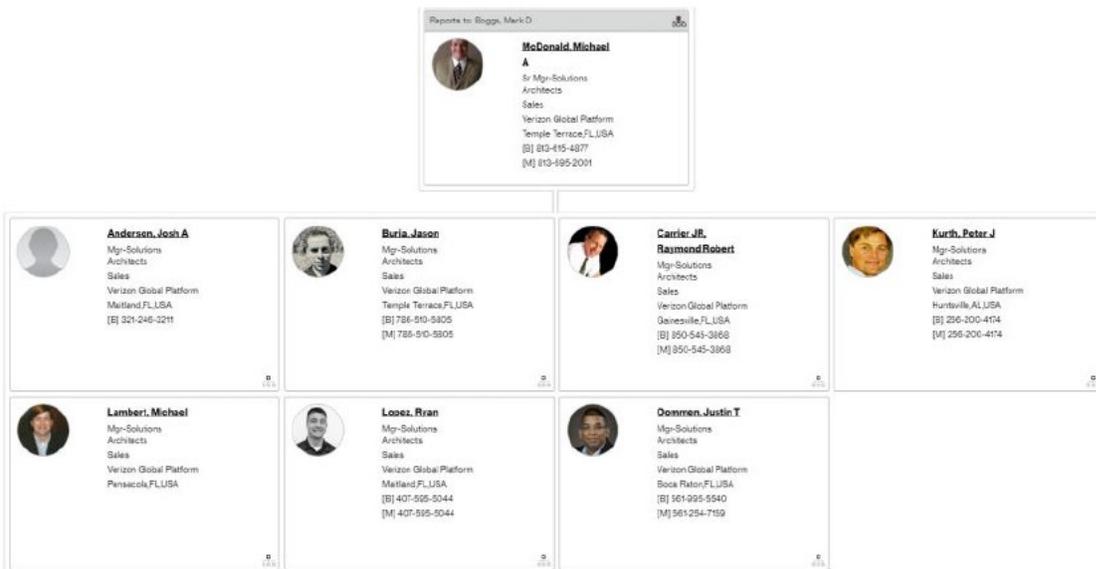
### South Florida Government Sales Support



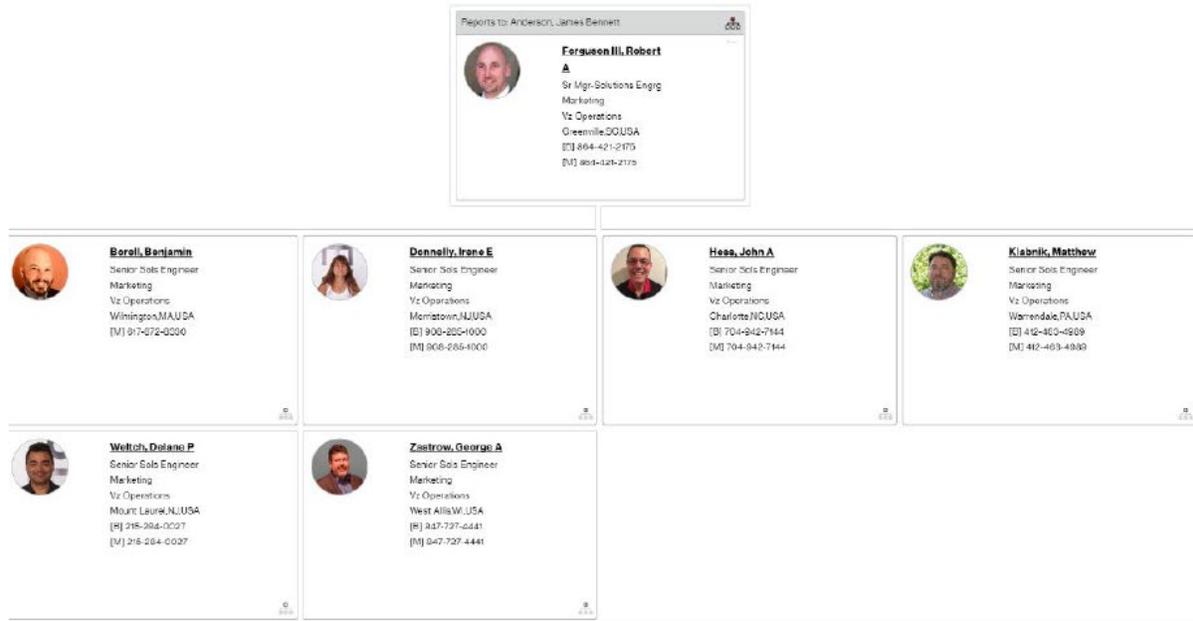
### South Florida Government Sales Support



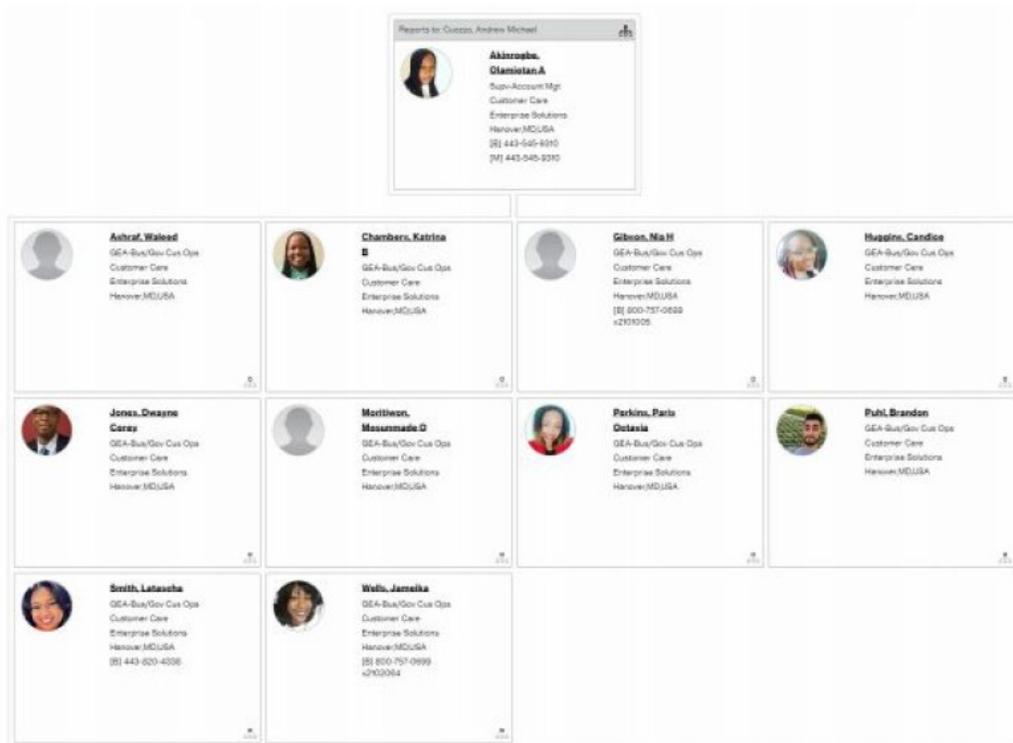
### Solutions Architects



### Solutions Engineer



### Business Government Customer Operations Support



## Letter of Bondability



November 5, 2020

Florida Department of Management Services  
4050 Esplanade Way  
Suite 335.3Y  
Tallahassee, FL 32339-0950

Re: Mobile Communication Services

To Whom It May Concern:

Liberty Mutual Insurance Company, a corporation under the laws of the State of Massachusetts, with an office and place of business 175 Berkeley Street, Boston, MA 02116, represents Verizon Wireless for surety bonding needs.

At the present time, Verizon Wireless is in a position to consider single projects up to \$5 within an aggregate limit of \$250 Million. The statement of these values is neither a commitment nor a limitation of the bonding capacity of Verizon Wireless. At the request of Verizon Wireless, Liberty Mutual Insurance Company will give favorable consideration to providing the required performance and payment bonds.

Please note that the decision to issue performance and payment bonds is a matter between Verizon Wireless and Liberty Mutual Insurance Company, and will be subject to Liberty Mutual Insurance Company's standard underwriting at the time of the final bond request, which will include but not limited to the acceptability of the contract documents, bond forms and financing. Liberty Mutual Insurance Company assumes no liability to Verizon Wireless, third parties or to you if for any reason Liberty Mutual Insurance Company does not execute said bonds.

If you have any questions or need any additional information, please do not hesitate to contact me.

Sincerely,

Erin M. Margelis  
FL Non-Resident License Number E095788  
Liberty Mutual Insurance Company  
A by A. M. Best Financial Size Category XV

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.





State of MARYLAND }  
County of PRINCE GEORGE'S } ss:

On November 5, 2020, before me, a Notary Public in and for said County and State, residing therein, duly commissioned and sworn, personally appeared

Erin M. Margelis

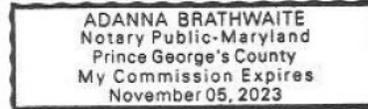
known to me to be Attorney-in-Fact of Liberty Mutual Insurance Company  
the corporation described in and that executed the within and foregoing instrument, and known to me to be the person who executed the said instrument in behalf of the said corporation, and he duly acknowledged to me that such corporation executed the same.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my official seal, the day and year stated in this certificate above.

My Commission Expires 11/05/2023

Adanna Brathwaite

Notary Public





This Power of Attorney limits the acts of those named herein, and they have no authority to bind the Company except in the manner and to the extent herein stated.

Liberty Mutual Insurance Company  
The Ohio Casualty Insurance Company  
West American Insurance Company

Certificate No: 8201331

**POWER OF ATTORNEY**

**KNOWN ALL PERSONS BY THESE PRESENTS:** That The Ohio Casualty Insurance Company is a corporation duly organized under the laws of the State of New Hampshire, that Liberty Mutual Insurance Company is a corporation duly organized under the laws of the State of Massachusetts, and West American Insurance Company is a corporation duly organized under the laws of the State of Indiana (herein collectively called the "Companies"), pursuant to and by authority herein set forth, does hereby name, constitute and appoint, Erin M. Margolis all of the city of Washington, state of District of Columbia, each individually if there be more than one named, its true and lawful attorney-in-fact, with full power and authority hereby conferred to sign, execute and acknowledge the above-referenced surety bond.

**IN WITNESS WHEREOF,** this Power of Attorney has been subscribed by an authorized officer or official of the Companies and the corporate seals of the Companies have been affixed thereto this 30th day of May, 2019.

Liberty Mutual Insurance Company  
The Ohio Casualty Insurance Company  
West American Insurance Company

By: David M. Carey  
David M. Carey, Assistant Secretary



STATE OF PENNSYLVANIA ss  
COUNTY OF MONTGOMERY

On this 30th day of May, 2019, before me personally appeared David M. Carey, who acknowledged himself to be the Assistant Secretary of Liberty Mutual Insurance Company, The Ohio Casualty Company, and West American Insurance Company, and that he, as such, being authorized so to do, execute the foregoing instrument for the purposes therein contained by signing on behalf of the corporations by himself as a duly authorized officer.

**IN WITNESS WHEREOF,** I have hereunto subscribed my name and affixed my notarial seal at King of Prussia, Pennsylvania, on the day and year first above written.



COMMONWEALTH OF PENNSYLVANIA  
Notarial Seal  
Teresa Pastella, Notary Public  
Upper Merion Twp., Montgomery County  
My Commission Expires March 28, 2021  
Member, Pennsylvania Association of Notaries

By: Teresa Pastella  
Teresa Pastella, Notary Public

This Power of Attorney is made and executed pursuant to and by authority of the following By-laws and Authorizations of The Ohio Casualty Insurance Company, Liberty Mutual Insurance Company, and West American Insurance Company which resolutions are now in full force and effect reading as follows:

**ARTICLE IV - OFFICERS:** Section 12. Power of Attorney.  
Any officer or other official of the Corporation authorized for that purpose in writing by the Chairman or the President, and subject to such limitation as the Chairman or the President may prescribe, shall appoint such attorneys-in-fact, as may be necessary to act in behalf of the Corporation to make, execute, seal, acknowledge and deliver as surety any and all undertakings, bonds, recognizances and other surety obligations. Such attorneys-in-fact, subject to the limitations set forth in their respective powers of attorney, shall have full power to bind the Corporation by their signature and execution of any such instruments and to attach thereto the seal of the Corporation. When so executed, such instruments shall be as binding as if signed by the President and attested to by the Secretary. Any power or authority granted to any representative or attorney-in-fact under the provisions of this article may be revoked at any time by the Board, the Chairman, the President or by the officer or officers granting such power or authority.

**ARTICLE XIII - Execution of Contracts:** Section 5. Surety Bonds and Undertakings.  
Any officer of the Company authorized for that purpose in writing by the chairman or the president, and subject to such limitations as the chairman or the president may prescribe, shall appoint such attorneys-in-fact, as may be necessary to act in behalf of the Company to make, execute, seal, acknowledge and deliver as surety any and all undertakings, bonds, recognizances and other surety obligations. Such attorneys-in-fact, subject to the limitations set forth in their respective powers of attorney, shall have full power to bind the Company by their signature and execution of any such instruments and to attach thereto the seal of the Company. When so executed such instruments shall be as binding as if signed by the president and attested by the secretary.

**Certificate of Designation** - The President of the Company, acting pursuant to the Bylaws of the Company, authorizes David M. Carey, Assistant Secretary to appoint such attorneys-in-fact as may be necessary to act on behalf of the Company to make, execute, seal, acknowledge and deliver as surety any and all undertakings, bonds, recognizances and other surety obligations.

**Authorization** - By unanimous consent of the Company's Board of Directors, the Company consents that facsimile or mechanically reproduced signature of any assistant secretary of the Company, wherever appearing upon a certified copy of any power of attorney issued by the Company in connection with surety bonds, shall be valid and binding upon the Company with the same force and effect as though manually affixed.

I, Renee C. Llewellyn, the undersigned, Assistant Secretary, of Liberty Mutual Insurance Company, The Ohio Casualty Insurance Company, and West American Insurance Company do hereby certify that this power of attorney executed by said Companies is in full force and effect and has not been revoked.

**IN TESTIMONY WHEREOF,** I have hereunto set my hand and affixed the seals of said Companies this 5th day of November, 2020.



By: Renee C. Llewellyn  
Renee C. Llewellyn, Assistant Secretary

Not valid for mortgage, note, loan, letter of credit, currency rate, interest rate or residual value guarantees.

To confirm the validity of this Power of Attorney call 1-610-832-8240 between 9:00am and 4:30pm EST on any business day.

Marsh MSurety POA LMIC OCIC WAIC Multi Co\_042019





LIBERTY MUTUAL INSURANCE COMPANY  
FINANCIAL STATEMENT — DECEMBER 31, 2019

<b>Assets</b>		<b>Liabilities</b>	
Cash and Bank Deposits.....	\$778,754,989	Unearned Premiums.....	\$8,007,146,482
*Bonds — U.S Government.....	2,780,808,610	Reserve for Claims and Claims Expense.....	21,532,853,787
*Other Bonds.....	12,645,608,792	Funds Held Under Reinsurance Treaties.....	507,868,920
*Stocks.....	16,385,435,431	Reserve for Dividends to Policyholders.....	1,143,826
Real Estate.....	235,608,378	Additional Statutory Reserve.....	125,722,000
Agents' Balances or Uncollected Premiums.....	6,217,983,641	Reserve for Commissions, Taxes and	
Accrued Interest and Rents.....	102,273,390	Other Liabilities.....	4,117,460,075
Other Admitted Assets.....	11,957,106,292	<b>Total.....</b>	<b>\$34,292,195,090</b>
		Special Surplus Funds.....	\$32,768,443
		Capital Stock.....	10,000,075
		Paid in Surplus.....	10,044,978,933
		Unassigned Surplus.....	6,723,636,983
<b>Total Admitted Assets.....</b>	<b><u>\$51,103,579,523</u></b>	<b>Surplus to Policyholders.....</b>	<b>16,811,384,434</b>
		<b>Total Liabilities and Surplus.....</b>	<b><u>\$51,103,579,524</u></b>



\* Bonds are stated at amortized or investment value; Stocks at Association Market Values.  
The foregoing financial information is taken from Liberty Mutual Insurance Company's financial statement filed with the state of Massachusetts Department of Insurance.

I, TIM MIKOLAJEWSKI, Assistant Secretary of Liberty Mutual Insurance Company, do hereby certify that the foregoing is a true, and correct statement of the Assets and Liabilities of said Corporation, as of December 31, 2019, to the best of my knowledge and belief.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the seal of said Corporation at Seattle, Washington, this 27<sup>th</sup> day of March, 2020.

*T. Mikolajewski*

Assistant Secretary



Office of the Secretary  
 4050 Esplanade Way  
 Tallahassee, FL 32399-0950  
 850-488-2786

**Ron DeSantis, Governor**

**Attachment C  
 Final Service Level Agreements (SLAs)**

Service Category	SLA Number	Deliverable Title	Performance Metric	Financial Consequence  All calendar days, unless otherwise stated	Additional SLA Clock Information
<b>Financial Consequences are capped at 4% of the annual revenue. This cap shall exclude all Project Management SLAs (i.e., SLA-D1 through D9).</b>					
Contractor Staffing	SLA-A1	Staffing Positions	a) Key staff positions will be filled within sixty (60) days from Contract execution, in accordance with SOW subsection 2.1  b) Key staff positions will be filled within one hundred and twenty (120) days of vacancy or within the timeframe established by the Department after a waiver of the one hundred and twenty (120) day requirement, in accordance with SOW subsection 2.1	a) \$250 per day, per vacancy b) \$250 per day, per vacancy c) \$250 per day, per incident	a) Should DMS invoke the right to review candidates for key staff positions, the SLA clock will be suspended during the DMS review.  b) Should DMS invoke the right to review candidates for key staff positions, the SLA clock will be suspended during the DMS review.

			c) DMS must receive a notification of a vacancy of a key staff position within fourteen (14) days of the vacancy, in accordance with SOW subsection 2.1		c) N/A
	SLA-A2	Final Staffing Organizational Chart	The final Staffing Organizational Chart shall be submitted to the Department no later than thirty (30) days from Contract execution, in accordance with SOW subsection 2.1	\$250 per day	The clock stops when an acceptable final Staffing Organizational Chart is provided to DMS. The SLA clock is on hold while DMS reviews.
Services and Devices for Mobile Communication Services	SLA-B1	Network-to-Network Interconnection Failover	Failover successfully accomplished within 500 seconds, in accordance with SOW subsection 3.6	5% of the affected end users' monthly recurring costs (MRC)	<p>The SLA is measured by the Contractor's equipment or system logs.</p> <p>The SLA clock starts when the logs indicate the loss of interconnectivity.</p> <p>The SLA clock stops when the interconnection with MFN operates without any loss of performance compared to the interconnection performance prior to failover.</p> <p>In the event there is an IP connectivity failure</p>

					<p>caused by the Contractor's primary IPsec VPN appliance, the Contractor's network shall failover to their secondary IPsec VPN appliance to maintain connectivity to MFN. The failover in any case shall be accomplished within five-hundred (500) seconds. The failover shall be governed by the BGP routing protocol operating between the MFN and Contractor devices or other as agreed upon by DMS.</p> <p>The financial consequence shall be charged to the Contractor if their primary and secondary VPN appliances fail simultaneously or other Contractor network event which causes a total outage or the VPN appliance failover does not occur in the specified time. The Contractor shall be exempt from this SLA</p>
--	--	--	--	--	---

					if the MFN primary and secondary VPN appliances fail simultaneously.
	SLA-B2	Network-to-Network Interconnection Performance Upgrade with MyFloridaNet	Required capacity upgrade must be completed within sixty (60) days, in accordance with SOW subsection 3.6	\$2,000 per day	<p>The SLA clock starts when an upgrade is needed as shown and documented by the Contractor.</p> <p>The SLA clock is on hold during DMS verification of the upgrade.</p> <p>The SLA clock stops when the required capacity upgrade has been accepted by DMS.</p>
	SLA-B3	SLA Compliance Report	The report will be provided monthly, two (2) Business Days before the monthly operational meeting, in accordance with SOW subsection 3.18.5	\$250 per day	The clock stops when an acceptable SLA Compliance Report is provided to DMS.

					The SLA clock is on hold while DMS reviews.
	SLA-B4	Escalation Activity Report	The report will be provided monthly, two (2) Business Days before the monthly operational meeting, in accordance with SOW subsection 3.19.1	\$250 per day	The clock stops when an acceptable Escalation Activity Report is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-B5	Zero Usage Report	The report will be provided quarterly and provided two (2) Business Days before the January, April, July, and October monthly operational meeting, in accordance with SOW subsection 3.19.2	\$250 per day	The clock stops when an acceptable Zero Usage Report is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-B6	Escalation Procedure Development and Updates	Developed within thirty (30) days of Contract execution, in accordance with SOW subsection 3.19.3 and section 4.  Updated within three (3) Business Days of email notification from DMS.	\$250 per day until developed or until updated	The clock stops when an acceptable Escalation Procedure Development and Updates are provided to DMS.  The SLA clock is on hold while DMS reviews.

	SLA-B7	Notification, Planned Maintenance	Notification of any planned maintenance must be received twenty-four (24) hours prior to any planned maintenance, in accordance with SOW subsection 3.19.4 and section 4.	\$250 per failure to timely notify	<p>The SLA is measured by the Contractor's logs and emails.</p> <p>The SLA applies automatically twenty-four (24) hours prior to any planned maintenance for which notice is not provided.</p>
	SLA-B8	Notification, Emergency Maintenance	<p>Notification received at least thirty (30) minutes prior to the emergency maintenance, in accordance with SOW subsection 3.19.4 and section 4</p> <p>The Contractor shall send a notification to DMS communicating the wireless services is not available in a generalized area, specific to switch locations, within Florida which includes an estimated time for service restoration (if available) within five (5) hours (maximum) from the outage start time. The SLA shall be measured and verified by the Contractor's system.</p>	\$250 per failure to timely notify	<p>The SLA is measured by the Contractor's logs and emails.</p> <p>The SLA automatically applies thirty (30) minutes prior to any emergency maintenance for which notice is not provided.</p>

	SLA-B9	Notification, Unplanned Outage	Notification received within sixty (60) minutes after the discovery of unplanned outage impact, in accordance with SOW subsection 3.19.4 and section 4. The Contractor shall send within sixty (60) minutes (minimum) an electronic notification which informs DMS of an unplanned outage which includes the date, time, and estimated duration of the maintenance. The SLA shall be measured and verified by the Contractor's system.	\$250 per failure to timely notify	<p>The SLA is measured by the Contractor's logs and emails.</p> <p>The SLA automatically applies sixty (60) minutes after discovery of unplanned outage impact for which notice is not provided.</p>
--	--------	--------------------------------	--	------------------------------------	--

	SLA-B10	Migration of Existing MCS Customers	Customer migration will be completed for State agencies within one-hundred and twenty (120) days of completion of the Services Infrastructure Checklist, and will be completed for current MCS OEU Customers within one-hundred and eighty (180) days of completion of the Services Infrastructure Checklist in accordance with SOW subsection 3.23	\$3.00 per day, and per wireless data/voice device, until completed	The SLA clock stops for incumbent Contractors when all State agency End-users are identified as either migrated or no longer receiving services from the Contractor.
Contractor Meetings with DMS	SLA-C1	Project Management Monthly Review Meeting	A Project Management Monthly Review Meeting must be conducted within fifteen (15) days upon Contract execution and monthly thereafter, in accordance with SOW subsection 3.25.3.	\$250 per day	The SLA clock is on hold if the Department requests the meeting be delayed or cancelled.
	SLA-C2	Project Implementation Phase - Project Kickoff Meeting	A Project Kickoff Meeting must be conducted within thirty (30) days upon Contract execution, in accordance with SOW subsection 3.25.4.	\$250 per day	The SLA clock is on hold if the Department requests the meeting be delayed or cancelled.

	SLA-D1	Project Management Plan	A Project Management Plan is due within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.1.2	\$250 per day	The clock stops when an acceptable Project Management Plan is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-D2	Disaster Recovery Plan	A Disaster Recovery Plan is due within three (3) months of Contract execution, in accordance with SOW subsection 3.26.1.7	\$500 per day	The clock stops when an acceptable Disaster Recovery Plan is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-D3	Project Status Reports	Project Status Reports must be submitted within two (2) weeks after the Project Kickoff Meeting and every two (2) weeks thereafter, in accordance with SOW subsection 3.26.2.3	\$250 per day	The clock stops when an acceptable Project Status Report is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-D4	Guides	Guides must be provided within three (3) months of Contract execution and within one (1) week, or as otherwise specified by DMS, upon requested updates, in accordance with SOW subsection 3.26.3	\$250 per day	The clock stops when acceptable Guides is provided to DMS.  The SLA clock is on hold while DMS reviews.

	SLA-D5	Project Closure Documentation	Project Closure Documentation must be provided within one (1) month from the close of the Project Implementation Phase, in accordance with SOW subsection 3.26.4	\$250 per day	The clock stops when acceptable Project Closure Documentation is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-D6	Implementation Plan	A Project Implementation Plan must be provided within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.5.1	\$1,000 per day	The clock stops when an acceptable Implementation Plan is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-D7	Incumbent Contractor Weekly Migration Report	An Incumbent Contractor Weekly Migration Report is due each week during implementation, in accordance with SOW subsection 3.26.5.1.b	\$1,000 per day	The clock stops when an acceptable Incumbent Contractor Weekly Migration Report is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-D8	Individual Customer Specific Migration Plans	Individual Customer-Specific Migration Plans must be provided within four (4) weeks of written notification of the requirement, in accordance with SOW subsection 3.26.5.2	\$250 per day	The clock stops when an acceptable Individual Customer Specific Migration Plans is provided to DMS.  The SLA clock is on hold while DMS reviews.

	SLA-D9	Services Infrastructure Checklist	The Services Infrastructure Checklist must have all items completed and be accepted by the Department and the Contractor within the timeline agreed to in writing in the Implementation and Migration Plan, in accordance with SOW subsection 3.27	\$5,000 per day	The clock stops when the Services Infrastructure Checklist is complete.  The SLA clock is on hold while DMS reviews.
Public Safety	SLA-E1	Public Safety Service Plans and Devices Report	The Public Safety Service Plans and Devices Report will be provided monthly, two (2) Business Days before the Monthly Operational Meeting, in accordance with SOW section 4.7	\$250 per day	The clock stops when an acceptable Public Safety Service Plans and Devices Report is provided to DMS.  The SLA clock is on hold while DMS reviews.
Business Operations	SLA-F1	Invoicing to DMS	Complete and accurate invoices to DMS must be submitted no later than the 10th calendar day of the month for services in arrears, in accordance with SOW subsection 5.10. This excludes Direct-Billed Accounts.	\$250 per day	The SLA clock stops when the timestamp for when the proper electronic billing file is submitted to the Department.

	SLA-F2	Application of Billing Credits	Apply each credit by the second available billing cycle after the credit has been determined, in accordance with SOW subsection 5.10 This excludes Direct-Billed Accounts.	\$750 per day	The SLA clock stops based upon the timestamp for when the complete and accurate electronic billing file is submitted to the Department.
Direct Ordering and Billing	SLA-G1	Cost Recovery Payment to DMS	An electronic Cost Recovery Payment will be provided within forty-five (45) days after the end of the calendar quarter to cover the fees collected for the previous quarter, in accordance with SOW subsection 6.2	\$750 per day	The SLA clock stops the date the check is deposited into the DMS account.
	SLA-G2	Direct-Billed Accounts Monthly Report	A Direct-Billed Accounts Monthly Report will be provided no later than the 30 <sup>th</sup> of the month on all direct-billed accounts, in accordance with SOW subsection 6.4	\$750 per day	The clock stops when an acceptable Direct-Billed Accounts Monthly Report is provided to DMS.  The SLA clock is on hold while DMS reviews.
	SLA-G3	Direct-Billed Accounts Quarterly Report	A Direct-Billed Accounts Quarterly Report will be provided no later than the 30 <sup>th</sup> of the month on all direct-billed accounts, in accordance with SOW subsection 6.5	\$750 per day	The clock stops when an acceptable Direct-Billed Accounts Quarterly Report is provided to DMS. The SLA clock is on hold while DMS reviews.

# Contract No.: DMS-19/20-006C

## Attachment D, Exhibit 1 – Vendor’s Services and Discount Pricing

### Definitions

**Access Discount:** Government Subscribers are eligible for a 23% access discount on qualified plans and features where noted.

**Accessory Discount.** Government Subscribers are eligible to receive a 25% discount from the retail price of qualifying accessories.

**Discount Eligible Data Feature(s):** Any generally available Verizon Wireless data feature with a monthly access fee of \$24.99 or higher, added to an Eligible Calling Plan, that does not prohibit discounts.

**Discount Eligible Plan(s):** Any generally available Verizon Wireless voice, data or M2M plan with a monthly access fee of \$34.99 or higher that does not prohibit discounts.

**Early Termination Fees (“ETF”):** ETFs are waived for Government Subscribers.

**Equipment:** Wireless telephones, data modems and similar devices and ancillary accessories used in conjunction with Wireless Service.

**Government Subscriber:** An employee of Customer utilizing Wireless Service whose account is set up in Customer’s name and for which Customer bears payment responsibility.

**Machine to Machine Service (“M2M Service”):** M2M refers to use of the Wireless Service for the transmission of data between wireless devices and computer servers or other machines, or between select wireless devices, with limited or no manual intervention or supervision.

**M2M Line(s):** An individual line of M2M Service used under this Pricing and Equipment Proposal which is set up in Customer’s name and for which Customer bears responsibility.

**Network Speeds on the Verizon Wireless Network (4G LTE): Uploads:** 2-5 Mbps and **Downloads:** 5-12 Mbps

**Plans, Features, Rates and Charges:** The voice, data or M2M plan and any options, features or applications that are selected by the Customer determine the applicable rates, charges, allowance of minutes or megabytes and Wireless Service coverage area for each line. Some plans may have restrictions on the type of Equipment that can be activated on them. Information about retail plans, options, features, and applications (*i.e.*, those that Verizon Wireless makes generally available to consumers or business customers) and their terms and conditions may be obtained at Verizon Wireless stores, on [verizonwireless.com](http://verizonwireless.com) or from Verizon Wireless business sales representatives. The voice, data or M2M plan monthly access fees and non-promotional allowance of minutes and/or megabytes for each line will not change during the Line Term as long as Customer does not change plans on that line. As detailed in the contract, rates, charges and fees, listed in Pricing Index may be changed following the formal Amendment process Verizon Wireless may discontinue any retail plans, options, features and applications for new activations without notice. If Customer changes or upgrades Equipment, Verizon Wireless may require it to change to a then-current plan that is compatible with the changed or upgraded Equipment. Customer may not activate Equipment purchase at a discount from Verizon Wireless on M2M Lines. Government discounts and pricing may not be available to purchases made through agents or at retail store locations.

**Subsidized Equipment:** Equipment purchased at Verizon Wireless government matrix and/or government promotional price. Subsidized Equipment must be active for 24 months or more before being eligible to be upgraded. In the event a Customer purchases a subsidized device and the Customer terminates services early, or moves to a lesser price plan or disconnects the devices from the Contractor’s network within twenty-four (24) months of the device activation, the Contractor may bill the Customer for the unpaid portion of the subsidized amount of the device.

**Term of Lines (“Line Term”):** The term for each line (the “Line Term”) begins on the date Wireless Service is activated for that line and continues for the period required by the calling plan or Equipment selected for that line (usually 2 years). Line Term extensions are required when Customer: (a) takes advantage of promotions or services that require a Line Term extension; or (b) purchases or upgrades Equipment except for ancillary accessories used in conjunction with Wireless Service. When the Line Term expires, Wireless Service

continues on a month-to-month basis. Activation fees are waived for Government Subscribers on voice and data plans and for M2M Lines.

**ThingSpace Mange:** ThingSpace Manage (“ThingSpace”) provides Customer with the ability to remotely monitor and manage its M2M/IoT devices. If Customer desires to access and use ThingSpace, it must so request in writing, and Verizon Wireless shall provision ThingSpace on Customer’s account. Applicable rates and charges, if any, shall be set forth in this Addendum. ThingSpace set-up time is estimated to take four to six weeks. The rights granted to Customer herein for access to and use of ThingSpace are specific to Customer and may not be transferred to another party without Verizon Wireless’ prior written consent. Verizon Wireless retains full and exclusive ownership of all intellectual property rights associated with the ThingSpace including any alterations, modifications, improvements and derivative works thereof.

**Legacy Pricing.** All custom plans and features excluding machine-to-machine plans existing under the Agreement prior to the Effective Date of the Agreement (“Legacy Plans”), shall be retired and will no longer be available for new line activations, lines changing plans or lines upgrading Equipment. Verizon Wireless will allow Customer’s existing Government Subscribers who are currently on such Legacy Plans to continue at the pricing, terms and conditions contained in such Legacy Plans until the Government Subscriber either changes plans or upgrades Equipment.

**Wireless Service:** Each and every radio service provided directly or indirectly by Verizon Wireless.

## STATE OF FLORIDA CUSTOM PER UNIT PLANS AND FEATURES

### Custom State of Florida Nationwide Voice Per Minute Calling Plan

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

200 Text/Picture/Video Message Option  
600 Mobile to Mobile Minutes (82587)

No Domestic Roaming or Long Distance Charges  
600 Night and Weekend Minutes (72711)

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Anytime Voice Allowance Minutes Per Month	Voice Per Minute Rate
(86680)	\$0.00	0	\$0.049

#### Optional Features

Text, Picture & Video Messaging	Per the applicable Custom State of Florida SMS/MMS Per Message Feature rate
Domestic Data Sent or Received	\$1.99 per MB or per Data Package
Unlimited Domestic Push To Talk Plus	\$10.00

**Notes:** 4G Basic handset devices Only. See attached Plan and Feature Details for important information about calling plans, features and options. 4G service requires 4G equipment and 4G coverage. Must request SMS and/or MMS option to receive 200 included Text/Picture/Video messages option. PTT Plus service requires; PTT Plus feature, PTT Plus enabled device, and PTT Plus coverage. Subscribers must supply their own authenticated Equipment (CPE) to be activated on these plans or may purchase equipment at full retail price. Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Coverage includes the Verizon Wireless 5G Nationwide® network, 4G network; and the 3G and 3G Extended networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international).

### Custom State of Florida Nationwide Machine to Machine (M2M)

#### Per Megabyte Calling Plan

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

Data for Telemetry (M2M) devices only

This plan may NOT be used for email

SOFL Plan Number	Machine to Machine (M2M) Monthly Access Charge Per Line	Domestic Megabytes (MB) Allowance Per Month	Data Per Megabyte Rate
86693	\$0.00	0	\$0.099

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Subscribers must supply their own authenticated Equipment (CPE) to be activated on these plans. Machine-to-machine coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international).

Current data coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com).

Only Customer-provided, 4G-capable machine-to-machine devices may be activated on this plan.

If the voice block feature is removed, subscribers will be charged \$0.049 per minute for voice calls.

## 4G Basic Phone Push to Talk Plus (PTT+) Only Plan: Government Subscribers Only

### Push to Talk Plus Only Plan

Monthly Access Charge	\$10.00
Domestic Anytime Voice Minutes Per Month	0
Push to Talk Plus	Unlimited
Domestic Voice Per Minute Rate	\$0.049
Data Sent or Received	\$1.99 per MB or per data package <sup>1</sup>

**Notes:** Current coverage details can be found at [www.verizonwireless.com](http://www.verizonwireless.com). No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Data usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international).

Push to Talk Plus is only available in the United States. This price plan can only be used with a 3G Basic or 4G Basic PTT+ capable device.

See attached Calling Plan and Feature Details for important information about calling plans, features and options. If the voice block feature is removed, subscribers will be charged \$0.049 per minute for non-Push to Talk Plus voice calls. (94976)

## 4G Smartphone Phone Push to Talk Plus (PTT+) Only Feature: Government Subscribers Only

### Push to Talk Plus Only Feature

Monthly Access Charge	\$10.00
Domestic Anytime Voice Minutes Per Month	0
Push to Talk Plus	Unlimited
Domestic Voice Per Minute Rate	per voice/data plan
Data Sent or Received	per data package <sup>1</sup>

**Notes:** Current coverage details can be found at [www.verizonwireless.com](http://www.verizonwireless.com). No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Data usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international).

Push to Talk Plus is only available in the United States. This price plan can only be used with a 3G Basic or 4G Basic PTT+ capable device.

See attached Calling Plan and Feature Details for important information about calling plans, features and options.

**State of Florida Nationwide Voice Calling Share Plans: Basic Phones Only  
Government Subscribers Only**

**The calling plans below reflect the monthly access charge discount. No additional discounts apply.**

<b>Monthly Access Charge (shared minutes)</b>	<b>\$14.99</b>	<b>\$29.99</b>
<b>Shared* Domestic Anytime Voice Minutes Per Month</b>	<b>200</b>	<b>500</b>
<b>Overage Rate per minute</b>	\$0.06	
<b>Domestic Night &amp; Weekend Minutes</b>	Unlimited	
<b>Domestic Mobile to Mobile Minutes</b>	Unlimited	
<b>Domestic Long Distance</b>	Included	
<b>Domestic Data (data can be blocked)</b>	\$1.99 per MB or per data package 4G data blocked. Data package must be selected.	

**OPTIONAL FEATURES**

<b>500 Domestic Text, Picture &amp; Video Messages</b>	\$0.00 SMS: \$0.10 outbound/\$0.02 inbound/overage MMS: \$0.25 per Picture or Video Message/overage
<b>Unlimited Domestic Push-to-Talk Plus (PTT+)</b>	\$2.00 (device dependent)
<b>Unlimited Domestic Picture &amp; Video Messages (SMS/MMS)</b>	\$10.00

**Notes:** Coverage area includes the Verizon Wireless 4G network; and the 3G and Extended partner networks, while available. Coverage includes the Verizon Wireless 5G Nationwide® network, 4G network; and the 3G and 3G Extended networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international). See attached Calling Plan and Feature Details for important information about calling plans, features and options.

\*Voice minutes can share with Nationwide voice and/or voice & data bundle plans that are eligible for sharing. Voice block may be added to these plans to accommodate PTT+ only.

**Profile Share- Voice Sharing:** At the end of each bill cycle, any unused voice allowances for lines sharing across multiple accounts will be applied proportionally to all lines with overages.

**State of Florida Nationwide Voice Calling Share Plans: Smartphones Only  
Government Subscribers Only**

**The calling plans below reflect the monthly access charge discount. No additional discounts apply.**

<b>Monthly Access Charge (shared minutes)</b>	<b>\$14.99</b>	<b>\$29.99</b>
<b>Shared* Domestic Anytime Voice Minutes Per Month</b>	<b>200</b>	<b>500</b>
<b>Overage Rate per minute</b>	\$0.06	
<b>Domestic Night &amp; Weekend Minutes</b>	Unlimited	
<b>Domestic Mobile to Mobile Minutes</b>	Unlimited	
<b>Unlimited Domestic Picture &amp; Video Messages (SMS/MMS)</b>	Included	
<b>Domestic Long Distance</b>	Included	
<b>Domestic Data</b>	Data package must be selected.	

**OPTIONAL FEATURE**

<b>Unlimited Domestic Push-to-Talk Plus (PTT+)</b>	\$2.00 (device dependent)	
--	---------------------------	--

**Notes:** Coverage area includes the Verizon Wireless 4G network; and the 3G and Extended partner networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international). Lines activating on this plan must be on 5G Nationwide or 4G HD voice-capable smartphones, except that existing lines on 3G smartphones may change to this plan while 3G service is available. See attached Calling Plan and Feature Details for important information about calling plans, features and options.

\*Voice minutes can share with Nationwide voice and/or voice & data bundle plans that are eligible for sharing. Voice block may be added to these plans to accommodate PTT+ only.

**Profile Share- Voice Sharing:** At the end of each bill cycle, any unused voice allowances for lines sharing across multiple accounts will be applied proportionally to all lines with overages.

## WIRELESS VOICE

### Custom State of Florida Nationwide Voice Calling Plans

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Unlimited National Mobile to Mobile Calling Minutes No Domestic Roaming or Long Distance Charges		Unlimited Night & Weekend Minutes		
SOFL Plan Number	Domestic Anytime Allowance Minutes*	Conventional and Smartphone Devices Monthly Access Charge	Overage Rate	Voice Roaming (Canada and Mexico)
(86195)	250	\$25.75	\$0.052	\$0.69
(86196)	600	\$36.05	\$0.052	\$0.69
Data Sent or Received		\$1.99 per MB or per Data Package		
Optional Feature				
Domestic Push-to-Talk Plus		\$0.00		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Coverage includes the Verizon Wireless 5G Nationwide® network, 4G network; and the 3G and 3G Extended networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international). Lines activating on this plan must be on 5G Nationwide or 4G HD voice-capable smartphones, except that existing lines on 3G smartphones may change to this plan while 3G service is available. \*Overage Rate applies after allowance. 4G Smartphones and 3G/4G Multimedia Phones require a data package. 4G service requires 4G equipment and 4G coverage. PTT Plus service requires PTT Plus enabled device and coverage.

**WIRELESS DATA****Custom State of Florida Mobile Broadband Data Plans\***

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Overage Rate	Unlimited Domestic SMS and MMS Messaging
86226	\$20.60	500MB	\$0.00849per MB	Included
86227	\$25.75	1,000MB		
86229	\$36.05	Unlimited*		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Overage Rate applies after allowance. Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Coverage includes the Verizon Wireless 5G Nationwide® network, 4G network; and the 3G and 3G Extended networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international). Lines activating on these plans must be on 5G Nationwide or 4G mobile broadband devices, except that existing lines on 3G mobile broadband devices may change to these plans while 3G service is available. \*Verizon Wireless will limit the data throughput speeds should 25 GB of data usage be reached in any given billing cycle on any line. Data throughput speeds for additional usage will be limited for the remainder of the then-current bill cycle for the line(s) that exceed the 25 GB high-speed data usage threshold. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB with prior written notice. Can be added to voice plans with a monthly access fee of \$14.99 and above. \*Router devices cannot be activated on these plans.

**Custom State of Florida Smartphone Data Feature Packages**

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

**Data for Smartphone devices only**

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Overage Rate	Unlimited Domestic SMS and MMS messaging
77294/ 79789	\$15.45	500MB	\$0.00849 per MB	Included*
(77295 and 79790)	\$20.60	1,000MB		
Exhibit (79740 79791)	\$23.69	2,000MB		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Overage Rate applies after allowance. Current coverage details and additional feature information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Coverage includes the Verizon Wireless 5G Nationwide® network, 4G network; and the 3G and 3G Extended networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. This feature can only be added onto: SOFL PPlan's 86192-86197. Lines activating on this feature must be on 5G Nationwide or 4G HD voice-capable smartphones. 4G service requires 4G equipment and 4G coverage. \*Not included with the State of Florida Nationwide Custom Pooled Voice Services Plans. May only be added to a voice plan with a monthly access fee of \$14.99 and above.

### Custom State of Florida Smartphone Unlimited Data Feature Package

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

#### Data for Smartphone devices only

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Overage Rate	Unlimited Domestic SMS and MMS messaging with Mobile Hotspot
(79407-4G), (79781-4G)	\$32.96	Unlimited*	N/A	Included**

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Overage Rate applies after allowance. 4G service requires 4G equipment and 4G coverage. Current coverage details and additional feature information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Coverage includes the Verizon Wireless 5G Nationwide® network, 4G network; and the 3G and 3G Extended networks, while available. For avoidance of doubt, Verizon's 5G Nationwide® network is a separate network from Verizon's 5G Ultra Wideband network. This feature can only be added onto: SOFL PPlan's 86192-86197. Lines activating on this feature must be on 5G Nationwide or 4G HD voice-capable smartphones. \*Verizon Wireless will limit the data throughput speeds should 25 GB of data usage be reached in any given billing cycle on any line. Data throughput speeds for additional usage will be limited for the remainder of the then-current bill cycle for the line(s) that exceed the 25 GB high-speed data usage threshold. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB with prior written notice \*\*Not available when bundled with the State of Florida Nationwide Custom Pooled Voice Services Plans. May only be added to a voice plan with a monthly access fee of \$14.99 and above.

### Custom State of Florida 4G Mobile Broadband Data Share Plans for Tablets

#### Government Subscribers Only

These plans are Not eligible for monthly access discounts.

Monthly Access Fee	\$10.00 (99775)	\$18.00 (31781)	\$22.00 (36656)	\$35.00 (36659)	\$50.00 (36660)
Domestic Shared Data Allowance	250 MB	1 GB	2 GB	5 GB	10 GB
Data Overage Rate	\$9.97 per GB				

**Notes:** Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Lines activating on these plans must be on 4G tablets except that existing lines on 3G tablets may change to these plans while 3G service is available.

**Data Sharing (Domestic Only): Account Share.** At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need.

## Custom State of Florida Unlimited Mobile Broadband Data Plans

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Overage Rate
86229	\$36.05	Unlimited*	N/A

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. 4G service requires 4G equipment and 4G coverage. \*Verizon Wireless will limit the data throughput speeds should 25 GB of data usage be reached in any given billing cycle on any line. Data throughput speeds for additional usage will be limited for the remainder of the then-current bill cycle for the line(s) that exceed the 25 GB high-speed data usage threshold. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB with prior written notice. Routers cannot be activated on this plan.

## Public Sector Mobile Broadband Share Plans: Government Subscribers Only

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Public Sector Mobile Broadband	5 Gigabytes	10 Gigabytes	20 Gigabytes
Monthly Access Charge	\$34.99 (90237)	\$59.99 (90240)	\$99.99 (90241)
Shared Domestic Data Allowance	5GB	10GB	20GB
Overage Per Gigabyte	\$8.00 Per Gigabyte		

**Note:** This plan is available for domestic data only devices, on the Verizon Wireless network only.

**Data Sharing:** At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need. Plan changes may not take effect until the billing cycle following the change request. New activations on these service plans require 4G LTE devices. The 5GB, 10GB, and 20GB Public Sector Mobile Broadband Plans are able to share with each other.

## Flexible Business Plans For Basic & Smartphones

The calling plans below reflect the monthly access fee discount. No additional discounts apply.

	Basic Phones*		Smartphones <sup>1</sup>			
Monthly Access Fee	\$35.00 (92731)	\$65.00 (92732)	\$75.00 (92736)	\$85.00 (92737)	\$95.00 (92738)	\$105.00 (92740)
Monthly Access Fee less discount	\$26.95	\$50.05	\$57.75	\$65.45	\$73.15	\$80.85
Shared Data Allowance	100 MB	2 GB	4 GB	6 GB	8 GB	10 GB
Data Overage	\$10.00 per GB					
Mobile Hotspot <sup>2</sup>	Included					
Monthly Anytime Minutes	Unlimited					
Messaging Allowance <sup>3</sup>	Unlimited Domestic and International Messaging					
<b>Optional Features</b>						
Domestic Push to Talk Plus	Additional monthly access fee per line \$5.00 per line					

**Notes:** Current coverage details and additional plan and feature information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). No Domestic Roaming or Long Distance Charges. 4G service requires 4G Equipment and 4G coverage. Government subscribers only.

\* Basic phones may only be added to an account with at least 1 Smartphone (bill account level).

1. Access to corporate email using BlackBerry Enterprise Server (BES) is available for an additional \$15.00 per line.
2. Mobile Hotspot is available on all capable devices and allows you to use your device and share data allowance with multiple Wi-Fi enabled devices.
3. Unlimited Messaging from within the United States to anywhere in the world where messaging services are available.

**Data Sharing:** Lines activated on these plans can only share with other lines on these plans and with lines on the Flexible Business Plans for Data Devices. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need. Plan changes may not take effect until the billing cycle following the change request.

### Flexible Business Plans For Data Devices

The calling plans below reflect the monthly access fee discount. No additional discounts apply.

	Connected Devices	Connected Devices, Tablets, Netbooks, Notebooks	Connected Devices, Tablets, Netbooks, Notebooks, Jetpacks, USBs, Mobile Broadband Devices				
Monthly Access Fee	\$5.00 (92739)	\$10.00 (92741)	\$35.00 (92742)	\$45.00 (92744)	\$55.00 (92745)	\$65.00 (92746)	\$75.00 (92747)
Monthly Access Fee less discount	\$5.00	\$10.00	\$26.95	\$34.65	\$42.35	\$50.05	\$57.75
Shared Data Allowance	1 MB	100 MB	2 GB	4 GB	6 GB	8 GB	10 GB
Data Overage Rate	\$10.00 per GB						

**Notes:** Current coverage details and additional plan and feature information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). 4G service requires 4G Equipment and 4G coverage. Government subscribers only.

**Data Sharing:** These plans only share with other lines on these plans and with lines on the Flexible Business Plans for Basic & Smartphones. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need. Plan changes may not take effect until the billing cycle following the change request.

### Flexible Business Plans For Data Devices - Connected Device / Internet with Voice

The calling plans below reflect the monthly access fee discount. No additional discounts apply.

	Connected Device*	Broadband Router				
Monthly Access Fee	\$5.00 (94532)	\$65.00 (94495)	\$75.00 (94496)	\$85.00 (94497)	\$95.00 (94500)	\$105.00 (94504)
Monthly Access Fee less discount	\$5.00	\$50.05	\$57.75	\$65.45	\$73.15	\$80.85
Shared Data Allowance	1 MB	2 GB	4 GB	6 GB	8 GB	10 GB
Domestic Data Overage Rate	\$10.00 per GB					

**Notes:** Current coverage details and additional plan and feature information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). 4G service requires 4G Equipment and 4G coverage. Government subscribers only.

**Data Sharing:** These plans only share with other lines on these plans and with lines on the Flexible Business Plans for Basic & Smartphones. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need. Plan changes may not take effect until the billing cycle following the change request.

### Flexible Business Plans For Data Devices - Connected Device / Internet with Voice

The calling plans below reflect the monthly access fee discount. No additional discounts apply.

	Connected Device*	Broadband Router				
Monthly Access Fee	\$5.00 (94532)	\$65.00 (94495)	\$75.00 (94496)	\$85.00 (94497)	\$95.00 (94500)	\$105.00 (94504)
Monthly Access Fee less discount	\$5.00	\$50.05	\$57.75	\$65.45	\$73.15	\$80.85
Shared Data Allowance	1 MB	2 GB	4 GB	6 GB	8 GB	10 GB
Domestic Data Overage Rate	\$10.00 per GB					

**Notes:** Current coverage details and additional plan and feature information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). 4G service requires 4G Equipment and 4G coverage. Government subscribers only.

**Data Sharing:** These plans only share with other lines on these plans and with lines on the Flexible Business Plans for Basic & Smartphones. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need. Plan changes may not take effect until the billing cycle following the change request.

### Custom State of Florida Nationwide Wireless Smartphone Data Plan with Mobile Hot Spot

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Data for Smartphone devices only

Monthly Access Charge Per Line	Domestic Data Allowance with Mobile Hot Spot (MHS)	Nationwide Calling Rate	Unlimited Domestic Mobile to Mobile, Nights and Weekends, and SMS and MMS Messaging
\$35.99 (93445)	Unlimited*	\$0.052 per minute	Included

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. 4G service requires 4G equipment and 4G coverage. \*Verizon Wireless will limit the data throughput speeds should 25 GB of data usage be reached in any given billing cycle on any line. Data throughput speeds for additional usage will be limited for the remainder of the then-current bill cycle for the line(s) that exceed the 25 GB high-speed data usage threshold. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB with prior written notice

### Mobile Broadband Machine to Machine (M2M) Share Group 1 Plans - Low Usage

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Mobile Broadband Machine-to-Machine Plans	1 Megabyte	5 Megabytes	25 Megabytes	50 Megabytes	150 Megabytes
<b>Domestic Shared Data Allowance Per Month</b>	<b>1 MB (87640)</b>	<b>5 MB (87641)</b>	<b>25 MB (87642)</b>	<b>50 MB (87643)</b>	<b>150MB (87644)</b>
Monthly Access Charge	\$5.00	\$7.00	\$10.00	\$15.00	\$18.00
Overage Rate Per Megabyte	\$1.00				

### Mobile Broadband Machine to Machine (M2M) Share Group 2 Plans - High Usage

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Mobile Broadband Machine-to-Machine Plans	250 Megabytes	1 Gigabyte	5 Gigabytes	10 Gigabytes
<b>Domestic Data Allowance Per Month</b>	<b>250 MB (87645)</b>	<b>1 GB (87646)</b>	<b>5 GB (87647)</b>	<b>10 GB (87648)</b>
Monthly Access Charge	\$20.00	\$25.00	\$38.50	\$61.60
Overage Rate Per Megabyte	\$0.015			

Note: Machine to Machine coverage included the Verizon Wireless 4G, 3G and 3G Extended networks. See attached Calling Plan and Feature Details for important information about calling plans, features and options. Government Subscribers may supply their own authenticated Equipment (CPE) approved by Verizon Wireless to be activated on these plans. Netbook, Smartphone, and Tablet devices are not eligible for Mobile Broadband M2M pricing. 4G service requires 4G Telemetry equipment and 4G coverage. All terms and conditions of the Agreement apply to M2M service and M2M Lines as a Wireless Service. Customer may select either the Account Share or Profile Share option on the Mobile broadband Machine-to-Machine (M2M) Share Plans.

### Machine to Machine Wireless Backup Router Plan

This Plan is NOT eligible for Monthly Access Fee Discounts.

Monthly Access	Data Allowance	Overage Rate
\$10.00 (86848-4G)	25 MB	\$10.00 per GB

**Note:** This plan is restricted to Verizon Wireless network use only; domestic and international roaming not available.. 4G service requires 4G equipment and 4G coverage. Customer must maintain a minimum of five (5) active M2M Lines to be eligible for this plan. Customer must provide its own Equipment, approved for use on the Verizon Wireless network, when activating service on this plan. Not all wireless routers can be provisioned on this plan.

This plan is approved for use as a backup solution for business continuity only and may not be used for primary connectivity. Verizon Wireless reserves the right to migrate lines on this plan to the standard 5 GB M2M Plan if usage on a line provisioned on this plan exceeds one GB for three consecutive bill cycles.

### Public Sector Mobile Broadband Machine to Machine (M2M) Share Plans:

Government Subscribers Only

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Public Sector Mobile Broadband	5 Gigabytes	10 Gigabytes	20 Gigabytes
Monthly Access Charge	\$34.99 (90231)	\$59.99 (90234)	\$99.99 (90235)
Shared Domestic Data Allowance	5GB	10GB	20GB
Overage Per Gigabyte	\$8.00 Per Gigabyte		

**Note:** This plan is available for domestic data only devices, on the Verizon Wireless network only.

**Data Sharing:** At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account beginning with the line with the lowest overage need. Plan changes may not take effect until the billing cycle following the change request. New activations on these service plans require 4G LTE devices. Netbook, Smartphone, and Tablet devices are not eligible for Mobile Broadband M2M pricing. Existing customers transitioning to one of these service plans are able to utilize existing 3G devices. The 5GB, 10GB, and 20GB Public Sector Mobile Broadband Machine to Machine Plans are able to share with each other.

**Custom Flat Rate Mobile Broadband - Government**

Government Subscribers Only

This plan is not eligible for monthly access fee discounts.

<b>Monthly Access Fee</b>	<b>\$34.99</b>
<b>Domestic Data Allowance*</b>	Unlimited
<b>Overage Rate per KB</b>	NA

NOTE: Subject to the Mobile Broadband terms and conditions; additional terms and conditions apply to Unlimited, Megabyte (MB), and Smartphone data Plans. Throughput speeds on the Custom Flat Rate Mobile Broadband will be limited up to 600kbps throughout the duration of each billing cycle while on the Verizon Wireless 4G network only. Data speeds are not guaranteed while on Extended or roaming partner networks. Devices utilized in conjunction with the Custom Flat Rate Mobile Broadband plan are limited to mobile (non-stationary) applications. Dedicated internet connections on stationary router devices and streaming video on stationary video surveillance cameras are expressly prohibited on this rate plan.

**Custom Mobile Broadband Plan II – Government Government Subscribers Only**

This plan is not eligible for monthly access fee discounts.

<b>Monthly Access Fee</b>	<b>\$44.99</b>
<b>Domestic Data Allowance</b>	Unlimited
<b>Overage Rate Per KB</b>	NA

NOTE: Subject to the Mobile Broadband terms and conditions; additional terms and conditions apply to Unlimited, Megabyte (MB), and Smartphone data Plans. Verizon Wireless will limit throughput of data speeds should 30GB of data be used within a given bill cycle. Devices utilized in conjunction with the Custom Mobile Broadband Plan II are limited to mobile (non-stationary) applications. Data speeds are not guaranteed while on Extended or roaming partner networks. Dedicated internet connections on stationary router devices and streaming video on stationary video surveillance cameras are expressly prohibited on this rate plan.

**Custom 4G Verizon Unlimited Smartphone Plan for Public Sector**

Government Subscribers Only

The calling plan below reflects the monthly access fee discount. No additional discounts apply.

Only 4G LTE GSM/UMTS global-capable smartphones can be activated on this plan.

<b>Monthly Access Fee (Discount Applied)</b>	<b>\$50.05</b>
<b>Monthly Minutes in U.S</b>	Unlimited
<b>Domestic Data Allowance</b>	Unlimited <sup>1</sup>
<b>Domestic Mobile Hotspot</b>	Unlimited <sup>2</sup>
<b>Domestic and International Messaging Allowance</b>	Unlimited <sup>3</sup>

**Notes:** Current coverage details can be found at [www.verizonwireless.com](http://www.verizonwireless.com). No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available.

(1) In the event of network congestion, after 22GB of data usage on a line during any billing cycle, usage on such line may result in slightly slower download speeds relative to another user. To ensure users are able to maximize their high-speed data use for business applications, video applications will stream at 480p.

(2) Mobile Hotspot is available on all capable devices and allows Corporate Subscribers to use their device and share data allowance with multiple Wi-Fi enabled devices. If 10GB of Mobile Hotspot data usage is exceeded on any line in any given billing cycle, Verizon Wireless will limit the data throughput speeds for additional usage for the remainder of the then-current billing cycle for the line that exceeds the data usage.

(3) Unlimited Messaging from within the United States to anywhere in the world where messaging services are available. For other messaging rates go to [www.verizonwireless.com](http://www.verizonwireless.com). (13656)

The "Custom 4G Unlimited Smartphone Plan for Public Sector – State of Florida Government" is eligible to use Travel Pass SPO code 383.

**Custom Business 5G Ultra Wideband Bolt-On Feature****Government Subscribers Only****Not eligible for discounts.****Monthly Access Fee****\$10.00**

**Notes:** Coverage includes the Verizon Wireless 5G Ultra Wideband (UWB) network, where available. Current coverage details can be found at [www.verizonwireless.com/5G](http://www.verizonwireless.com/5G). This feature is only available to 5G UWB capable smartphones on Custom Unlimited Business Plan for Smartphones. (13656)

**4G Business TravelPass Feature<sup>1</sup>:****Custom 4G Verizon Unlimited Smartphone Plan for Public Sector****Government Subscribers Only Rates are not eligible for discounts.**

<b>Canada and Mexico Daily Rate<sup>2</sup></b>	<b>\$5.00 (SPO 383)</b>
<b>Rest of World Daily Rate<sup>2,3</sup></b>	<b>\$10.00/day</b>
<b>Non-Travel Pass Countries<sup>4</sup></b>	Pay As You Go Rates

Notes: <sup>1</sup>This feature requires a 4G LTE GSM/UMTS global-capable device. <sup>2</sup>The daily rate covers a 24-hour time period. <sup>3</sup>For eligible countries, <sup>4</sup>non-TravelPass country rates and additional information, see attached International services pricing for further details. For voice-capable devices, this feature may be added to plans that have an unlimited voice and messaging allowance and an unlimited or capped data allowance using the account share option. For data usage in Canada and Mexico and all Rest of World TravelPass countries, after the first 512 MB of usage in a day, throughput speeds for additional usage will be reduced for the remainder of the day. All data usage decrements from the domestic data allowance when added to a capped allowance plan. Verizon Wireless will terminate a line if more than half of the usage over three consecutive billing cycles is outside of the United States, following 30 days' notice to Customer. This feature can only be added to lines activated on the following plan Custom 4G Verizon Unlimited Smartphone Plan for Public Sector (13656) under this Agreement. This is a commercially available feature which is subject to availability and change.

## GLOBAL SERVICES

### International Options Monthly Features: Mexico and Canada

The calling features below reflect the monthly access fee discount. No additional discounts apply.

International Options Monthly Features: Mexico and Canada	0 Voice Minutes	0 Voice Minutes	100 Voice Minutes	250 Voice Minutes	500 Voice Minutes
Monthly Access Fee	\$10.00 (SPO 428)	\$20.00 (SPO 426)	\$15.00 (SPO 441)	\$30.00 (SPO 425)	\$25.00 (SPO 443)
Monthly Access Fee less discount	<b>\$10.00</b>	<b>\$20.00</b>	<b>\$15.00</b>	<b>\$22.50</b>	<b>\$18.75</b>
Voice Overage Rate	Pay Go		\$0.10/minute		\$0.05/minute
Data Allowance <sup>1</sup>	100 MB	250 MB	100 MB	250 MB	1 GB
Data Overage Rate After Allowance <sup>2</sup>	\$10.00/100 MB				\$20.00/1 GB
Messaging Allowance <sup>3</sup>	Pay Go		100 sent; unlimited incoming	250 sent; unlimited incoming	500 sent; unlimited incoming
Messaging Overage Rate After Allowance <sup>2</sup>	Pay Go		\$0.10/Sent Message		\$0.05/Sent Message

**Notes:** <sup>1</sup>The data allowance applies in Canada and Mexico only, where coverage is available. All data usage, including dedicated Mobile Hotspot, deducts from the same data allowance. Requires an eligible domestic data plan or feature and an International GSM capable device. <sup>2</sup>The overage rate is not eligible for discounts. <sup>3</sup>Multimedia messages (MMS) are included in the allowance, but incur data transport charges (deducts from the International data allowance). Pay Go rates for International Voice, International Messaging, and Data Roaming see attached International services pricing for further details..

**This is a monthly feature and will be removed from the account one month after being added to an account.**

### International Options Monthly Features : 140+ Countries

The calling features below reflect the monthly access fee discount. No additional discounts apply.

International Options Monthly Features: 140+ Countries	0 Voice Minutes	0 Voice Minutes	100 Voice Minutes	250 Voice Minutes
Monthly Access Fee	\$25.00 (SPO 431)	\$50.00 (SPO 433)	\$40.00 (SPO 445)	\$85.00 (SPO 423)
Monthly Access Fee less discount	<b>\$18.75</b>	<b>\$37.50</b>	<b>\$30.00</b>	<b>\$63.75</b>
Voice Overage Rate	Pay Go		\$0.25/minute	
Data Allowance <sup>1</sup>	100 MB	250 MB	100 MB	250 MB
Data Overage Rate After Allowance <sup>2</sup>	\$25.00/100 MB			
Messaging Allowance <sup>3</sup>	Pay Go		100 sent; unlimited incoming	250 sent; unlimited incoming
Messaging Overage Rate After Allowance <sup>2</sup>	Pay Go		\$0.25/Sent Message	

**Notes:** <sup>1</sup>The data allowance applies in 140+Countries, where coverage is available. All data usage, including dedicated Mobile Hotspot, deducts from the same data allowance. Requires an eligible domestic data plan or feature and an International GSM capable device. <sup>2</sup>The overage rate is not eligible for discounts. <sup>3</sup>Multimedia messages (MMS) are included in the allowance, but incur data transport charges (deducts from the International data allowance). Pay Go rates for International Voice, International Messaging, and Data Roaming see attached International services pricing for further details..

**This is a monthly feature and will be removed from the account one month after being added to an account.**

### International Options Monthly Recurring Features: Mexico and Canada

The calling features below reflect the monthly access fee discount. No additional discounts apply.

International Options Monthly Recurring Features: Mexico and Canada	0 Voice Minutes	0 Voice Minutes	100 Voice Minutes	250 Voice Minutes	500 Voice Minutes
Monthly Access Fee	\$10.00 (SFO 427)	\$20.00 (SFO 446)	\$15.00 (SFO 434)	\$30.00 (SFO 424)	\$25.00 (SFO 442)
Monthly Access Fee less discount	<b>\$10.00</b>	<b>\$20.00</b>	<b>\$15.00</b>	<b>\$22.50</b>	<b>\$18.75</b>
Voice Overage Rate	Pay Go		\$0.10/minute		\$0.05/minute
Data Allowance <sup>1</sup>	100 MB	250 MB	100 MB	250 MB	1 GB
Data Overage Rate After Allowance <sup>2</sup>	\$10.00/100 MB				\$20.00/1 GB
Messaging Allowance <sup>3</sup>	Pay Go		100 sent; unlimited incoming	250 sent; unlimited incoming	500 sent; unlimited incoming
Messaging Overage Rate After Allowance <sup>2</sup>	Pay Go		\$0.10/Sent Message		\$0.05/Sent Message

**Notes:** <sup>1</sup>The data allowance applies in Canada and Mexico only, where coverage is available. All data usage, including dedicated Mobile Hotspot, deducts from the same data allowance. Requires an eligible domestic data plan or feature and a International GSM capable device. <sup>2</sup>The overage rate is not eligible for discounts. <sup>3</sup>Multimedia messages (MMS) are included in the allowance, but incur data transport charges (deducts from the International data allowance). Pay Go rates for International Voice, International Messaging, and Data Roaming see attached International services pricing for further details..

**This is a recurring feature and will remain on the account until removed.**

### International Options Monthly Recurring Features: 140+ Countries

The calling features below reflect the monthly access fee discount. No additional discounts apply.

International Options Monthly Recurring Features: 140+ Countries	0 Voice Minutes	0 Voice Minutes	100 Voice Minutes	250 Voice Minutes
Monthly Access Fee	\$25.00 (SFO 412)	\$50.00 (SFO 432)	\$40.00 (SFO 444)	\$85.00 (SFO 422)
Monthly Access Fee less discount	<b>\$18.75</b>	<b>\$37.50</b>	<b>\$30.00</b>	<b>\$63.75</b>
Voice Overage Rate	Pay Go		\$0.25/minute	
Data Allowance <sup>1</sup>	100 MB	250 MB	100 MB	250 MB
Data Overage Rate After Allowance <sup>2</sup>	\$25.00/100 MB			
Messaging Allowance <sup>3</sup>	Pay Go		100 sent; unlimited incoming	250 sent; unlimited incoming
Messaging Overage Rate After Allowance <sup>2</sup>	Pay Go		\$0.25/Sent Message	

**Notes:** <sup>1</sup>The data allowance applies in 140+ Countries, where coverage is available. All data usage, including dedicated Mobile Hotspot, deducts from the same data allowance. Requires an eligible domestic data plan or feature and a International GSM capable device. <sup>2</sup>The overage rate is not eligible for discounts. <sup>3</sup>Multimedia messages (MMS) are included in the allowance, but incur data transport charges (deducts from the International data allowance). Pay Go rates for International Voice, International Messaging, and Data Roaming see attached International services pricing for further details..

**This is a recurring feature and will remain on the account until removed.**

### Global Data Optional Features

The Data Packages are eligible for monthly access fee discounts and promotions, when available.

Monthly Access Fee	Allowance	Rate per MB (Canada)	Rate per MB (Mexico)	Rate per MB (Rest of the World)
N/A	N/A	\$2.05/MB	\$5.12MB	\$20.48/MB

**Notes:** See Calling Plan Optional Features section for important information about calling plans, features and options. Applies to all global-capable phones and internet devices. Customer must subscribe to a domestic Mobile Hotspot plan to use the service globally. The majority of your monthly usage must be in the United States. All data usage, including tethering and hotspot, deducts from the same data allowance. See attached International services pricing for further details.

### SingleRate for Enterprise Domestic Shared Business Email and Messaging with International Travel Voice, Email, and Messaging

Government Subscribers Only  
This plan is not eligible for monthly access fee discounts.

<b>Monthly Access Fee</b>	<b>\$65.00 (4G) 95266</b>	<b>\$85.00 (4G ) 95268</b>
<b>Monthly Domestic Voice Allowance in US/Canada/Mexico</b>	Unlimited	Unlimited
<b>Domestic Data Allowance in U.S. (with Sharing)</b>	2 GB	3 GB
<b>Domestic Data Overage Rate</b>	\$10.00 per GB	\$10.00 per GB
<b>Mobile Hotspot*</b>	Included	Included
<b>Domestic and International Travel Messaging Allowance<sup>†</sup></b>	Unlimited	Unlimited
<b>International Travel Voice Allowance (ROW)**</b>	120 Minutes	180 Minutes
<b>International Travel Voice Overage Rate</b>	\$0.40 per minute	\$0.30 per minute
<b>International Travel Data Allowance<sup>††</sup></b>	1 GB	1 GB
<b>International Travel Data Overage Rate</b>	\$45.00 per GB	\$40.00 per GB
<b>International Long Distance – Toll Free</b>	Included	Included

**Notes:** Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Domestic coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Only a 4G LTE GSM/UMTS global-capable smartphone can be activated on these plans.

<sup>††</sup>The international travel data allowance applies in Canada, Mexico, and the **\*\*rest of the world (ROW)**, where coverage is available; aircraft and cruise ship data usage is not included. To see supported countries, go to [www.verizonwireless.com/international](http://www.verizonwireless.com/international). \*Mobile Hotspot is available on all capable devices and allows a line to share its data allowance with multiple Wi-Fi enabled devices. International travel voice minutes and international travel data allowances do not share.

<sup>†</sup>Prevailing rates apply to all other messaging types. Verizon Wireless reserves the right to terminate a line if more than half of the usage over three consecutive billing cycles is outside of the United States, following 30 days' notice to the customer.

**Data Sharing (Domestic Only) Profile Share:** Lines on the same profile can share data. At the end of each billing cycle, any unused data allowances for lines sharing across multiple accounts will be applied proportionally to lines with an overage. Any remaining overage will be billed in KBs.

## ADDITIONAL WIRELESS FEATURES

### Custom State of Florida SMS/MMS Messaging Features

The calling features below reflect the monthly access charge discount. No additional discounts apply.

Text, Picture or Video Messaging for Conventional (Basic) and Smartphone devices only

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Message Allowance	Overage Rate
77328	\$2.00	300 messages	\$0.05 per message
77341	\$3.00	500 messages	
77329	\$7.00	Unlimited	N/A

**Text Messaging:** Text Messaging includes Short Message Service (SMS up to 160 characters) and Enhanced Messaging Service (EMS up to 1120 characters). Enhanced Text Messages sent to most SMS handsets will be delivered as multiple Text messages of up to 160 characters each. Subscribers have the option to have text messages disabled entirely without affecting voicemail or other related services. Overage Rate applies after allowance. Text Messaging plans do not include Operator Assisted Messaging or International Messaging, which is available for 25¢ per message sent and 20¢ per message received, see attached International services pricing for further details.; **Multi-Media Messaging (MMS):** Multi-Media Messaging (MMS) includes picture and video messaging and is only available within the National Enhanced Services Rate and Coverage Area. In addition, MMS messages are \$0.25 per message, per address. In addition to the MMS per message charges, MMS uses calling plan Anytime Minutes or kilobytes. Messaging features are available to all Basic and Smartphone voice, and voice and data bundles.

### Custom State of Florida Field Force Manager Features

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

Conventional (Basic) Phone or Smartphone

	Limited	Basic	Pro*
Monthly Access Charge	\$9.99 per user (75681 for Basic and Smartphone)	\$20.00 per user (76722 - Basic) (76637 – Smartphone)	\$25.00 per user (76723 - Basic) (76638 – Smartphone)

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Field Force Manager ("FFM") Features may only be added onto a Custom State of Florida calling plan with a monthly access fee of \$20.00 or higher. Data plan required. Requires a minimum 500 MB Data Package for Smartphones. FFM is available on select devices only. \*FFM Pro is not available on all devices. If the Block Voice Feature is removed, a per minute rate of \$0.25 shall apply for all voice calls. Downloading the FFM application requires approximately 2 MB (megabytes) of data.

**Push to Talk Plus License (PTT+): Government Subscribers Only**

Push to Talk License licenses are not eligible for any further discounts.

Product	Monthly Access
Tablet	\$3.75
Inter-carrier (only any device)	\$3.75
3rd Party Web (HTML) API Client	\$3.75
Dispatch (License) Windows PC with PTT and mapping	\$22.50

**Notes:** . See attached Calling Plan and Feature Details for important information about calling plans, features and options. Push to Talk license only. Push to Talk Plus requires PTT+ capable device.

**Land Mobile Radio (LMR) for PTT+ : Government Subscribers Only**

Push to Talk Plus service is required.

LMR licenses are not eligible for any further discounts.

Product	Monthly Access
LMR Channel per account	\$0.00

**Notes:** Customer may have multiple channels.

**LMR FEATURE Only**

(When added to a Basic/Smartphone Device with PTT+)

Basic/Smartphone Devices (FEATURE)	\$4.50 (85280)
------------------------------------	----------------

**Notes:** LMR cannot be added to any device without Domestic Push to Talk Plus. Push to Talk Plus requires PTT+ capable device.

**LMR License bundled with PTT+ License**

Tablet	\$8.25
Inter-carrier (any device)	\$8.25
3rd Party Web (HTML) API Client	\$8.25

**Notes:** . See attached Calling Plan and Feature Details for important information about calling plans, features and options. Land Mobile Radio (LMR) Interoperability works with all PTT+ capable devices. To use PTT+, Customer needs a PTT+ feature (or a software license for tablets and dispatch) and a PTT+ compatible device. An Internet Protocol (IP) link is required to connect Verizon's PTT+ service with the customer's LMR network through the "IP Gateway". By purchasing the Land Mobile Radio for PTT+ Customer consents to the tracking of Land Mobile Radio for PTT+ equipment and must obtain authorized consent to tracking from all users and affected persons. No guarantee of accuracy of information transmitted, disclosed, displayed or otherwise conveyed or used. Service could be interrupted or disrupted due to atmospheric conditions, inaccurate ephemeris data and other factors associated with use of satellites and satellite data.

### PTT+ LMR Interoperability Deployment Services.

The below services provide for the integration and deployment of Verizon PTT+ with a customer's LMR network based on either a ROIP (Radio Over IP) or ISSI (Inter Sub-System Interface) LMR network architecture.

Radio Over Internet Protocol (ROIP) and Inter Sub-System Interface (ISSI) Virtual Deployment							
Additional Discounts Not to Apply for Virtual Deployments.							
*Virtual Deployment type	Price Software Plan Id and Description	Provided Via Email	Provided Via Phone	Project Management	Configuration of Equipment	Testing of Equipment	Up to 4 Talk Groups
<b>Onetime Fee</b>							
ROIP Assisted Virtual Deployment	\$2,500	Included	Not Included	Not Included	Not Included	Not Included	Not Included
	623458: PTT+/LMR Assisted Install: ONE TIME						
<b>Onetime Fee</b>							
ROIP Managed Virtual Deployment	\$8,000	Included	Included	Included	Included	Included	Included
	623459: PTT+/LMR Managed Remote: ONE TIME						
<b>Onetime Fee</b>							
ISSI Managed Virtual Deployment	\$25,000	Included	Included	Included	Included	Included	Included
	623461: PTT+/LMR Managed Plus P25: ONE TIME						
<p><b>Note:</b> *Customer must select a type of Virtual Deployment; selection cannot be mixed and/or matched. Customer must also purchase separately a ROIP gateway and cables. Customer must physically install the gateway and provide Virtual Private Network ("VPN") connectivity to the gateway. In addition, Customer must purchase an associated Land Mobile Radio ("LMR") feature and associated authorizations.</p> <p>Virtual Deployments include on-boarding one single facility, accessible by Customer site to site VPN (Verizon Wireless will not go on-site for any Virtual Deployment).</p> <p>Warranty: Verizon Wireless makes no warranties, express or implied, with respect to ROIP or ISSI Virtual Deployment which it provides to Customer on an "AS IS" basis "WITH ALL FAULTS" and "AS AVAILABLE." The accuracy, timeliness, completeness, suitability, or availability of any aspect of ROIP or ISSI Virtual Deployment cannot be guaranteed. THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE HEREBY EXPRESSLY DISCLAIMED IN THEIR ENTIRETY.</p> <p><b>ROIP Assisted Virtual Deployment</b> <i>Customer Requirements:</i></p>							

Physical Installation and configuration.	Access to add network elements to Customer's network (IT administration).
VPN turn up capability (IP Network expertise).	Purchase and configure ROIP Gateway(s) and cables for connected LMR.
Assign a single point of contact.	Provide mobile radio for connectivity to each channel connected to ROIP Gateway(s).
Assign individual to receive and program ROIP Gateway(s) (The customer must have an acute knowledge on how to program land mobile radio equipment).	Provide VPN peer details.

*Virtual Deployment provided:* ROIP Assisted Virtual Deployment is only provided via email. Requests for deployment assistance can be reached at [KODVZLMRSupport@motorolasolutions.com](mailto:KODVZLMRSupport@motorolasolutions.com).

ROIP Assisted Virtual Deployment ends once a successful configuration and functional test occur:

A successful configuration for ROIP and ISSI occurs when:

- Backhaul connectivity successfully verified with IP gateway VPN
- Two-way traffic observed inside backhaul interface
- LMR Group Mobile Directory Number's (MDN) ordered and recorded

A successful functional test occurs when based on the following criteria:

*RoIP Virtual Deployment:*

- Verizon Push to Talk (PTT) Plus Service has LMR linked group published over the air to handsets
- Verizon PTT Plus Service originated group calls to RoIP Gateway successful
- RoIP Gateway originated group calls to Verizon PTT Plus Service successful

*ISSI Virtual Deployment:*

- Verizon PTT Plus Service has LMR linked group published over the air to handsets
- Verizon PTT Plus Service originated group calls to ISSI Interconnect successful
- Talker ID Alias of LMR Group MDN observed on Verizon Push to Talk Plus Service handsets when LMR User is speaking

#### **ROIP Managed Virtual Deployment and ISSI Managed Virtual Deployment**

*Virtual Deployment Includes:*

Working with Customer to engineer network segments for ROIP	Engage with Customer on VPN solution completion
Develop milestones	Verify Customer is configured in PTT Plus Service
Project manage critical milestones	Finalize ROIP Gateway tuning settings including latency and call setup timers based on Customer's network.
Present final design	Validate all configuration steps of the IP Gateway
Define technical parameters for VPN	Configure ROIP Gateway(s)

Requests for managed deployment assistance can be reached at:

Phone Requests: (469) 476-0820

Email Requests: [KODVZLMRSupport@motorolasolutions.com](mailto:KODVZLMRSupport@motorolasolutions.com).

*Customer Requirements: Customer shall be required to do the following:*

Assign a project Single Point of Contact.	Provide mobile / portable radio for connectivity to each channel connected to ROIP Gateway(s).
Backhaul Technology Selection.	Manage schedule and report availability for turn up.
Provide VPN Peer Details.	Approve necessary authorizations to be billed to the account.
Order IP Gateway.	Review designs.
Complete Site Survey Web Form.	Provide resulting LMR Group MDN authorization numbers assigned in Enterprise Contact Management (ECM) Tool to Verizon.
Physical Installation.	Approve the one-time Virtual Deployment charges for managed install.
Build Talk Groups in PTT+ online portal Enterprise Contact Management (ECM), including ROIP Gateway authorization.	Configure VPN on local network to data center.
Assign single point of contact for VPN configuration.	Customer to confirm the required networking elements completed.
Assign individual to receive ROIP Gateway(s).	Configure network elements as needed (if sourced as a part of project).
Access to add network elements to Customer's network.	Test and successfully complete calls between Push to Talk Plus Service and the LMR network.
Purchase separately ROIP Gateway(s) and cables for connected LMR.	

ROIP Managed Virtual Deployment and ISSI Managed Virtual Deployment end once a successful configuration and functional test occur:

A successful configuration for ROIP or ISSI occurs when:

- Backhaul connectivity successfully verified with IP gateway VPN
- Two-way traffic observed inside backhaul interface
- LMR Group MDN(s) ordered and recorded

A successful functional test occurs when based on the following criteria:

*RoIP Virtual Deployment:*

- Verizon PTT Plus Service has LMR linked group published over the air to handsets
- Verizon PTT Plus Service originated group calls to RoIP Gateway successful
- RoIP Gateway originated group calls to Verizon PTT Plus Service successful

**ISSI Virtual Deployment:**

- Verizon PTT Plus Service has LMR linked group published over the air to handsets
- Verizon PTT Plus Service originated group calls to ISSI Interconnect successful
- Talker ID Alias of LMR Group MDN observed on Verizon PTT Plus Service handsets when LMR User is speaking

### Name ID Features

**The features below reflect the monthly access charge discount. No additional discounts apply**

Feature	Monthly Access
Share Name ID*	\$0.00
Company Name ID	\$1.99 per line

**Note:** Depending upon the service provider and/or carrier to which the called party is subscribed, the called party (terminating device) may or may not be able to view the caller's name. The Call Filter Plus feature is purchased separately.

**Company Name ID**

- Allows Government customers to display their agency name, number and logo on outbound calls on a line-by-line basis to Verizon Call Filter Plus subscribers. It may also display on other carrier devices.
- The **Logo display service** is compatible only with Android Devices.
- Users must be subscribed to the My Business portal to use this feature.

**Share Name ID**

- A free service that allows Government customers to personalize their name (as per Account Owner's Billing Name) on outbound calls to Verizon Call Filter Plus subscribers. It may also display on other carrier devices. .

1. Users must be subscribed to the My Business portal to use this feature.

### Call Filter Plus Service Fees

**This feature is NOT eligible for monthly access fee discounts.**

Monthly Access Fee <sup>1</sup>	\$0.75
<b>Notes:</b> Additional feature information is attached hereto. <sup>1</sup> This feature can only be added onto an eligible device. Call Filter service is eligible for Android and iOS customers when they enroll and activate on a smartphone device. Call filter is not available on all call, all devices and in all areas. The Call Filter app is pre-loaded on most capable devices or can be downloaded from the app store. * Once enabled all lines have the ability to access call filter. Call filter features are billed separately; however, all supported options will appear and cannot be blocked.	

### Call Filter Free Service

**This feature is NOT eligible for monthly access fee discounts.**

Monthly Access Fee <sup>1</sup>	\$0.00
<b>Notes:</b> Additional feature information is attached hereto. <sup>1</sup> This feature can only be added onto an eligible device. Call Filter service is eligible for Android and iOS customers when they enroll and activate on a smartphone device. Call filter is not available on all call, all devices and in all areas. The Call Filter app is pre-loaded on most capable devices or can be downloaded from the app store. * Once enabled all lines have the ability to access call filter. ** 4G LTE GSM/UMTS capable devices, require VoLTE/HD Voice. Call filter features are billed separately; however, all supported options will appear and cannot be blocked.	

## ENHANCED SERVICES AND SOLUTIONS

### 4G Smartwatch with NumberShare<sup>1</sup> Unlimited Plan - Government

This plan is not eligible for monthly access fee discounts.

<b>Monthly Access Fee</b>	\$10.00 (13413)
<b>Domestic Anytime Minutes</b>	Unlimited
<b>Domestic Data Allowance<sup>2</sup></b>	Unlimited
<b>Domestic and International Messaging Allowance<sup>3</sup></b>	Unlimited
<p><b>Notes:</b> This plan is for use only in the United States on the Verizon Wireless 4G network. When NumberShare is active on a 4G Smartwatch, certain services will not work on the Smartwatch device including: Call Forwarding, No Answer Transfer, Busy Transfer, Caller Name ID, Voicemail (access voicemail on the Smartwatch device by dialing the host smartphone number and pin)), and RingBack Tones. Calls and messages to/from blocked contacts will not be blocked on the Smartwatch when NumberSharing with a host smartphone. Verizon does not guarantee that NumberShare will work at all times in every situation and the service works only with eligible devices.</p> <p>1. Only lines on select smartwatches with the NumberShare service can be activated on this plan. Certain conditions must be met prior to activation. This plan can only be used when paired with a Verizon Wireless Smartphone that has unlimited data.</p> <p>2. Usage may be prioritized behind other customers in the event of network congestion.</p> <p>3. Unlimited messaging from within the United States to anywhere in the world where messaging services are available.</p>	

### Verizon Mobile Device Management (MDM): Government Subscribers Only

Verizon MDM is not eligible for the monthly access charge discount. No additional discounts apply.

Verizon MDM Feature	Access Fee
<b>Enterprise Firmware Over the Air (FOTA) Management<sup>1</sup></b>	\$0.00 (license requirement with service)
<b>Device Diagnostics<sup>2</sup></b>	\$0.99 / per device per month
<b>Broadband Hotspot Management<sup>3</sup></b>	\$1.49 / per device per month <b>OR</b> \$15.00 / per device per year
<b>Unified Endpoint Management</b>	\$1.00 / per device per month <b>OR</b> \$10.00 / per device per year

Notes: See attached Calling Plan and Feature Details for important information about calling plans, features and options. MDM supports select devices and operating systems and may require installation of a software agent. MDM features are billed separately; however, all supported options will appear and cannot be blocked. Due to a number of features that require HTML 5, Verizon MDM requires Internet Explorer Version 10 and above to work efficiently. <sup>1</sup> Enterprise Firmware Over the Air (FOTA) Management supports Android devices, including Jetpacks and USB devices. <sup>2</sup> Device Diagnostics supports Verizon Android devices operating on OS 4.0 and higher excluding Apple IOS and Google Pixel/Nexus Devices. <sup>3</sup> Broadband Hotspot Management currently supports the MiFi 7730L, AC791L, Jetpack MiFi 6620L, and USB730L.

## MobileIron Enterprise Mobility Management License Fees

### On-Premise (Core)

**(Minimum 500+ MI Core Licenses Required for initial order/installation)**

A discount has been applied. MobileIron Licenses and Installation services are not eligible for any further discounts.

### On-Premise (Core) (Software Subscription License)

Annual Subscription License Bundle per Device with Direct Support				Annual Subscription License Bundle per User with Direct Support (3 Devices per User)		
License Type	Description/SKU	Monthly Cost	Annual Cost	Description/SKU	Monthly Cost	Annual Cost
Silver	MobileIron Core (on-premise) EMM Silver Bundle per Device	\$3.00	\$36.00	MobileIron Core (on-premise) EMM Silver Bundle per User	\$4.50	\$54.00
	SKU: MICore Silver Per Device			SKU: MICore Silver Per User		
Gold	MobileIron Core (on-premise) EMM Gold Bundle per Device	\$4.50	\$54.00	MobileIron Core (on-premise) EMM Gold Bundle per User	\$6.75	\$81.00
	SKU: MICore Gold Per Device			SKU: MICore Gold Per User		
Platinum	MobileIron Core (on-premise) EMM Platinum Bundle per Device	\$5.63	\$67.50	MobileIron Core (on-premise) EMM Platinum Bundle per User	\$8.63	\$103.50
	SKU: MICore Platinum Per Device			SKU: MICore Platinum Per User		

### On-Premise (Core) (Software Perpetual License)

Annual Subscription License Bundle per Device and Direct Support					Annual Subscription License Bundle per User and Direct Support (3 Devices per User)			
Type	Description/SKU	Monthly Cost	Annual Cost	One-Time Cost	Description/SKU	Monthly Cost	Annual Cost	One-Time Cost
Silver License	MobileIron Core (on-premise) EMM Silver per Device Perpetual License	-	-	\$56.25	MobileIron Core (on-premise) EMM Silver per User Perpetual License	-	-	\$82.50
	SKU: MICore Silver Per Device Perpetual License				SKU: MICore Silver Per User Perpetual License			
Silver Support (REQUIRED)	Maintenance Support for MobileIron Core (on-premise) EMM Silver per Device Perpetual License	\$0.94	\$11.25	-	Maintenance Support MobileIron Core (on-premise) EMM Silver per User Perpetual License	\$1.38	\$16.50	-
	SKU: Maintenance Support MICore Silver Per Device Perpetual License				SKU: Maintenance Support MICore Silver Per User Perpetual License			
Gold License	MobileIron Core (on-premise) EMM Gold per Device Perpetual License	-	-	\$82.50	MobileIron Core (on-premise) EMM Gold per User Perpetual License	-	-	\$123.75
	SKU: MICore Gold Per Device Perpetual License				SKU: MICore Gold Per User Perpetual License			

Gold Support (REQUIRE D)	Maintenance Support MobileIron Core (on-premise) EMM Gold per Device Perpetual License  SKU: Maintenance Support MICore Gold Per Device Perpetual License	\$1.38	\$16.50	-	Maintenance Support MobileIron Core (on-premise) EMM Gold per User Perpetual License  SKU: Maintenance Support MICore Gold Per User Perpetual License	\$2.06	\$24.75	-
Platinum License	MobileIron Core (on-premise) EMM Platinum per Device Perpetual License  SKU: MICore Platinum Per Device Perpetual License	-	-	\$105.00	MobileIron Core (on-premise) EMM Platinum per User Perpetual License  SKU: MICore Platinum Per User Perpetual License	-	-	\$157.50
Platinum Support (REQUIRE D)	Maintenance Support MobileIron Core (on-premise) EMM Platinum per Device Perpetual License  SKU: Maintenance Support MICore Platinum Per Device Perpetual License	\$1.75	\$21.00	-	Maintenance Support MobileIron Core (on-premise) EMM Platinum per User Perpetual License  SKU: Maintenance Support MICore Platinum Per User Perpetual License	\$2.63	\$31.50	-

**PROFESSIONAL SERVICES**

**On-Premise (Core) Installation<sup>1</sup>**

Support and Maintenance Included

License Type	Description/SKU	One-time Cost <sup>2</sup>
Silver	MICore Silver Installation MI-PS-DEPLOY1	\$3,000.00
Gold	MICore Gold Installation MI-PS-DEPLOY2	\$6,000.00
Platinum	MICore Platinum Installation MI-PS-DEPLOY3	\$8,000.00

**MobileIron Remote Technical Product Training<sup>3</sup>**

Remote Technical Product Training	Up to six (6) hours of training on the features of MobileIron software (e.g. customization, configuration and support) typically divided into three 2-hour sessions.	\$1,500.00
-----------------------------------	--	------------

Note. Customer must choose one License Type; selection cannot be mixed and/or matched. <sup>1</sup>A minimum of 500 MobileIron licenses are required for On-Premise (Core) for initial order for new MobileIron Customers. <sup>2</sup>On-premise (Core) requires integration and setup with backend systems. Installation charges are prepackaged services providing access to a Professional Services Engineer to assist customer in installing/integrating the MobileIron platform. Pricing above applies to the installation of up to 5,000 MobileIron licenses. If Customer installation requires more than 5,000 MobileIron licenses, MobileIron Premium Implementation Services may apply which provides advisory services and an implementation engineer at a cost of \$25,000.00 to manage large scale deployments; alternatively, Customer may use its own installation services. <sup>3</sup>Remote Technical Product Training (“Training”) does NOT include any installation or setup activities, project management of the Customer deployment, or roll out or implementation of Software. If Customer should need additional product training hours, additional charges apply. Training must be scheduled within 90 days of MobileIron license and services purchase and must be completed within 180 days of purchase (“Term”). Training costs are nonrefundable.

## MobileIron Enterprise Mobility Management License Fees

### Cloud

**(Minimum 25+ MI Cloud Licenses Required for initial order/installation)**

A discount has been applied. MobileIron Licenses and Installation services are not eligible for any further discounts.

#### Cloud License

Annual Subscription License Bundle per Device with Direct Support				Annual Subscription License Bundle per User with Direct Support (3 Devices per User)		
License Type	Description/SKU	Monthly Cost	Annual Cost	Description/SKU	Monthly Cost	Annual Cost
Silver	MobileIron Cloud EMM Silver Bundle per Device	\$3.00	\$36.00	MobileIron Cloud EMM Silver Bundle per User	\$4.50	\$54.00
	SKU: MICloud Silver Per Device			SKU: MICloud Silver Per User		
Gold	MobileIron Cloud EMM Gold Bundle per Device	\$4.50	\$54.00	MobileIron Cloud EMM Gold Bundle per User	\$6.75	\$81.00
	SKU: MICloud Gold Per Device			SKU: MICloud Gold Per User		
Platinum	MobileIron Cloud EMM Platinum Bundle per Device	\$5.63	\$67.50	MobileIron Cloud EMM Platinum Bundle per User	\$8.63	\$103.50
	SKU: MICloud Platinum Per Device			SKU: MICloud Platinum Per User		

#### PROFESSIONAL SERVICES

##### Cloud Installation<sup>1</sup>

Support and Maintenance Included

License Type	SKU	One-time Cost <sup>2</sup>
Silver	MICloud Silver Installation MI-PS-DEPLOY1-MICLOUD	\$1,500.00
Gold	MICloud Gold Installation MI-PS-DEPLOY2-MICLOUD	\$3,000.00
Platinum	MICloud Platinum Installation MI-PS-DEPLOY3-MICLOUD	\$4,000.00
MobileIron Remote Technical Product Training <sup>3</sup>		
Remote Technical Product Training	Up to six (6) hours of training on the features of MobileIron software (e.g. customization, configuration and support) typically divided into three 2-hour sessions.	\$1,500.00

Note. Customer must choose one License Type; selection cannot be mixed and/or matched. <sup>1</sup>A minimum of 25 MobileIron licenses are required for initial Cloud order for new MobileIron customers. <sup>2</sup>MICloud requires integration and setup with backend systems. Installation charges are prepackaged services providing access to a Professional Services Engineer to assist customer in installing/integrating the MobileIron platform. Pricing above applies to the installation of up to 5,000 MobileIron licenses. If Customer installation requires more than 5,000 MobileIron licenses, MobileIron Premium Implementation Services may apply which provides advisory services and an implementation engineer at a cost of \$25,000.00 to manage large scale deployments; alternatively, Customer may use its own installation services. <sup>3</sup>Remote Technical Product Training ("Training") does NOT include any installation or setup activities, project management of the Customer deployment, or roll out or implementation of Software. If Customer should need additional product training hours, additional charges apply. Training must be scheduled within 90 days of MobileIron license and services purchase and must be completed within 180 days of purchase ("Term"). Training costs are nonrefundable.

## MobileIron Enterprise Mobility Management: Government Subscribers On-Premise and Cloud Managed Service Features

All features are available on both On-premise and Cloud managed installations. Included features are determined by MobileIron License Type

Feature	Functionality	Included Features by License		
		Silver	Gold	Platinum
Apple DEP	Supports Apple DEP (for iOS devices)	✓	✓	✓
Android for Work	Supports AFW (on AFW enabled devices)	✗	✓	✓
Samsung KNOX	Integrates with Samsung KNOX (KNOX sold separately)	✗	✓	✓
Email Access	Secure Active Sync (all bundles) Divide PM (Gold/Platinum bundles for additional fee)	✓	✓	✓
Secure Enterprise Gateway (Sentry)	In-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems. (Requires user setup/installation)	✓	✓	✓
Apps@Work	Enterprise App Store Basic Container	✓	✓	✓
Content Catalog	Secure Doc catalog and publishing (basic content repository)	25 files/ 2MB each	50 files/ 25MB each	
Docs@Work	Access, annotate and share documents from email, and on-premise management repositories	✗	✓	✓
AppConnect	Containerization of Application at Rest App wrapping AppConnect ecosystem (3rd Party applications already compatible with MobileIron container)	✗	✓	✓
Web@Work	Secure Browser Secure data in motion No VPN required	✗	✓	✓
Tunnel	iOS per App VPN native functionality	✗	✗	✓
Help@Work	Customizable app that enables screen sharing on device for trouble shooting for internal customer trouble shooting	✗	✗	✓
Identity@Work	MobileIron's ability to proxy Kerberos allows iOS devices that are not on the corporate network to use iOS 7 SSO without needing to expose the Kerberos Key Distribution Center (KDC)	✗	✗	✓
Service Connect Integrations	ServiceNow integration to streamline IT workflows	✗	✗	✓

**Notes.** Customer may purchase MobileIron, Inc. ("MobileIron") licenses and services ("MobileIron Services"), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the MobileIron Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. MobileIron Services are manufactured by MobileIron, Inc. Any license for MobileIron Services must be obtained directly from MobileIron either upon purchase or installation of the MobileIron Services. MobileIron Services are subject to MobileIron's terms and conditions attached hereto. Verizon Wireless will direct MobileIron to fulfill Customer's MobileIron Services order. Customer support for MobileIron Services must be obtained directly from MobileIron, Inc. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to MobileIron Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate MobileIron representatives.

## MobileIron Enterprise Mobility Management Remote Technical Product Training: Government Subscribers

MobileIron Remote Technical Product Training services are not eligible for discounts

Includes up to six (6) hours of MobileIron software training

### Common Training Project Activities

Session	Activity	Description
<b>Administrative Training Session 1</b>	<b>Administrative Training – Session 1:</b> <ol style="list-style-type: none"> <li>1. MobileIron Architecture</li> <li>2. Installation/Setup Review</li> <li>3. MobileIron Admin Portal*</li> <li>4. System Portal</li> <li>5. User Management</li> <li>6. Sentry Overview</li> <li>7. High Availability Overview (if applicable)</li> </ol>	<ul style="list-style-type: none"> <li>• Walk-through of the overall Software architecture</li> <li>• Review installation basics (review only - no installation activity)</li> <li>• Provide a deep dive into the administration portal features and functionality</li> <li>• Provide deployment and configuration set up best practices</li> <li>• Provide policy configuration guidance for common security, sync, and application control policies</li> <li>• Review setup options for Sentry and Core High Availability</li> </ul>
<b>Administrative Training Session 2</b>	<b>Administrative Training – Session 2:</b> <ol style="list-style-type: none"> <li>1. Device Registration/Management Details*</li> <li>2. Common Troubleshooting Steps</li> </ol>	<ul style="list-style-type: none"> <li>• Provide a deep dive into registering users and the user management tools</li> <li>• Review the most common troubleshooting tips and tricks MobileIron administrators and help-desk staff members encounter during the operational rollout</li> </ul>
<b>Help Desk Training</b>	<b>Help Desk Training:</b> <ol style="list-style-type: none"> <li>1. MobileIron Architecture</li> <li>2. UI Basics</li> <li>3. MobileIron Policies</li> <li>4. User Management</li> <li>5. Device Registration/Management Details*</li> </ol>	<ul style="list-style-type: none"> <li>• The same topics as above, but covered for the help desk audience supporting, rather than administering, the MobileIron application</li> </ul>

## Canvas

Canvas is a service that helps you replace paper forms and processes with efficient mobile business apps and forms to save money and time on data collection. Canvas offers 3 plans: Startup Business and Professional. Customers can only select one of the plans at a time (e.g. cannot mix plans on the same account.) Monthly or annual subscription available.

Item Name	Canvas Startup	Canvas Business	Canvas Professional
Number of Users Supported	1 - 5	Unlimited	Unlimited
Monthly Service Fee	\$15.00	\$25.00	\$35.00
Annual Service Fee	\$156.00	\$264.00	\$372.00

## Canvas Features

Features	Startup	Business	Professional
Form Submissions	Unlimited	Unlimited	Unlimited
3 <sup>rd</sup> Party Cloud Integration	✓	✓	✓
App Builder	✓	✓	✓
PDF Designer	✓	✓	✓
Email/Chat Support	✓	✓	✓
Mobile and Web Editing		✓	✓
Phone Support		✓	✓
Dispatch		✓	✓
Submission Status		✓	✓
HIPPA Compliance		✓	✓
Dedicated Support Representative			✓
Dispatch Scheduling			✓
Advanced Password Management			✓
Webservices			✓
Work flow			✓
Canvas Connect			✓

Products shown or referenced are provided by Canvas, a Verizon Partner Program Member, which is solely responsible for the representations and the functionality, pricing and service agreements. Canvas can connect to several different systems including cloud based and server based applications. Customer may purchase Canvas licenses and services ("Canvas Services"), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the Canvas Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. Canvas Services are manufactured by Canvas Solutions, Inc. Any license for Canvas Services must be obtained directly from Canvas either upon purchase or installation of the Canvas Services. Canvas Services are subject to Canvas' terms and conditions. Verizon Wireless will direct Canvas to fulfill Customer's Canvas Services order. Customer support for Canvas Services must be obtained directly from Canvas Solutions, Inc. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to Canvas Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate Canvas representatives.

## SAMSUNG Knox FOR ENTERPRISE

### Samsung Knox Premium

Knox Premium is a cloud-based cross-platform enterprise mobility management solution combined with an on-device secure container for Samsung devices.

Subscription	Monthly (Month to month)	1 – Year Term (Paid in advance)	2 – Year Term (Paid in advance)
License Fee	\$0.75	\$9.00	\$18.00
SKU#	Knox Premium EMM - Monthly	Knox Premium EMM - 1- Year	Knox Premium EMM - 2-Year

### Samsung Knox Workspace

Knox Workspace is an on-device container that isolates business applications and data from personal ones with government-grade security. Knox Workspace also provides enhanced granular controls over device features to enterprise IT administrators. Requires an additional MDM/EMM (like Knox Premium) to manage the container. Manage the container by integrating Knox IT policies with your existing MDM solution. Only available for Samsung Devices.

Subscription	Monthly (Month to month)	1 – Year Term (Paid in advance)	2 – Year Term (Paid in advance)
License Fee	\$2.70	\$32.40	\$64.80
SKU#	Knox Workspace - Monthly	Knox Workspace - 1-Year	Knox Workspace - 2-Year

### Knox Customization

Knox Customization is a comprehensive set of tools and services that allow businesses to customize and deploy end-to-end mobile solutions. Transform Samsung devices into purpose-built solutions for any industry. \*Requires upfront proof of device ownership.

One Time Charge	\$3.00/per license
-----------------	--------------------

### Samsung Knox Solutions

Knox™ is Samsung's mobile device defense-grade security platform. The Knox Platform services multiple user segments through three separate offerings.

**Samsung Knox Premium** is cloud-based device management that allows users to securely manage the business side of corporate devices. **Samsung Knox Workspace**, another offering, is an enterprise device container that acts as a secure and productive environment for work data and apps.

	Package Name	Samsung Knox Premium	Samsung Knox Workspace
	Target Audience	SMB & Enterprise with basic security needs	Enterprise, Government & Regulated Industries
Components	End-to-end secure mobile platform bundled with Samsung cloud EMM for device management	✓	
	Works on both Android and iOS ecosystems	✓	
	Knox container with essential policy controls	✓	✓

	Knox Workspace container with expanded and advanced policy controls		✓
	IT Admin management of employee devices		✓
	Enterprise can black list/white list apps within the Knox Workspace container		✓
	Can manage VPN profiles in Knox Workspace container		✓

Customer may purchase SAMSUNG Knox FOR ENTERPRISE licenses and services (“Knox Services”), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the Knox Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. Knox Services are manufactured by Samsung Electronics Co., Ltd. (“Samsung”). Any license for Knox Services must be obtained directly from Samsung either upon purchase or installation of the Knox Services. Knox Services are subject to Knox Services’ terms and conditions attached hereto. Verizon Wireless will direct Knox Services to fulfill Customer’s Knox Services order. Customer support for Knox Services must be obtained directly from Samsung. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to Knox Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate Knox Services representatives.

## IBM® MaaS360® Enterprise Mobility Management (EMM)

### Unified Endpoint Management (UEM)

#### IBM MaaS360 Unified Endpoint Management License Fees

A discount has been applied. IBM MaaS360 UEM Licenses and services are not eligible for any further discounts.

IBM MaaS360 UEM offers a comprehensive, highly secure platform that manages and protects Devices and Things (smartphones, tablets, laptops, desktops,), People and Identity (authentication, authorization, Single Sign On, secure use access), Apps and Content combined with cognitive technology.

Subscription License Bundle: <b>per Device</b> (One (1) license per device)				Subscription License Bundle: <b>per User</b> (One (1) license per single user with multiple devices)		
License Type	Description/SKU	Monthly Cost	Annual Cost	Description/SKU	Monthly Cost	Annual Cost
Essential	EMM Essentials Suite Per Device License	\$2.25	\$27.00	EMM Essentials Suite Per User	\$4.50	\$54.00
	SKU: D1P3GLL (Monthly/Annual)			SKU: D1P3ILL (Monthly/Annual)		
Deluxe	EMM Deluxe Suite Per Device License	\$3.75	\$45.00	EMM Deluxe Suite Per User License	\$7.50	\$90.00
	SKU: D1P3LLL (Monthly/Annual)			SKU: D1P3NLL (Monthly/Annual)		
Premiere	EMM Premier Suite Per Device	\$4.69	\$56.25	EMM Premier Suite Per User License	\$9.38	\$112.50
	SKU: D1P3RLL (Monthly/Annual)			SKU: D1P3TLL (Monthly/Annual)		
Enterprise	EMM Enterprise Suite Per Device	\$6.75	\$81.00	EMM Enterprise Suite Per User License	\$13.50	\$162.00
				SKU: D1P3YLL		

	SKU: D1P3WLL (Monthly/Annual)			(Monthly/Annual)		
Additional UEM License Options						
License Type	Description/SKU			Monthly Cost	Annual Cost	
Laptop Location	Laptop Location SKU: D1AM8LL (Monthly/Annual)			\$0.38	\$4.50	

IBM MaaS360 UEM Service Features					
Included features are determined by IBM MaaS360 UEM License Type					
Feature	Functionality	Included Features by License			
		Essential	Deluxe	Premier	Enterprise
Device Management	Manage smartphones, tablets & laptops featuring iOS, Android, Windows 10 Mobile, Windows 7, Windows 10 & macOS	✓	✓	✓	✓
App Management	Deploy custom enterprise app catalogs Blacklist, whitelist & require apps	✓	✓	✓	✓
Patch and Update Management	Identify & report on missing OS patches Schedule distribution and installation of Windows OS & macOS patches	✓	✓	✓	✓
Identity Management	Single sign-on & touch access Conditional access to trusted devices Identity federation with apps	✓	✓	✓	✓
Advisor	Improve IT operational efficiency by applying best practices & learning from industry & peer benchmarks	✓	✓	✓	✓
Container App	A separate, corporate mobile workplace for iOS, Android & Windows Productivity apps for work in one place	✓	✓	✓	✓
Mobile Expense Management	Monitor mobile data usage with real-time alerts Set policies to restrict or limit data & voice roaming	✓	✓	✓	✓
Secure Mobile Email	Contain emails, attachments & chat to prevent data leakage Enforce authentication, copy/paste & forwarding restrictions FIPS 140-2 compliant, AES-256 bit encryption for data at res	✗	✓	✓	✓
Secure Mobile Chat	Contain all chat mobile conversations and data Establish quick connections via corporate directory lookup	✗	✓	✓	✓
OS VPN	Leverages the hosted MaaS360 Certificate Authority to issue authentication certs Deployed alongside your corporate VPN solution	✗	✗	✓	✓
Secure Browser	A feature-rich web browser for secure access to intranet sites Define URL filters & security policies based on categories Block known malicious websites	✗	✗	✓	✓
Gateway for Browser	Enable MaaS360 Secure Mobile Browser to access enterprise intranet sites, web apps & network resources Access seamlessly & securely without needing a VPN session on mobile device	✗	✗	✓	✓

Content Management	Enforce authentication, copy/paste & view-only restrictions	x	x	✓	✓
Gateway for Documents	Secure access to internal files: e.g., SharePoint & Windows File Share	x	x	✓	✓
App Security	Enforce authentication & copy/paste restrictions	x	x	✓	✓
Gateway for Apps	Add per app VPN to Application Security to integrate behind-the-firewall data in private apps	x	x	✓	✓
Mobile Document Editor	Create, edit & save content in a secure, encrypted container	x	x	x	✓
Mobile Document Sync	Restrict copy/paste & opening in unmanaged apps Store content securely, both in the cloud & on devices	x	x	x	✓
Mobile Threat Management	Detect and analyze mobile malware on compromised devices Automate remediation via near real-time compliance engine Take action on jailbroken/rooted devices over-the-air	x	x	x	✓

**Notes.** Customer may purchase IBM MaaS360 software licenses and services ("IBM MaaS360 Services"), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the IBM MaaS360 Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. IBM MaaS360 Services are manufactured by International Business Machines Corporation, Inc. Any license for IBM MaaS360 Services must be obtained directly from IBM MaaS360 either upon purchase or receipt of notification from IBM of access to IBM MaaS360 Services. IBM MaaS360 Services are subject to IBM MaaS360's terms and conditions attached hereto. Verizon Wireless will direct IBM MaaS360 to fulfill Customer's IBM MaaS360 Services order. Customer support for IBM MaaS360 Services must be obtained directly from International Business Machines Corporation, Inc. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to IBM MaaS360 Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate IBM MaaS360 representatives.

## Networkfleet Service Options for State of Florida

The Service Options below have been discounted. No additional discounts apply.

Service Options	Purchase Cost
5200-GPS Only	\$17.00
5500-Diagnostics + GPS	\$19.00
H6100 Expressfleet	\$13.86
AssetGuard BX Non-Powered Asset Tracking	\$13.00
Connect	\$2.95
Customizable Update Rates ("CUR") 1 Minute	\$0.00
Customizable Update Rates ("CUR") 45 Seconds	\$1.00
Customizable Update Rates ("CUR") 30 Seconds	\$2.00
Customizable Update Rates ("CUR") 15 Seconds	\$3.00
Satellite	\$34.95
Data Services	\$0.00

**Notes:** Only one Hardware tier and one Service tier per Customer Account. Must be on a 12 month service agreement. Applicable taxes are not included in the above pricing. Any applicable taxes will be applied to the billing invoice. Additional terms & conditions apply to Networkfleet Service that are subject to review by end user government agencies.

**Customizable Update Rates (CUR).** Authorized registered user may change a device update rate through the Self Service Portal (SSP) to 60 seconds at no additional cost. Please note, if the device update rate is changed to a 45 (CUR45), 30 (CUR30), or 15 (CUR15) second update rate, an additional charge per device would apply per the CUR list price for the selected rate.

## Networkfleet Device/Hardware Options for State of Florida

The Devices/Hardware Options below have been discounted. No additional discounts apply.

Device/Hardware Options	Purchase Cost
5200-GPS Only	\$85.00
5500-Diagnostics + GPS	\$85.00
1009N2VD-6100 Expressfleet	\$55.00
AssetGuard BX Non-Powered Asset Tracking	\$150.00

**Notes:** Only one Hardware tier and one Service tier per Customer Account. Must be on a 12 month service agreement. Applicable taxes are not included in the above pricing. Any applicable taxes will be applied to the billing invoice.

Item Number	Accessory	Price
PARTS030	Reinstallation Kit	\$3.00
PARTS031	Tamper Resistant Zip Ties (100 per pack)	\$50.00
PARTS032	Combination Antenna A (standard)	\$30.00
PARTS037	AT-1400 Replacement Battery	\$45.00
PARTS039	AT-1400 Bracket	\$20.00
PARTS040	Window-Mount GPS Antenna Module (5500/5200)	\$35.00
PARTS041	Sensor Input Harness (5500/5200)	\$10.00
PARTS042	OBD-II Adapter Kit only including Core Connector & 8 Adapters (5500/5200)	\$20.00
PARTS043	6-pin Heavy Duty Harness (5500/5200)	\$35.00
PARTS044	9-pin Heavy Duty Harness with Square Flange (5500/5200)	\$35.00
PARTS045	9-pin Heavy Duty Harness with "D" Mount (5500/5200)	\$35.00
PARTS069	OBD Harness Extension	\$10.00
PARTS070	16-Pin Heavy Duty Harness	\$35.00
PARTS046	Universal Harness (5200)	\$10.00
PARTS047	Light Duty Harness plus OBD-II Adapter Kit (5500/5200)	\$35.00
PARTS090	Alternate Power/Ground Adapter (5200/5500)	\$20.00
PARTS053	Garmin FMI 45 Cable with Traffic for Connect	\$145.95
PARTS054	Garmin FMI Modified Cable	\$55.00
PARTS057	Pelican Micro Case for 5200 w/ 15' Universal Harness	\$74.95
A-PEM001	PEM Port Expansion Module	\$140.00
PARTS059	Quick Install Harness	\$10.00
A-SAT001	Satellite Modem	\$550.00
PARTSS063	Satellite Antenna	\$50.00
PARTSS064	Satellite Harness	\$50.00
KIT-SAT	Satellite Kit (includes one modem, antenna & harness)	\$650.00
PARTS065	Asset Guard BX Replacement Batter (1)	\$75.00
PARTS066	Asset Guard BX Magnet Mount Kit (set of 4) *See Note	\$75.00
PARTS095	ID Reader Adapter Install Kit	\$30.00
PARTS060	Driver ID Reader	\$15.00
PARTS061	Driver ID Key	\$3.50
PARTS087	Audible Driver ID Alert	\$15.00
PARTS071	Bluetooth Extension	\$0.00
PARTS093	Universal Harness (6100)	\$10.00
PARTS058	Universal Harness	\$10.00
PARTS097	5000 9-Pin "D" Mount Harness Type 2	\$35.00
PARTS098	5000 9-Pin Square Harness Type 2	\$35.00
PARTS111	USM 9-Pin "D" Mount Harness Type 2 Pins F-G	\$35.00
PARTS112	USM 9-Pin Square Harness Type 2 Pins F-G	\$35.00

**Notes:** \* Asset Guard BX Magnet Mount Kit includes CalAmp 133561 hardware and lanyard & CalAmp 1M101-MNC25 magnets (set of 4).

Item Number	Installation Type	Pricing (per unit)	Notes
I-INSTALL-UNIT	Base Installation – Plug/Play or 3 Wire	<b>\$65.00</b>	Base Installation includes 1 Device and 1 Harness
D-INSTALL-UNIT	Limited Lifetime Base Installation	<b>\$2.00</b>	Monthly Service Fee
I-INSTALL-FMI	Add-On to Base Installation (Garmin)	<b>\$35.00</b>	
I-INSTALL-SENSOR	Add-On to Base Installation (Sensor)	<b>\$65.00</b>	Sensor Install is \$65.00 PER SENSOR
I-INSTALL-AG	Add-On to Base Installation (AssetGuard BX)	<b>\$65.00</b>	
I-INSTALL-PMC	Add-On to Base Installation (Pelican Micro Case)	<b>\$35.00</b>	
I-INSTALL-PEM	Add-On to Base Installation (Port Expansion Module)	<b>\$35.00</b>	
I-INSTALL-SAT	Add-On to Base Installation (Satellite)	<b>\$35.00</b>	
I-INSTALL-DID	Add-On to Base Installation (Driver ID)	<b>\$35.00</b>	

I-INSTALL –BTE	Add-On to Base Installation (Bluetooth)	<b>\$35.00</b>	
D-INSTALL-BTE	Limited Lifetime Add-On to Base Installation (Bluetooth)	<b>\$1.00</b>	Monthly Service Fee
D-INSTALL-FMI	Limited Lifetime Add-On to Base Installation (Garmin)	<b>\$1.00</b>	Monthly Service Fee
D-INSTALL-SENSOR	Limited Lifetime Add-On to Base Installation (Sensor)	<b>\$1.00</b>	
D-INSTALL-AG	Limited Lifetime Add-On to Base Installation (AssetGuard BX/PW)	<b>\$2.00</b>	
D-INSTALL-PMC	Limited Lifetime Add-On to Base Installation (Pelican Micro Case)	<b>\$1.00</b>	Monthly Service Fee
D-INSTALL-PEM	Limited Lifetime Add-On to Base Installation (Port Expansion Module)	<b>\$1.00</b>	Monthly Service Fee
D-INSTALL-SAT	Limited Lifetime Add-On to Base Installation (Satellite)	<b>\$1.00</b>	Monthly Service Fee
D-INSTALL-DID	Limited Lifetime Add-On to Base Installation (Driver ID)	<b>\$1.00</b>	Monthly Service Fee
I-SWAP-UNIT	Device Swap	<b>\$65.00</b>	
I-TRANSFER-UNIT	Device Transfer	<b>\$65.00</b>	
I-REMOVAL-UNIT	Removal	<b>\$65.00</b>	Removal of device.
I-NOSHOW	No Show	<b>\$75.00</b>	Applies per trip if the installer makes the trip and the designated vehicle is not available so the unit cannot be installed.
I-TROUBLESHOOT-UNIT	Troubleshoot; Mileage	<b>\$65.00</b>	Per Trip
TRAINING-HALF	½ Day Installation Training	<b>\$150.00</b>	
TRAINING-FULL	Full Day Installation Training	<b>\$300.00</b>	

## One Talk Solution: Government Subscribers Only

The plans/features below reflect any applicable discount. No additional discounts apply.

**One Talk** is a business telephone system that combines landline and mobile phone capabilities into a fully integrated mobile and office solution providing a **single telephone number ("Mobile Data Number/MDN")** with the same mobile and landline features.

### One Talk Solution: Desk Phone/Mobile Client

Price Plan Type	Line Level Plans
One Talk Primary MDN	Monthly Access
One Talk Price Plan (100 MB Data)	\$10.00
One Talk Feature	\$15.00
One Talk Line Access Charge	N/A

### One Talk Solution: Auto Receptionist (AR)

#### Auto Receptionist

Price Plan Type	Line Level Plans
One Talk Primary MDN	Monthly Access
One Talk AR Price Plan (100 MB Data)	\$10.00
One Talk AR Feature	\$10.00
One Talk AR Line Access Charge	N/A

### One Talk Solution: Hunt Group (HG)

Hunt Group - Every ECPD profile will be allowed to activate two Hunt Groups by default; additional Hunt Groups can be purchased as long as the ratio of active One Talk lines to Hunt Groups is 3:1 respectively

Price Plan Type	Line Level Plans
One Talk Primary MDN	Monthly Access
One Talk HG Price Plan (100 MB Data)	\$0.00
One Talk HG Feature	\$0.00
One Talk HG Line Access Charge	N/A

### Optional Features

One Talk Premium Visual Voicemail for Android Smartphone	\$2.99
One Talk Premium Visual Voicemail for Desk Phone & Mobile Client	\$2.99
One Talk Voicemail Talk To Text for iOS Smartphones	\$2.99
One Talk Caller Name ID	\$2.99

### Additional Devices

For MDN's activated on a Smartphone, Desk Phone, Mobile Client, a maximum of up to eight (8) devices can be shared with the MDN as follows: 1 Smartphone, up to 2 desk phones and up to 5 mobile clients.

Smartphone Device	Desk Phone <sup>1</sup>	Mobile Client <sup>2</sup> (Includes Smartphones and Tablets)	Auto Receptionist/ Hunt Group
Additional devices (endpoint) incur a \$10.00 monthly access	\$0.00 for additional devices (excluding Smartphone devices with One Talk Basic Dialer)	\$0.00 for additional devices (excluding Smartphone devices with One Talk Basic Dialer)	N/A

**Notes:** One Talk service is applied to the Verizon Wireless MDN and is available on all of the user's devices. One Talk is **not** compatible with Fax machines, credit card POS solutions, or Security Systems. One Talk calls drop if either party leaves Verizon 4G LTE coverage. When outside of the 4G LTE coverage area and without 3G or WiFi service, the device operates as a standard device (1X calling) with standard voice and SMS messaging capabilities with no One Talk features available to the user. Mobile client is the One Talk client. <sup>1</sup>One (1) additional Desk Phone can be added as an additional device per MDN. <sup>2</sup>Mobile Client eligible devices (includes devices from other carriers); Smartphones (without One Talk Basic Dialer), wireless and WiFi tablets; limit five (5) total per MDN (including primary device. Installing the One Talk Mobile client consumes an estimated 50MB of data. Additional information regarding One Talk is attached hereto

## 4G Business Unlimited One Talk Auto Receptionist Plan

Government Subscribers Only

This plan is NOT eligible for monthly access fee discounts.

Monthly Access Fee	\$10.00 (99319)
Voice Minutes Allowance	Unlimited
Data Allowance <sup>1</sup>	Unlimited

**Notes:** Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Only One Talk Auto Receptionist Devices can be activated on this plan.

This is a current retail plan and is subject to change or be discontinued without notice to the customer. This Business Unlimited Plan is not compatible with Private Network Traffic Management (PNTM) or Private Network.

<sup>1</sup>If 22 GB of domestic data usage is exceeded on any line in any given billing cycle, Verizon Wireless will limit the data throughput speeds to up to 200 Kbps for additional usage for the remainder of the then-current billing cycle for the line that exceeds the data usage. To ensure users are able to maximize their high-speed data use for business applications, video applications will stream at up to 1080p. For data usage in Canada and Mexico, after the first 512 MB of usage in a day, throughput speeds for additional usage will be reduced for the remainder of the day. Usage outside of the United States requires a 4G LTE GSM/UMTS global-capable device.

## 4G Business Unlimited One Talk Mobile Client/Desk Phone Plan

Government Subscribers Only

This plan is NOT eligible for monthly access fee discounts.

Monthly Access Fee	\$10.00 (99320)
Voice Minutes Allowance	Unlimited
Data Allowance <sup>1</sup>	Unlimited

**Notes:** Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Only One Talk Desk Phone Devices can be activated on this plan.

This is a current retail plan and is subject to change or be discontinued without notice to the customer. This Business Unlimited Plan is not compatible with Private Network Traffic Management (PNTM) or Private Network.

<sup>1</sup>If 22 GB of domestic data usage is exceeded on any line in any given billing cycle, Verizon Wireless will limit the data throughput speeds to up to 200 Kbps for additional usage for the remainder of the then-current billing cycle for the line that exceeds the data usage. To ensure users are able to maximize their high-speed data use for business applications, video applications will stream at up to 1080p. For data usage in Canada and Mexico, after the first 512 MB of usage in a day, throughput speeds for additional usage will be reduced for the remainder of the day. Usage outside of the United States requires a 4G LTE GSM/UMTS global-capable device.

## One Talk Call Queue

Government Subscribers Only

No Domestic Roaming or Long Distance Charges

This plan is NOT eligible for monthly access fee discounts.

Monthly Access Fee	\$25.00	\$45.00
Calls in Queue	10 calls held in queue	25 calls held in queue
Monthly Call Queue Agent Feature	\$1.00 per line/per month*	

**Notes:** One Talk service is applied to the Verizon Wireless MDN and is available on all of the user's devices. One Talk is not compatible with Fax machines, credit card POS solutions, or Security Systems. One Talk calls drop if either party leaves Verizon 4G LTE coverage. When outside of the 4G LTE coverage area and without 3G or WiFi service, the device operates as a standard device (1X calling) with standard voice and SMS messaging capabilities with no One Talk features available to the user. Mobile client is the One Talk client. <sup>1</sup>One (1) additional Desk Phone can be added as an additional device per MDN. <sup>2</sup>Mobile Client eligible devices (includes devices from other carriers); Smartphones (without One Talk Basic Dialer), wireless and WiFi tablets; limit five (5) total per MDN (including primary device. Installing the One Talk Mobile client consumes an estimated 50MB of data. For additional information regarding One Talk please refer to the One Talk documents attached hereto.

1. Call queue has a maximum limit of 40 agents per call queue setup.
2. Dial MDN direct or be routed through Auto Receptionist

## NETMOTION

These products Do Not qualify for additional discounts

Service Item	Software Plan ID	SKU	Frequency/ Payment Plan	Price	Function
"Mobility VPN" (Virtual Private Network for wireless connections) - An encrypted, secure tunnel for mobile devices	651968	NMSVZW-GOV-SILVER-Monthly: MONTHLY	Monthly	\$4.33	"Mobility VPN" (Virtual Private Network for wireless connections) An encrypted, secure tunnel for mobile devices -- Works with Android, iOS, Windows and Mac devices -- Criminal Justice Information Systems (CJIS) Compliance
	651969	NMSVZW-GOV-SILVER-Annual: ANNUAL	Annual	\$52.00	
"Mobility VPN" + "Modules" (Policy, Network Access Control, Mobile Analysis)	651970	NMSVZW-GOV-GOLD-Monthly: MONTHLY	Monthly	\$6.93	All features of the Mobility VPN base product, plus the Policy, Network Access Control (NAC) and Mobile Analysis Modules
	651971	NMSVZW-GOV-GOLD-Annual: ANNUAL	Annual	\$83.20	
"Mobility VPN" + "Modules" + "Diagnostics" which includes connectivity problem identification, security reinforcement, improved end user productivity and powerful reporting.	651972	NMSVZW-GOV-PLATINUM-Monthly: MONTHLY	Monthly	\$8.67	All features of the Mobility VPN base product and the Policy, Network Access Control (NAC) and Mobile Analysis Modules, Plus Diagnostics
	651973	NMSVZW-GOV-PLATINUM-Annual: ANNUAL	Annual	\$104.00	
Mobility VPN + "Modules" + "Diagnostics" + "Mobile IQ" which includes performance assessment, threat defense, cost control, location intelligence and inventory, troubleshooting and system-wide status	651974	NMSVZW-GOV-DIAMOND-Monthly: MONTHLY	Monthly	\$13.00	All features of the Mobility VPN base product and the Policy, Network Access Control (NAC) and Mobile Analysis Modules, Plus Diagnostics + MobileIQ
	651975	NMSVZW-GOV-DIAMOND-Annual: ANNUAL	Annual	\$156.00	
Comprehensive data collection and root cause detection software (add-on feature)	651976	NMSVZW-GOV-DIAGS-Monthly: MONTHLY	Monthly	\$4.33	Comprehensive data collection and root cause detection software
	651977	NMSVZW-GOV-DIAGS-Annual: ANNUAL	Annual	\$52.00	
Visual troubleshooting, analytics and alerting dashboards (add-on feature)	651978	NMSVZW-GOV-MIQ-Monthly: MONTHLY	Monthly	\$4.33	Visual troubleshooting, analytics and alerting dashboards
	651979	NMSVZW-GOV-MIQ-Annual: ANNUAL	Annual	\$52.00	
Professional Services - Up to 8 Hours	651980	11NMPS-GOV-8HR-S - One Time: ONE TIME	One-Time	\$2,000.00	Off-site Services
Professional Services - Up to 4 Hours	651981	11NMPS-GOV-4HR-S - One Time: ONE TIME	One-Time	\$1,000.00	Off-site Services

Mobility Certification Training	651982	11NMTR-GOV-C - One Time: ONE TIME	One-Time	\$2,295.00	Off-site Services
Elite Technical Service (0 - 4,999 licenses)	651983	11NMETS-GOV - One Time: ONE TIME	One-Time	\$30,000.00	Off-site Services
Elite Technical Service (5,000+ licenses)	651984	11NMETS5K-GOV - One Time: ONE TIME	One-Time	\$50,000.00	Off-site Services
Dedicated Technical Account Manager (1 year)	651985	11NMPS-GOV-TAM - One Time: ONE TIME	One-Time	\$40,000.00	Off-site Services

**Note:** Customer may purchase NetMotion Software, Inc. ("NetMotion") licenses and services ("NetMotion Services") at the prices listed above. NetMotion Services listed in the pricing sheet marked with an asterisks \*\*\* cannot be mixed or matched with other NetMotion Licenses or Services. Verizon Wireless is not the licensor of the NetMotion Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. NetMotion Services are manufactured by NetMotion. NetMotion Software is subject to a separate End User License Agreement (EULA) with NetMotion attached hereto. Use of the NetMotion licenses or NetMotion Services is deemed to be the Customer's acceptance of the terms of the EULA. Customer must accept the EULA as the party liable for each license, and agrees that the Customer will comply with the obligations under the EULA. Verizon Wireless reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause. Customer's sole and exclusive remedy for any damages, losses, claims, costs, and expenses arising out of or relating to use of the Solution will be termination of service.

A.

Verizon Wireless will direct NetMotion to fulfill Customer's NetMotion Services order. Basic functionality questions and other general customer support can be obtained by calling Verizon Wireless Customer Support. All other customer support questions and issues for NetMotion Services must be obtained directly from NetMotion Software, Inc. If Verizon Wireless, in its sole discretion, determines that an inquiry from a subscriber is related to NetMotion Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate NetMotion representatives.

**Asavie Moda** is a network-based “all-in-one” web portal security and data management solution that enables organizations to easily and effectively manage security and productivity, along with rich reporting insights on all their mobile devices.

The Asavie Moda solution extends the security provided by the customer’s Mobile Device Management platform into the network by delivering real-time visibility, control and security of the data in transit for any mobile device.

Asavie Moda Government Customers Only					
The price below reflects the monthly access discounts. No additional discounts apply.					
Description	SKU Name	Plan ID	Quantity	Annual	Monthly
<sup>1</sup> Asavie Moda for MPN Gov Customers	ModaMPNG	677970 (Annual)	1-199	\$80.92	\$7.49
			200-499	\$68.85	\$6.38
			500-999	\$60.75	\$5.63
		677971 (Monthly)	1000-2499	\$52.65	\$4.88
			2500-9999	\$48.60	\$4.50
			10000+	\$40.50	\$3.75
<sup>2</sup> Asavie Moda Global (OTT) Gov Customers	ModaGLOBAL	677969 (Annual)	1-199	\$80.92	\$7.49
			200-499	\$68.85	\$6.38
			500-999	\$60.75	\$5.63
		677968 (Monthly)	1000-2499	\$52.65	\$4.88
			2500-9999	\$48.60	\$4.50
			10000+	\$40.50	\$3.75

Notes. Asavie Moda is an all-in-one web portal that is an easy to deploy security and data management solution for an entire mobile estate.

<sup>1</sup>Asavie Moda for MPN Gov Customers – **Does** require customers to use pricing and equipment in accordance with the Private Network terms and conditions as your contract allows.

<sup>2</sup>Asavie Moda Global (OTT) Gov Customers – **Does not** require Private Network.

Products shown or referenced are provided by Asavie Technologies, Inc. (“Asavie”), a Verizon Partner Program Member, which is solely responsible for the representations and the functionality, pricing and service agreements. Asavie can connect to several different systems including cloud based and server based applications. Customer may purchase Asavie licenses and services (“Asavie Services”), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the Asavie Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. Asavie Services are manufactured by Asavie Technologies, Inc. Any license for Asavie Services must be obtained directly from Asavie either upon purchase or installation of the Asavie Services. Asavie Services are subject to Asavie terms and conditions attached hereto. Verizon Wireless will direct Asavie to fulfill Customer’s Asavie Services order. Customer support for Asavie Services must be obtained directly from Asavie Technologies, Inc. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to Asavie Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate Asavie representatives.

**Asavie IoT Connect®** provides Private Network connectivity on demand for remote sites and IoT devices. Provides direct, enterprise-grade connection that bypasses the public Internet, helping to reduce exposure to possible cyber threats.

**Asavie IoT Connect®  
Government Customers Only**

The price below reflects the monthly access discounts. No additional discounts apply.

Name	SKU Name	Plan ID	Quantity	Annual	Monthly
IoT MPN 25 MB	IOTCMPN25MBG	677959 (Annual)	1-199	\$24.22	\$2.24
			200-499	\$20.59	\$1.91
			500-999	\$18.16	\$1.68
		677958 (Monthly)	1000-2499	\$15.74	\$1.46
			2500-9999	\$14.53	\$1.35
			10000+	\$12.11	\$1.12

Notes. Asavie IoT Connect runs over Verizon's secure Private Network.

<sup>1</sup> Requires customers to use pricing and equipment in accordance with the Private Network terms and conditions as your contract allows.

Products shown or referenced are provided by Asavie Technologies, Inc. ("Asavie"), a Verizon Partner Program Member, which is solely responsible for the representations and the functionality, pricing and service agreements. Asavie can connect to several different systems including cloud based and server based applications. Customer may purchase Asavie licenses and services ("Asavie Services"), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the Asavie Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. Asavie Services are manufactured by Asavie Technologies, Inc. Any license for Asavie Services must be obtained directly from Asavie either upon purchase or installation of the Asavie Services. Asavie Services are subject to Asavie terms and conditions attached hereto. Verizon Wireless will direct Asavie to fulfill Customer's Asavie Services order. Customer support for Asavie Services must be obtained directly from Asavie Technologies, Inc. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to Asavie Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate Asavie representatives.

**Asavie IoT Connect® with Cloud Connect  
Government Customers Only**

The price below reflects the monthly access discounts. No additional discounts apply.

<b>IoT MPN 25 MB CC</b>	<b>IOTCMPN25MBCCG</b>	<b>677953 (Annual)</b>	1-199	31.46	2.99
			200-499	26.74	2.54
			500-999	23.59	2.24
		<b>677952 (Monthly)</b>	1000-2499	20.45	1.95
			2500-9999	18.87	1.80
			10000+	15.73	1.5
<b>IoT MPN 150 MB</b>	<b>IOTCMPN150MBG</b>	<b>677957 (Annual)</b>	1-199	\$40.42	\$3.74
			200-499	\$34.36	\$3.18
			500-999	\$30.31	\$2.81
		<b>677956 (Monthly)</b>	1000-2499	\$26.27	\$2.43
			2500-9999	\$24.25	\$2.25
			10000+	\$20.21	\$1.87
<b>IoT MPN 150+ MB</b>	<b>IOTCMPN150MBPLUSG</b>	<b>677955 (Annual)</b>	1-199	\$80.92	\$7.49
			200-499	\$68.78	\$6.37
			500-999	\$60.69	\$5.62
		<b>677954 (Monthly)</b>	1000-2499	\$52.60	\$4.87
			2500-9999	\$48.55	\$4.50
			10000+	\$40.46	\$3.75

Notes. Asavie IoT Connect runs over Verizon's secure Private Network.

<sup>1</sup> Requires customers to use pricing and equipment in accordance with the Private Network terms and conditions as your contract allows.

Products shown or referenced are provided by Asavie Technologies, Inc. ("Asavie"), a Verizon Partner Program Member, which is solely responsible for the representations and the functionality, pricing and service agreements. Asavie can connect to several different systems including cloud based and server based applications. Customer may purchase Asavie licenses and services ("Asavie Services"), to be billed by Verizon Wireless, at the prices listed above. Verizon Wireless is not the licensor of the Asavie Services and makes no representations or warranties whatsoever, either express or implied, with respect to them. Asavie Services are manufactured by Asavie Technologies, Inc. Asavie Services are subject to Asavie terms and conditions attached hereto. Verizon Wireless will direct Asavie to fulfill Customer's Asavie Services order. Customer support for Asavie Services must be obtained directly from Asavie Technologies, Inc. If Verizon Wireless in its sole discretion determines that an inquiry from a subscriber is related to Asavie Services and is not one concerning Equipment or Wireless Service, it may transfer the service request to appropriate Asavie representatives.

## Verizon Secure Cloud Gateway

Powered by iboss

Secure Cloud Gateway is a cloud-based secure web gateway service that provides security for web traffic and protects users from internet-threats through enforcement of internet policy compliance. Built for the cloud and the modern, distributed organization, Secure Cloud Gateway helps meet the cybersecurity needs of today's organizations who are challenged with enforcing internet policy and security across decentralized networks, branch offices, and remote and mobile users. The Secure Cloud Gateway service is powered by iboss, a leading web security company.

These licenses are not eligible for monthly access discounts.

SKU	Price Plan ID	Description	Frequency	Cost
CF-WIRELESS-NNI-SLED	Price plan ID 699515	Core Gateway	Monthly	\$2.72
MDF-WIRELESS-NNI-SLED	Price Plan ID 699514	Malware Defense	Monthly	\$4.17

**Note:** Secure Cloud Gateway powered by iboss solution requires a Mobile Private Network Tiered Hierarchy design where iboss operates the parent private network and each mutual customer of iboss and Verizon Wireless must have a private network built as a child of the iboss parent. \*A minimum quantity of 100 user licenses per order is required. Licenses bill in full monthly increments with no prorations with a one year line term.

\*Devices that are certified for private network include:

- Verizon Jetpacks
- LTE Enabled routers – [\[Consult with sales and product manager for the number of licenses associated with multi user devices.\]](#)
- LTE enabled tablets, phones and laptops

<sup>1</sup>These SKUs are mutually exclusive and cannot be combined.

### Verizon Secure Cloud Gateway Core Package: Web Gateway

### Verizon Secure Cloud Gateway Plus Package: Malware Defense

Core Package delivers compliance based web gateway features to all devices	Plus Package delivers all Core Package features and advanced malware defense
<ul style="list-style-type: none"> <li>• Web and Content Filtering</li> <li>• Protection for outdated browsers and Operating System (OS)</li> <li>• Secured Socket Layer (SSL) visibility and traffic management</li> <li>• Single pane of glass management</li> <li>• Cloud apps and social media controls</li> <li>• Advanced, near real-time reporting</li> <li>• Flexible data traffic re-direction for devices, virtually everywhere</li> </ul>	<ul style="list-style-type: none"> <li>• Advanced malware detection and prevention for polymorphic threats.</li> <li>• Command and Control (CnC) callback monitoring across enterprise ports and protocols.</li> <li>• Signature based intrusion detection and prevention.</li> <li>• Protection across all devices and locations including HQ, remote offices, mobile and Bring Your Own Device (BYOD).</li> <li>• Behavioral Malware Sandboxing</li> </ul>

Note: Pricing includes 24/7 Mission Critical Support and Basic Implementation Support (8 hours of policy setup and dashboard help).

## Lookout Mobile Endpoint Security

These products do not qualify for further discounts.

Lookout Mobile Endpoint Security helps organizations prevent data loss and leakage through mobile devices by delivering advanced security and comprehensive policy-based protection against the spectrum of mobile risk.

SKU	Description	Term	Price
MES-GOV-C-P-U1Y-PU	GOV Comprehensive - User w Phishing	Annual	\$75.60
MES-GOV-C-P-U1Y-PD	GOV Comprehensive/Dev w Phishing	Annual	\$54.00
GOV-SPT-MES-PRMPLS-U1Y-PD	GOV Prem Plus Support/Device	Annual	\$8.10
GOV-SPT-MES-PRMPLS-U1Y-PU	GOV Prem Plus Support/User	Annual	\$11.34
GOV-SPT-MES-PRM-U1Y-PD	GOV Premium Support/Device	Annual	\$4.50
GOV-SPT-MES-PRM-U1Y-PU	GOV Premium Support/User	Annual	\$6.75

**Note:** In order to be able to purchase Lookout Mobile Endpoint Security, Customer is required to maintain a minimum of one (1) active and billing Verizon Wireless line of service. Additionally, Customer is required to provide an active corporate email address to complete the activation process.

**Verizon provides support for ordering Lookout Mobile Endpoint Security licenses, billing, and will provide Tier one (1) customer support for Lookout.**

**Lookout will provide Tier two (2) when required through a Verizon Wireless call transfer.**

### LTE Vehicle Internet

These hardware Sku bundles are not eligible for further discounts.

The LTE Vehicle Internet solution supports in-Vehicle connectivity providing ruggedized routers and cloud-managed services. Services are designed to allow departments to deploy, configure, manage and scale quickly and in real time. Devices support dual carrier with SIM-based Auto-Carrier Selection, Public Safety and Data plans, and are available on many public-sector contract vehicles.

SKU#	Description	OEM P/N	Price
5642701	1-yr NetCloud Mobile FIPS Essentials and Advanced Plans and IBR900 FIPS router with WiFi (1000Mbps modem)	MA1-900F120B-XFA	\$1,097.10
5642703	5-yr NetCloud Mobile FIPS Essentials and Advanced Plans and IBR900 FIPS router with WiFi (1000Mbps modem)	MA5-900F120B-XFA	\$1,853.10
5642698	1-yr NetCloud Mobile FIPS Essentials and Advanced Plans and IBR1700 FIPS router with WiFi (1200Mbps modem)	MA1-170F120B-XFA	\$1,574.10
5642700	5-yr NetCloud Mobile FIPS Essentials and Advanced Plans and IBR1700 FIPS router with WiFi (1200Mbps modem)	MA5-170F120B-XFA	\$2,330.10
5642692	1-yr NetCloud Mobile Essentials Plan and IBR900 router with WiFi (1000Mbps modem)	MA1-0900120B-NNA	\$899.10
5642694	5-yr NetCloud Mobile Essentials Plan and IBR900 router with WiFi (1000Mbps modem)	MA5-0900120B-NNA	\$1,358.10
5584528	1-yr NetCloud Mobile Essentials Plan and IBR1700 router with WiFi (1200Mbps modem)	MA1-1700120B-NNA	\$1,448.10
5642691	5-yr NetCloud Mobile Essentials Plan and IBR1700 router with WiFi (1200Mbps modem)	MA5-1700120B-NNA	\$1,943.10
5691111	3-yr NetCloud IoT Essentials Plan and IBR600C router with WiFi (150 Mbps modem), North America	TB3-600C150M-NNN	\$458.10
5691112	5-yr NetCloud IoT Essentials Plan and IBR600C router with WiFi (150 Mbps modem), North America	TB5-600C150M-NNN	\$512.10
5642722	1-yr NetCloud Branch Essentials Plan with AER2200 router with WiFi (1200Mbps modem), North America	BA1-2200120B-NNN	\$1,412.10
5642723	3-yr NetCloud Branch Essentials Plan with AER2200 router with WiFi (1200Mbps modem), North America	BA3-2200120B-NNN	\$1,655.10
5642724	5-yr NetCloud Branch Essentials Plan with AER2200 router with WiFi (1200Mbps modem), North America	BA5-2200120B-NNN	\$1,916.10
5691113	3-yr NetCloud IoT Gateway Essentials Plan and IBR200 router with WiFi (10 Mbps modem) for Verizon	TB3-020010M-VNN	\$278.10
5691114	5-yr NetCloud IoT Gateway Essentials Plan and IBR200 router with WiFi (10 Mbps modem) for Verizon	TB5-020010M-VNN	\$332.10
5642707	LTE Advanced Pro (1200Mbps) modem upgrade for Mobile.	MA-MC400-1200M-B	\$539.99

	Includes IBR1700 & COR Dock doors, no antennas		
5584526	3-yr NetCloud Mobile Essentials Plan and IBR1700 router with WiFi (1200Mbps modem), no AC power supply or antennas, North America	MA3-17001200-NNA	\$1,682.10
5642693	3-yr NetCloud Mobile Essentials Plan and IBR900 router with WiFi (1000Mbps modem), no AC power supply or antennas, North America	MA3-09001200-NNA	\$1,123.20

**Note:** NetCloud functions vary for FIPS Hardware enabled devices. Consult the Cradlepoint website for specifics. . Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. These hardware bundles can be used with 4G Mobile Broadband, Machine to Machine, and Public Safety Mobile Broadband Price Plans. A data plan is required for each modem purchase. There are no returns or exchanges and no Proration's. Reference Cradlepoint terms of service attached hereto.

LTE Vehicle Internet			
These Accessories Sku's are not eligible for further discounts.			
SKU#	Description	OEM P/N	Price
4765224	COR IBR1700, IBR900 power supply North America	170716-000	\$22.49
3715571	Dual-band 2.4/5.0 GHz external WiFi antenna for AER3100, AER2100, IBR900, IBR1100 (1X)	170628-000	\$13.49
5427545	Black, Universal 600MHz-6GHz 3G/4G/LTE 2dBi/3dBi 6 in antenna with SMA connector (1x)	170760-000	\$13.49
3774498	Vehicle power adapter for COR	170635-000	\$22.49
5503087	3 meter power and GPIO cable (direct wire) for IBR1700, IBR9x0	170585-001	\$13.04
4381062	Serial DB9 to GPIO cable, 3 meters	170676-000	\$16.19
4979362	Panorama antenna 5IN1 Blk dome 2LTE 2WIFI 1GPS	LP-IN1958-B	\$283.78
4979363	Panorama antenna 5IN1 Wht dome 2LTE 2WIFI 1GPS	LP-IN1958-W	\$283.78
5166824	Panorama antenna 9IN1 Blk dome 4LTE 4WIFI 1GPS	LG-IN2293-B	\$461.83
5166826	Panorama antenna 9IN1 Wht dome 4LTE 4WIFI 1GPS	LG-IN2293-W	\$461.83

**Note:** There are no returns or exchanges. Accessories can be purchased separately from hardware bundles. Reference Panorama Antenna terms attached hereto.

### LTE Business Internet 10 Mbps Speed Tier Machine-to-Machine Plans\*

These plans are eligible for monthly access fee discounts.

	\$70.00 (41121)	\$90.00 (41135)	\$140.00 (41205)	\$190.00 (41212)
<b>Monthly Access Fee<sup>1</sup></b>				
<b>Speed Tier Limit (Up to)<sup>2</sup></b>	10 Mbps	10 Mbps	10 Mbps	10 Mbps
<b>Data Deprioritization Threshold<sup>3</sup></b>	25 GB	50 GB	100 GB	150 GB
<b>Data Throughput Limit Threshold<sup>4</sup></b>	50 GB	100 GB	200 GB	300 GB
<b>Throttled Speed (Up to)</b>	600 Kbps	600 Kbps	600 Kbps	600 Kbps

**Notes:** These plans are restricted to the Verizon Wireless 4G network (domestic and international roaming are not available). Only select Customer-provided 4G data routers can be activated on these plans. <sup>1</sup>The monthly access fee will not be pro-rated when moving to a higher speed tier plan during a billing cycle (the higher access fee will be billed); a line cannot move to a lower speed tier during a billing cycle. <sup>2</sup>Speeds represent the maximum speed but may be lower in the event of network congestion. <sup>3</sup>After the data deprioritization threshold is met on a line during any billing cycle, usage may be prioritized behind other customers in the event of network congestion. <sup>4</sup>If the data throughput limit threshold is exceeded on any line in any given billing cycle, Verizon Wireless will limit the data throughput speeds for additional usage for the remainder of the then-current billing cycle for the line that exceeds the data usage to the applicable throttled speed. Voice calls cannot be placed or received on these plans other than to 611 or 911 (these calls may be placed anywhere in the Nationwide Rate and Coverage Area). If the voice block feature is removed, there will be a \$0.25 per minute charge for voice calls. Text messages cannot be sent or received on these plans. If the text message block feature is removed, there will be a \$0.20 per message charge for messages sent or received. These plans can be used for point-of-sale, mobile terminal, and business productivity applications. Prohibited applications include, but are not limited to, continuously streaming video, web hosting, and public/guest Wi-Fi systems without prior approval from Verizon Wireless. \*These plans are for machine-to-machine service ("M2M Service"). "M2M Service" refers to use of the Wireless Service for the transmission of data between wireless devices and computer servers or other machines, or between wireless devices, with limited or no manual intervention or supervision.

### Single Basic Phone Unlimited Talk Plus 500MB Plan

Government Subscribers Only

No Domestic Roaming or Long Distance Charges

This plan is NOT eligible for monthly access fee discounts.

<b>Monthly Access Fee</b>	\$30.00
<b>Monthly Anytime Minutes</b>	Unlimited
<b>BPC Data Rate 500 MB</b>	\$10.00 per GB

**Notes:** Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). \*May only be activated on a Verizon Wireless Home Phone Approved Device (BPC100). This is not a Home Phone Service. This service is generally utilized to replace POTS lines.

### Custom wireless Home Phone Connect Plan

Government Subscribers Only

No Domestic Roaming or Long Distance Charges

This plan is NOT eligible for monthly access fee discounts.

<b>Monthly Access Fee</b>	\$20.00
<b>Monthly Anytime Minutes</b>	Unlimited

**Notes:** Current coverage details and additional plan information can be found at [www.verizonwireless.com](http://www.verizonwireless.com). Activation on this phone requires a separate billing account. Activations on this plan are limited to no more than 9 lines per account. \*May only be activated on a Verizon Wireless Home Phone Approved Device. This is not a Home Phone Service. This service is generally utilized to replace POTS lines. Wireless Home Phone is not compatible with any data applications.

## PUBLIC SAFETY CUSTOM PLANS

### Custom 4G Unlimited Smartphone Plan with Mobile Broadband Priority and Preemption for National Security, Public Safety, and Emergency Preparedness

Government Liable Subscribers Only.

**This plan is not eligible for monthly access fee discounts.**

#### Mission Critical

Only 4G LTE GSM/UMTS global-capable smartphones can be activated on this plan.

<b>Monthly Access Fee</b>	<b>\$39.99</b>
<b>Monthly Minutes in U.S</b>	Unlimited
<b>Domestic Data Allowance<sup>(1)</sup></b>	Unlimited
<b>Domestic Messaging Allowance</b>	Unlimited
<b>Optional Features</b>	
<b>Domestic Mobile Hotspot</b>	\$5.00 additional per month
<b>Push-to-Talk</b>	\$2.00 additional per month

**Notes:** . No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. <sup>(1)</sup> Data usage on this rate plan is not subject to speed reductions ("throttling") within a given billing cycle. However, in the event a user consumes more than 25GB each billing cycle for three (3) consecutive billing cycles, data throughput speeds will automatically be reduced for data usage exceeding 25GB per billing cycle on a go-forward basis. Data usage for actively engaged and deployed fire, police, emergency medical technicians, emergency management agency, and assigned federal law enforcement users on this plan will not be subject to speed reductions regardless of data usage during any billing cycle. To ensure users are able to maximize their high-speed data use for business applications, video applications will stream at 480p. This service plan includes Mobile Broadband Priority and Preemption. Mobile Broadband Priority ensures customers can connect to the network with priority by leveraging a pool of radio resources dedicated to enable their connection. Mobile Broadband Priority identifies the user with an Access Priority setting, giving them higher priority for network access than lower Access Class users. Preemption automatically activates to provide approved personnel uninterrupted access to the network in those uncommon times when the network is fully utilized. 911 calls are never preempted. This service plan is available to National Security, Public Safety, and Emergency Preparedness customers only as defined by the following NAICS (formerly SIC) Codes\*: (PP# 16807)

621910 Ambulance Services	923120 Administration of Public Health Programs
922110 Courts	928110 National Security
922120 Police Protection	926120 Regulation and Administration of Transportation Programs
922130 Legal Counsel and Prosecution	926150 Regulation, Licensing, and Inspection of Misc. Commercial Sectors
922140 Correctional Institutions	926130 Regulation and Administration of Comms, Electric, Gas, and Other Utilities
922150 Parole Offices and Probation Offices	921150 American Indian and Alaska Native Tribal Governments
922160 Fire Protection (except private)	921190 Other General Government Support
922190 Other Justice, Public Order, and Safety Activities	921110 Executive Offices

\*Standard Industrial Classification (SIC) and North American Industrial Classification System (NAICS) codes identify an entity's primary business activity.

## Custom Unlimited Basic Phone Plan for National Security, Public Safety, and Emergency Preparedness

Government Liable Subscribers Only

**This plan is not eligible for monthly access fee discounts.**

This Public Safety Plan does not provide a Mission Critical service standard.

<b>Monthly Access Fee</b>	<b>\$22.99</b>
<b>Monthly Minutes in U.S</b>	Unlimited
<b>Domestic Data Allowance</b>	100MB
<b>Domestic Messaging Allowance</b>	Unlimited
<b>Domestic Data Overage</b>	\$10.00 per GB

**Notes:** . No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. This service plan is available to National Security, Public Safety, and Emergency Preparedness customers only as defined by the following NAICS (formerly SIC) Codes\*: (PP# 16810)

621910 Ambulance Services	923120 Administration of Public Health Programs
922110 Courts	928110 National Security
922120 Police Protection	926120 Regulation and Administration of Transportation Programs
922130 Legal Counsel and Prosecution	926150 Regulation, Licensing, and Inspection of Misc. Commercial Sectors
922140 Correctional Institutions	926130 Regulation and Administration of Comms, Electric, Gas, and Other Utilities
922150 Parole Offices and Probation Offices	921150 American Indian and Alaska Native Tribal Governments
922160 Fire Protection (except private)	921190 Other General Government Support
922190 Other Justice, Public Order, and Safety Activities	921110 Executive Offices

\*Standard Industrial Classification (SIC) and North American Industrial Classification System (NAICS) codes identify an entity's primary business activity.

## Custom Unlimited Push to Talk Only Plan for National Security, Public Safety, and Emergency Preparedness

Government Liable Subscribers Only.

**This plan is not eligible for monthly access fee discounts.**

This Public Safety Plan does not provide a Mission Critical service standard.

<b>Monthly Access Fee</b>	<b>\$17.99</b>
<b>Monthly Push to Talk Minutes</b>	Unlimited
<b>Domestic Voice Per Minute Rate</b>	\$0.25
<b>Notes:</b> No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. This service plan is available to National Security, Public Safety, and Emergency Preparedness customers only as defined by the following NAICS (formerly SIC) Codes*: (PP#96625/4G Only – PP#96625 3G/4G)	
621910 Ambulance Services 922110 Courts 922120 Police Protection 922130 Legal Counsel and Prosecution 922140 Correctional Institutions 922150 Parole Offices and Probation Offices 922160 Fire Protection (except private) 922190 Other Justice, Public Order, and Safety Activities	923120 Administration of Public Health Programs 928110 National Security 926120 Regulation and Administration of Transportation Programs 926150 Regulation, Licensing, and Inspection of Misc. Commercial Sectors 926130 Regulation and Administration of Comms, Electric, Gas, and Other Utilities 921150 American Indian and Alaska Native Tribal Governments 921190 Other General Government Support 921110 Executive Offices

\*Standard Industrial Classification (SIC) and North American Industrial Classification System (NAICS) codes identify an entity's primary business activity.

## Mobile Broadband Priority Feature for National Security, Public Safety, and Emergency Preparedness

Government Liable Subscribers Only.

### Mission Critical

<b>Monthly Access Fee</b>	<b>\$0.00</b>
<b>Mobile Broadband Priority</b> ensures customers can connect to the network with priority by leveraging a pool of radio resources dedicated to enable their connection. Mobile Broadband Priority identifies the user with an Access Priority setting, giving them higher priority for network access than lower Access Class users. This feature is available to National Security, Public Safety, and Emergency Preparedness customers only as defined by the following NAICS (formerly SIC) Codes*: (PP#86124)	
621910 Ambulance Services 922110 Courts 922120 Police Protection 922130 Legal Counsel and Prosecution 922140 Correctional Institutions 922150 Parole Offices and Probation Offices 922160 Fire Protection (except private) 922190 Other Justice, Public Order, and Safety Activities	923120 Administration of Public Health Programs 928110 National Security 926120 Regulation and Administration of Transportation Programs 926150 Regulation, Licensing, and Inspection of Misc. Commercial Sectors 926130 Regulation and Administration of Comms, Electric, Gas, and Other Utilities 921150 American Indian and Alaska Native Tribal Governments 921190 Other General Government Support 921110 Executive Offices

\*Standard Industrial Classification (SIC) and North American Industrial Classification System (NAICS) codes identify an entity's primary business activity.

## Custom 4G Unlimited Mobile Broadband Plan with Mobile Broadband Priority and Preemption for National Security, Public Safety, and First Responders

Government Liable Subscribers Only.

This plan is not eligible for monthly access fee discounts.

### Mission Critical

Only 4G LTE GSM/UMTS global-capable devices can be activated on this plan.

<b>Monthly Access Fee</b>	<b>\$36.05</b>
<b>Domestic Data Allowance<sup>(1)</sup></b>	Unlimited

**Notes:** . No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Data usage on this plan is restricted to Verizon Wireless network use only; roaming is not available. <sup>(1)</sup> Data usage on this rate plan is not subject to speed reductions (“throttling”) within a given billing cycle. However, in the event data usage exceeds 25GB each billing cycle for three (3) consecutive billing cycles, data throughput speeds will automatically be reduced for data usage exceeding 25GB per billing cycle on a go-forward basis. Data usage for actively engaged and deployed fire, police, emergency medical technicians, emergency management agency, and assigned federal law enforcement users on this plan will not be subject to speed reductions regardless of data usage during any billing cycle. To ensure users are able to maximize their high-speed data use for business applications, video applications will stream at 720p. This service plan includes Mobile Broadband Priority and Preemption. Mobile Broadband Priority ensures customers can connect to the network with priority by leveraging a pool of radio resources dedicated to enable their connection. Mobile Broadband Priority identifies the user with an Access Priority setting, giving them higher priority for network access than lower Access Class users. Preemption automatically activates to provide approved personnel uninterrupted access to the network in those uncommon times when the network is fully utilized. 911 calls are never preempted. Devices utilized in conjunction with this plan are limited to mobile device applications. Dedicated internet connections (including but not limited to, stationary wireless networking router devices), streaming video on non-smartphone devices (including but not limited to, body cameras and stationary video surveillance cameras), and Internet of Things (“IoT”) devices\* are expressly prohibited on this rate plan. This plan is only available to National Security, Public Safety, and First Responder customers only as defined by the following NAICS (formerly SIC) Codes\*\*:

621910 Ambulance Services 922110 Courts 922120 Police Protection 922130 Legal Counsel and Prosecution 922140 Correctional Institutions 922150 Parole Offices and Probation Offices 922160 Fire Protection (except private) 922190 Other Justice, Public Order, and Safety Activities	923120 Administration of Public Health Programs 928110 National Security 926120 Regulation and Administration of Transportation Programs 926150 Regulation, Licensing, and Inspection of Misc. Commercial Sectors 926130 Regulation and Administration of Comms, Electric, Gas, and Other Utilities 921150 American Indian and Alaska Native Tribal Governments 921190 Other General Government Support 921110 Executive Offices
---	---

\*Internet of Things (“IoT”) devices. Devices other than smartphones, aircards, jetpacks, modems, and tablets that transfer data over the network (e.g. M2M).

\*\*Standard Industrial Classification (SIC) and North American Industrial Classification System (NAICS) codes identify an entity’s primary business activity.

## Verizon Wireless Preemption Service Feature for National Security, Public Safety, and First Responders

Government Liable Subscribers Only,

### Mission Critical

Monthly Access Fee Per MDN

**\$0.00**

**NOTE:** Preemption Service ("Preemption") is a capability that reallocates network resources to customers so that they can connect in emergencies. In those uncommon times when the network is fully utilized, Preemption automatically activates to provide approved personnel uninterrupted access to the network. It helps ensure our national security, public safety, and first responder customers can continue to communicate with each other during times of high network use. Preemption capability is available on the Verizon Wireless 3G and 4G LTE data network. While Preemption capability may also be available on the networks of Verizon Wireless's domestic roaming partners, Verizon Wireless makes no representation of Preemption availability or reliability on such networks. Preemption is limited to select service rate plans and cannot be used in conjunction with devices or service plans utilized with dedicated internet connections (including but not limited to, stationary wireless networking router devices), streaming video on non-smartphone devices (including but not limited to, body cameras and stationary video surveillance cameras), and IoT devices are expressly prohibited from using this feature. Please note: Calls to 911 are never preempted. This feature is available to National Security, Public Safety, and First Responder customers only as defined by the following NAICS (formerly SIC) Codes: (PP# 86428 Basic/Smart Phone and 86433 Non-Phone)

621910 Ambulance Services	923120 Administration of Public Health Programs
922110 Courts	928110 National Security
922120 Police Protection	926120 Regulation and Administration of Transportation Programs
922130 Legal Counsel and Prosecution	926150 Regulation, Licensing, and Inspection of Commercial Sectors
922140 Correctional Institutions	926130 Regulation and Administration of Comms, Electric, Gas, Utilities
922150 Parole Offices and Probation Offices	921150 American Indian and Alaska Native Tribal Governments
922160 Fire Protection (except private)	921190 Other General Government Support
922190 Other Justice, Public Order, and Safety Activities	921110 Executive Offices

## Private Responder Core Service for National Security, Public Safety, and Emergency Preparedness

Government Liable Subscribers Only.

### Mission Critical

<b>Monthly Access Fee</b>	<b>\$0.00</b>
<p><b>Verizon Wireless Private Responder Core Service for National Security, Public Safety, and Emergency Preparedness ("Private Core"):</b> Private Core extends Customer's IP network to its wireless equipment by segregating the data between such devices and Customer's servers from the public Internet (the "Internet"). This service is available to National Security, Public Safety, and Emergency Preparedness customers only as defined by the following NAICS (formerly SIC) Codes*:</p>	
<p><b>National Security/ First Responders / Public Safety</b></p> <ul style="list-style-type: none"> <li>• 621910 Ambulance Service</li> <li>• 922110 Courts</li> <li>• 922120 Police Protection</li> <li>• 922130 Legal Counsel and Prosecution</li> <li>• 922140 Correctional Institutions</li> <li>• 922150 Parole Offices and Probation Offices</li> <li>• 922160 Fire Protection (except private)</li> <li>• 922190 Other Justice, Public Order and Safety Activities</li> <li>• 928110 National Security</li> <li>• 921190 Other General Government Support</li> <li>• 921110 Executive Offices</li> <li>921150 American Indian/Alaska Native Tribal Governments</li> </ul> <p><b>Water</b></p> <ul style="list-style-type: none"> <li>• 924110 Water Infrastructure</li> <li>• 221320 Sewage Treatment Facilities</li> <li>• 221310 Water Supply and Irrigation Systems</li> </ul> <p><b>Transportation</b></p> <ul style="list-style-type: none"> <li>• 482111 Railway Transportation</li> <li>• 481111 Passenger Air Transportation</li> <li>• 481112 Freight Air Transportation</li> <li>• 483111 Shipping Transportation</li> <li>• 926120 Transportation Administration</li> <li>• 491110 Postal Service</li> <li>• 926120 Public Transportation</li> <li>• 926120 Regulation and Administration of Transportation Programs</li> </ul> <p><b>Information Technology</b></p> <ul style="list-style-type: none"> <li>• 541512 Computer Integration</li> <li>• 541519 Computer Disaster Recovery</li> </ul>	<p><b>Chemical</b></p> <ul style="list-style-type: none"> <li>• 561612 Protective Services</li> <li>• 541330, 541690 Chemical Engineering and Consulting</li> <li>• 239210 Pharmaceutical</li> </ul> <p><b>Communications</b></p> <ul style="list-style-type: none"> <li>• 517110 Telecommunications, Wired</li> <li>• 517212 Cellular and other Wireless Telecommunications</li> <li>• 238210, 334290 and 561620 Alarm Systems</li> </ul> <p><b>Critical Manufacturing</b></p> <ul style="list-style-type: none"> <li>• 237310 Highway, Street and Bridge Construction</li> <li>• 811310 Industry Equipment Repair</li> <li>• 236210 Industrial Building Construction</li> <li>• 211113 Extraction; 236220 Construction Management</li> <li>• 926150 Regulation, Licensing and Inspection of Miscellaneous Commercial Sectors</li> </ul> <p><b>Energy</b></p> <ul style="list-style-type: none"> <li>• 333611 Wind Turbine</li> <li>• 221111 Hydroelectric Power Generation</li> <li>• 221122 Electric Power Distribution</li> <li>• 221118 Other Electric Power Generation</li> <li>• 221210 Natural Gas Distribution</li> <li>• 926130 Regulation and Administration of Communications, Electric, Gas and Other Utilities</li> <li>• 221113 Nuclear Electric Power Generation</li> <li>• 562211 Hazardous Waste Treatment and Disposal</li> </ul> <p><b>Healthcare and Public Health</b></p> <ul style="list-style-type: none"> <li>• 621112 Health Care Practitioners</li> <li>• 923120 Public Health Programs</li> </ul>

\*Standard Industrial Classification (SIC) and North American Industrial Classification System (NAICS) codes identify an entity's primary business activity.

## 4G LTE Private Network Traffic Management (PNTM) Private IP Only (fixed WAN) Government Subscribers Only

Metered Data Pricing only. Not compatible with Unlimited Data Plans.

### Mission Critical

The plans below reflect any applicable discount. No additional discounts apply.

<b>Class of service ("CoS")</b>	Customer can allocate bandwidth for applications into the Mission Critical CoS according to the PNTM Service Option selected.
<b>Mission Critical CoS Applications</b>	Recommended for video, Voice over IP, interactive services, and other mission critical applications.
<b>Best Effort CoS Applications</b>	Suitable for best effort applications (e.g. email, web browsing)

PNTM Service Options:	Enhanced (Entry Level)	Premium (Mid Level)	Public Safety (Highest Level) <small>(Qualifying Public Safety NAICS Only)</small>
Monthly Access Fee (per line)	Waived - \$0.00	Waived - \$0.00	Waived - \$0.00
Mission Critical CoS Speeds	Mapped Up to 0.5 Mbps	Mapped Up to 2 Mbps	Mapped Up to 2 Mbps
Best Effort CoS Applications Speeds	Remaining available 4G LTE bandwidth	Remaining available 4G LTE bandwidth	Remaining available 4G LTE bandwidth
RF Priority on access network	N/A	N/A	During heavy network usage periods

**Qualifying Public Safety NAICS:** Public Safety Subscribers classified with the following NAICS codes\*, performing First Responder responsibilities only. The Public Safety PNTM service option is not an on demand service. The Public Safety PNTM must be provisioned on the account prior to use in the event of an emergency situation.

621910 Ambulance Services	928110 National Security
922110 Courts	926120 Regulation and Administration of Transportation Programs
922120 Police Protection	926150 Regulation, Licensing, and Inspection of Misc. Commercial Sectors
922130 Legal Counsel and Prosecution	926130 Regulation and Administration of Comms, Electric, Gas, and Other Utilities
922140 Correctional Institutions	921150 American Indian/Alaska Native Tribal Governments
922150 Parole Offices and Probation Offices	921190 Other General Government Support
922160 Fire Protection (except private)	921110 Executive Offices
922190 Other Justice, Public Order, and Safety Activities	

Notes. 4G LTE Private Network subscribers with unlimited data plans are ineligible for Private Network Traffic Management. This service is only available while on Verizon Wireless' 4G network and is not available while roaming. VZ Private IP (MPLS) connectivity required. PNTM relies on customer's applications (VoIP, video, etc.) to appropriately mark IP sessions in order to prioritize their application over the 4G LTE Private Network using Internet Protocol Differentiated Services Code Point (IP DSCP). PNTM 4G LTE device must be certified for use on the Verizon Wireless network (e.g. Open Development/Open Access certified, validated for Private Network and Private Network Traffic Management.)

\* North American Industrial Classification System (NAICS) codes identify an entity's primary business activity.

**DNS Safeguard Plus Feature for Public Safety  
National Security, Public Safety, and First Responders  
Government Liable Subscribers Only**

**Mission Critical**

These features are not eligible for access discounts.

**DNS Safeguard Plus Feature for Public Safety** is a network feature that will provide enhanced Domain Name Service (DNS) security for Responder Private Core customers to proactively detect and prevent cyberattacks.

Code	Description	Device Provisioning	Monthly Access Fee
87898	DNS Safe Guard Plus RPC PS	Android and other OS devices only (Non-Apple).Provisions PSINTERNET and DNS Security Plus	\$0.00
87901	DNS Safe Guard Plus RPC PS APPLE	Apple Devices only (Smartphones and tablets). Provisions PSINTERNET and DNS Security Plus.	\$0.00

**Note:** These features are stacked with Responder Private Core Internet Access Core as a mandatory feature. The DNS Safeguard Plus features are not compatible with Wireless Private Network, Private Network Traffic Management, or One Talk. These features are open to all plans and devices as allowed with Responder Private Core Internet Access Core.

These features are available to National Security, Public Safety, and First Responder customers only as defined by the following NAICS (formerly SIC) Codes:

<p><b>National Security/ First Responders / Public Safety</b></p> <ul style="list-style-type: none"> <li>• 485111 Mixed Mode Transit Systems (Rail &amp; Buses)</li> <li>• 485112 Commuter Rail Systems</li> <li>• 621910 Ambulance Services</li> <li>• 922110 Courts</li> <li>• 922120 Police Protection</li> <li>• 922130 Legal Counsel and Prosecution</li> <li>• 922140 Correctional Institutions</li> <li>• 922150 Parole Offices and Probation Offices</li> <li>• 922160 Fire Protection (except private)</li> <li>• 922190 Other Justice, Public Order, and Safety Activities</li> <li>• 923120 Administration of Public Health Programs</li> </ul>	<ul style="list-style-type: none"> <li>• 928110 National Security</li> <li>• 926120 Regulation and Administration of Transportation Programs</li> <li>• 926150 Regulation, Licensing, and Inspection of Commercial Sectors</li> <li>• 926130 Regulation and Administration of Comms, Electric, Gas, Utilities</li> <li>• 921150 American Indian and Alaska Native Tribal Governments</li> <li>• 921190 Other General Government Support</li> <li>• 921110 Executive Offices</li> </ul>
--	--

**DNS Safeguard Plus Feature for Public Sector  
National Security, Public Safety, and First Responders  
Government Liable Subscribers Only**

## Mission Critical

**DNS Safeguard Plus Feature for Public Sector** is a network feature that will provide enhanced Domain Name Service (DNS) security for Responder Private Core customers to proactively detect and prevent cyberattacks.

Code	Description	Device Provisioning	Monthly Access Fee
87896	DNS Safe Guard Plus RPC PS	Android and other OS devices only (Non-Apple).Provisions PSINTERNET and DNS Security Plus	\$1.25
87900	DNS Safe Guard Plus RPC PS APPLE	Apple Devices only (Smartphones and tablets). Provisions PSINTERNET and DNS Security Plus.	\$1.25

**Note:** These features are stacked with Responder Private Core Internet Access Core as a mandatory feature. The DNS Safeguard Plus features are not compatible with Wireless Private Network, Private Network Traffic Management, or One Talk. These features are open to all plans and devices as allowed with Responder Private Core Internet Access Core.

These features are available to National Security, Public Safety, and First Responder customers only as defined by the following NAICS (formerly SIC) Codes:

<p><b>Water</b> 924110 Water Infrastructure 221320 Sewage Treatment Facilities 221310 Water Supply and Irrigation Systems</p> <p><b>Transportation</b> 482111 Railway Transportation 481111 Passenger Air Transportation 481112 Freight Air Transportation 483111 Shipping Transportation 491110 Postal Service</p> <p><b>Information Technology</b> 541512 Computer Integration 541519 Computer Disaster Recovery</p> <p><b>Chemical</b> 561612 Protective Services 541330, 541690 Chemical Engineering and</p> <p><b>Consulting</b> 239210 Pharmaceutical</p> <p><b>Communications</b> 517110 Telecommunications, Wired 517212 Cellular and other Wireless</p>	<p><b>Telecommunications</b> 238210, 334290 and 561620 Alarm Systems</p> <p><b>Critical Manufacturing</b> 237310 Highway, Street and Bridge Construction 811310 Industry Equipment Repair 236210 Industrial Building Construction 211113 Extraction; 236220 Construction Management</p> <p><b>Energy</b> 333611 Wind Turbine 221111 Hydroelectric Power Generation 221122 Electric Power Distribution 221118 Other Electric Power Generation 221210 Natural Gas Distribution 221113 Nuclear Electric Power Generation 562211 Hazardous Waste Treatment and Disposal</p> <p><b>Healthcare and Public Health</b> 621112 Health Care Practitioners 923120 Public Health Programs</p>
--	---

**DNS Safeguard Advance Feature for Public Safety and Public Sector  
National Security, Public Safety, and First Responders  
Government Liable Subscribers Only**

## Mission Critical

**DNS Safeguard Advance Feature for Public Sector** is a network feature that will provide enhanced Domain Name Service (DNS) security for Responder Private Core customers to proactively detect and prevent cyberattacks.

Code	Description	Device Provisioning	Monthly Access Fee
87897	DNS Safe Guard Adv RPC	Android and Other OS Devices only (Non-Apple) Smartphones, Tablets, Routers, Modems, etc. Provisions PSINTERNET and DNS Security Advanced.	\$2.00
87899	DNS Safe Guard Adv RPC APPL	Apple Devices only (Smartphones and tablets). Provisions PSINTERNET and DNS Security Advanced.	\$2.00

**Note:** These features are stacked with Responder Private Core Internet Access Core as a mandatory feature. The DNS Safeguard Advance features are not compatible with Wireless Private Network, Private Network Traffic Management, or One Talk. These features are open to all plans and devices as allowed with Responder Private Core Internet Access Core.

These features are available to National Security, Public Safety, and First Responder customers only as defined by the following NAICS (formerly SIC) Codes:

<p><b>National Security/ First Responders / Public Safety</b></p> <ul style="list-style-type: none"> <li>621910 Ambulance Service</li> <li>922110 Courts</li> <li>922120 Police Protection</li> <li>922130 Legal Counsel and Prosecution</li> <li>922140 Correctional Institutions</li> <li>922150 Parole Offices and Probation Offices</li> <li>922160 Fire Protection (except private)</li> <li>922190 Other Justice, Public Order and Safety Activities</li> <li>928110 National Security</li> <li>921190 Other General Government Support</li> <li>921110 Executive Offices</li> <li>921150 American Indian/Alaska Native Tribal Governments</li> </ul> <p><b>Water</b></p> <ul style="list-style-type: none"> <li>924110 Water Infrastructure</li> <li>221320 Sewage Treatment Facilities</li> <li>221310 Water Supply and Irrigation Systems</li> </ul> <p><b>Transportation</b></p> <ul style="list-style-type: none"> <li>482111 Railway Transportation</li> <li>481111 Passenger Air Transportation</li> <li>481112 Freight Air Transportation</li> <li>483111 Shipping Transportation</li> <li>926120 Transportation Administration</li> <li>491110 Postal Service</li> </ul> <p><b>Public Transportation</b></p> <ul style="list-style-type: none"> <li>926120 Regulation and Administration of Transportation Programs</li> <li>485111 Mixed Mode Transit Systems (Rail &amp; Buses)</li> <li>485112 Commuter Rail Systems</li> </ul> <p><b>Information Technology</b></p> <ul style="list-style-type: none"> <li>541512 Computer Integration</li> <li>541519 Computer Disaster Recovery</li> </ul>	<p><b>Chemical</b></p> <ul style="list-style-type: none"> <li>561612 Protective Services</li> <li>541330, 541690 Chemical Engineering and Consulting</li> <li>239210 Pharmaceutical</li> </ul> <p><b>Communications</b></p> <ul style="list-style-type: none"> <li>517110 Telecommunications, Wired</li> <li>517212 Cellular and other Wireless <b>Telecommunications</b></li> <li>238210, 334290 and 561620 Alarm Systems</li> <li>Critical Manufacturing</li> <li>237310 Highway, Street and Bridge Construction</li> <li>811310 Industry Equipment Repair</li> <li>236210 Industrial Building Construction</li> <li>211113 Extraction</li> <li>236220 Construction</li> </ul> <p><b>Management</b></p> <ul style="list-style-type: none"> <li>926150 Regulation, Licensing and Inspection of Miscellaneous Commercial Sectors</li> </ul> <p><b>Energy</b></p> <ul style="list-style-type: none"> <li>333611 Wind Turbine</li> <li>221111 Hydroelectric Power Generation</li> <li>221122 Electric Power Distribution</li> <li>221118 Other Electric Power Generation</li> <li>221210 Natural Gas Distribution</li> <li>926130 Regulation and Administration of Communications, Electric, Gas and Other Utilities</li> <li>221113 Nuclear Electric Power Generation</li> <li>562211 Hazardous Waste Treatment and Disposal</li> </ul> <p><b>Healthcare and Public Health</b></p> <ul style="list-style-type: none"> <li>621112 Health Care Practitioners</li> <li>923120 Public Health Programs</li> </ul>
---	---

**Push To Talk Responder  
Public Safety**

**Mission Critical**

<b>Product Description</b>	<b>Monthly Access</b>	<b>Notes</b>
Push to Talk Responder Service Voice Only <sup>1</sup> (87911)	\$12.00 per month	Calls will not be rated
<b>Optional Feature Must be added with above if selected</b>		
Push to Talk Responder with Interoperability <sup>2</sup> (87694)	\$10.00 per month	Calls will not be rated
<b>Software</b>		
Push to Talk Responder licenses are not eligible for any further discounts.		

Dispatch SW License	VZMCPTDISPCLSW	\$3,000 per chair	One time charge
---------------------	----------------	-------------------	-----------------

**Note:** Coverage includes the Verizon Wireless 4G network only. Usage outside of the United States is not supported. Lines activating on these plans must be on 4G HD voice-capable smartphones. **^Lines will need to add the Responder Private Core Internet APN Feature code to be on Push to Talk Responder.**

Push to Talk Responder users have the capability to make PTT calls, video calls, send and receive message and send/receive data files via the Push to Talk Responder application. Push to Talk Responder services will be charged based on the type of services the user is using as follows:

1. Push to Talk Responder service voice only can be added to any Smartphone plan as a stand-alone feature.

**Public Safety NAICS Codes:**

485111 Mixed Mode Transit Systems (Rail & Buses)	922190 Other Justice, Public Order, and Safety Activities
485112 Commuter Rail Systems	923120 Administration of Public Health Programs
621910 Ambulance Services	928110 National Security
922110 Courts	926120 Regulation and Administration of Transportation Programs
922120 Police Protection	926150 Regulation, Licensing, and Inspection of Commercial Sectors
922130 Legal Counsel and Prosecution	926130 Regulation and Administration of Comms, Electric, Gas, Utilities
922140 Correctional Institutions	921150 American Indian and Alaska Native Tribal Governments
922150 Parole Offices and Probation Offices	921190 Other General Government Support
922160 Fire Protection (except private)	921110 Executive Offices

**\*\*These features cannot be used with any other Push to Talk Plus plans or features\*\***

**Push To Talk Responder  
Public Sector Customers (extended NAICS Codes)**

**Mission Critical**

<b>Product Description</b>	<b>Monthly Access</b>	<b>Notes</b>
Push to Talk Responder Service Voice Only <sup>1</sup>	\$15.00 per month	Calls will not be rated

Optional Feature Must be added with above if selected

Push to Talk Responder with Interoperability <sup>2</sup>	\$10.00 per month	Calls will not be rated
<b>Software</b>		
Push to Talk Responder license are not eligible for any further discounts.		
Dispatch SW License	VZMCPTTDISPCLSW	\$3,000 per chair
One time charge		
<p><b>Note:</b> Coverage includes the Verizon Wireless 4G network only. Usage outside of the United States is not supported. Lines activating on these plans must be on 4G HD voice-capable smartphones.</p> <p>^ As a condition for accessing and using Push to Talk Responder, the Purchasing Entity must have authorized access from Verizon to use Responder Private Core Internet Access.</p> <p>Push to Talk Responder users have the capability to make PTT calls, video calls, send and receive message and send/receive data files via the Push to Talk Responder application. Push to Talk Responder services will be charged based on the type of services the user is using as follows:</p> <ol style="list-style-type: none"> <li>1. Push to Talk Responder service w/o video can be added to any Smartphone plan as a stand-alone feature.</li> <li>2. Push to Talk Responder Interoperability calls cannot be stand-alone features with any Smartphone plan. They must be added with the Push to Talk Responder service w/o video.</li> </ol> <p><b>**These features cannot be used with any other Push to Talk Plus plans or features**</b></p> <p><b>Customers must be on the below qualifying NAICS Codes:</b></p>		
<p><b>Water</b></p> <ul style="list-style-type: none"> <li>• 924110 Water Infrastructure</li> <li>• 221320 Sewage Treatment Facilities</li> <li>• 221310 Water Supply and Irrigation Systems</li> </ul> <p><b>Transportation</b></p> <ul style="list-style-type: none"> <li>• 482111 Railway Transportation</li> <li>• 481111 Passenger Air Transportation</li> <li>• 481112 Freight Air Transportation</li> <li>• 483111 Shipping Transportation</li> <li>• 926120 Transportation Administration</li> <li>• 491110 Postal Service</li> <li>• 926120 Public Transportation</li> </ul> <p><b>Information Technology</b></p> <ul style="list-style-type: none"> <li>• 541512 Computer Integration</li> <li>• 541519 Computer Disaster Recovery</li> </ul> <p><b>Healthcare and Public Health</b></p> <ul style="list-style-type: none"> <li>• 621112 Health Care Practitioners</li> </ul>	<p><b>Chemical</b></p> <ul style="list-style-type: none"> <li>• 561612 Protective Services</li> <li>• 541330, 541690 Chemical Engineering and Consulting</li> <li>• 239210 Pharmaceutical</li> </ul> <p><b>Communications</b></p> <ul style="list-style-type: none"> <li>• 517110 Telecommunications, Wired</li> <li>• 517212 Cellular and other Wireless Telecommunications</li> <li>• 238210, 334290 and 561620 Alarm Systems</li> </ul> <p><b>Critical Manufacturing</b></p> <ul style="list-style-type: none"> <li>• 237310 Highway, Street and Bridge Construction</li> <li>• 811310 Industry Equipment Repair</li> <li>• 236210 Industrial Building Construction</li> <li>• 211113 Extraction; 236220 Construction Management</li> </ul> <p><b>Energy</b></p> <ul style="list-style-type: none"> <li>• 333611 Wind Turbine</li> <li>• 221111 Hydroelectric Power Generation</li> <li>• 221122 Electric Power Distribution</li> <li>• 221118 Other Electric Power Generation</li> <li>• 221210 Natural Gas Distribution</li> <li>• 221113 Nuclear Electric Power Generation</li> <li>• 562211 Hazardous Waste Treatment and Disposal</li> </ul>	

Group First Response provides the next tier, in terms of Push To Talk features. Specifically it allows, fast setup time, ability to handle very large groups, and a strong security and priority handling. Group First Response is based on international 3GPP standards (Mission Critical Push To Talk (MCPTT)) that ensures that the user gets “LMR like” features

**Group First Response for  
National Security, Public Safety, and First Responders  
Government Subscribers Only**

**Mission Critical**

Features \$25.00 and above are eligible for monthly access discounts.

Description	Feature Code	Monthly Access Fee
^Group First Response <sup>1</sup>	87781	\$35.00
Push to Talk Plus Video <sup>1,2</sup>	87787	\$20.00

**Note:** Group First Response features work with 5G Nationwide® network and 4G network plans. For avoidance of doubt, Verizon’s 5G Nationwide® network is a separate network from Verizon’s 5G Ultra-Wideband network.

<sup>1</sup>**Group First Response is a Push to Talk Plus bolt-on feature. All lines must have a Push to Talk Plus feature to be eligible to purchase Group First Response.**

<sup>2</sup>Customers must have the Group First Response feature enabled to be eligible for the Push To Talk Plush Video bolt-on feature.

^As a condition for accessing and using Group First Response, the Purchasing Entity must have authorized access from Verizon to use Responder Private Core Internet Access.

Group First Response compatible device required. Group First Response is only supported on certain devices, as it requires the device to support specific hardware capabilities.

**\*\*\*\*Disclaimer:** These direct services (plus any development or modification of software related to the services) may be performed outside of the borders of the United States, and restricted and sensitive data or other secure or sensitive data or personal customer data, may be collected, developed, analyzed, or otherwise used or obtained by persons or entities working outside the boundaries of the United States. These services cannot be subject to any requirements to limit the performance of the services or storage of data within the United States and should not be ordered if these are requirements in your jurisdiction.

These features are available to National Security, Public Safety, and First Responder customers only as defined by the below NAICS (formerly SIC) codes.

<p><b>National Security/ First Responders / Public Safety</b></p> <ul style="list-style-type: none"> <li>• 485111 Mixed Mode Transit Systems (Rail &amp; Buses)</li> <li>• 485112 Commuter Rail Systems</li> <li>• 621910 Ambulance Services</li> <li>• 922110 Courts</li> <li>• 922120 Police Protection</li> <li>• 922130 Legal Counsel and Prosecution</li> <li>• 922140 Correctional Institutions</li> <li>• 922150 Parole Offices and Probation Offices</li> <li>• 922160 Fire Protection (except private)</li> <li>• 922190 Other Justice, Public Order, and Safety <b>Activities</b></li> <li>• 923120 Administration of Public Health Programs</li> </ul>	<ul style="list-style-type: none"> <li>• 928110 National Security</li> <li>• 926120 Regulation and Administration of Transportation Programs</li> <li>• 926150 Regulation, Licensing, and Inspection of Commercial Sectors</li> <li>• 926130 Regulation and Administration of Comms, Electric, Gas, Utilities</li> <li>• 921150 American Indian and Alaska Native Tribal <b>Governments</b></li> <li>• 921190 Other General Government Support</li> <li>• 921110 Executive Offices</li> </ul>
---	---

**Group First Response for  
Non Public Sector Customers**

**Mission Critical**

Features \$25.00 and above are eligible for monthly access discounts.

Description	Feature Code	Monthly Access Fee
^Group First Response <sup>1</sup>	87781	\$35.00
Push to Talk Plus Video <sup>1,2</sup>	87787	\$20.00

**Note:** Group First Response features work with 5G Nationwide® network and 4G network plans. For avoidance of doubt, Verizon’s 5G Nationwide® network is a separate network from Verizon’s 5G Ultra-Wideband network.

<sup>1</sup>**Group First Response is a Push to Talk Plus bolt-on feature. All lines must have an active Push to Talk Plus feature to be eligible to purchase Group First Response.**

<sup>2</sup>Customers must have the Group First Response feature enabled to be eligible for the Push To Talk Plush Video bolt-on feature.

^Group First Response requires each line to have Responder Private Core Internet Access (RPC IAC) on their lines to enable the feature.

Group First Response compatible device required. Group First Response is only supported on certain devices, as it requires the device to support specific hardware capabilities.

\*\*\*\*Disclaimer: These direct services (plus any development or modification of software related to the services) may be performed outside of the borders of the United States, and restricted and sensitive data or other secure or sensitive data or personal customer data, may be collected, developed, analyzed, or otherwise used or obtained by persons or entities working outside the boundaries of the United States. These services cannot be subject to any requirements to limit the performance of the services or storage of data within the United States and should not be ordered if these are requirements in your jurisdiction.

These features are available to National Security, Public Safety, and First Responder customers only as defined by the below NAICS (formerly SIC) codes

<p><b>Water</b> 924110 Water Infrastructure 221320 Sewage Treatment Facilities 221310 Water Supply and Irrigation Systems</p> <p><b>Transportation</b> 482111 Railway Transportation 481111 Passenger Air Transportation 481112 Freight Air Transportation 483111 Shipping Transportation 491110 Postal Service</p> <p><b>Information Technology</b> 541512 Computer Integration 541519 Computer Disaster Recovery</p> <p><b>Chemical</b> 561612 Protective Services 541330, 541690 Chemical Engineering and</p> <p><b>Consulting</b> 239210 Pharmaceutical</p> <p><b>Communications</b> 517110 Telecommunications, Wired</p>	<p><b>Telecommunications</b> 238210, 334290 and 561620 Alarm Systems</p> <p><b>Critical Manufacturing</b> 237310 Highway, Street and Bridge Construction 811310 Industry Equipment Repair 236210 Industrial Building Construction 211113 Extraction; 236220 Construction Management</p> <p><b>Energy</b> 333611 Wind Turbine 221111 Hydroelectric Power Generation 221122 Electric Power Distribution 221118 Other Electric Power Generation 221210 Natural Gas Distribution 221113 Nuclear Electric Power Generation 562211 Hazardous Waste Treatment and Disposal</p> <p><b>Healthcare and Public Health</b> 621112 Health Care Practitioners 923120 Public Health Programs</p>
---	---

517212 Cellular and other Wireless

**Group First Response Dispatch and Video Bundles  
National Security, Public Safety, and First Responders  
Government Subscribers Only**

**Mission Critical**

Description	License Bundles	Frequency	Price
Dispatch Group Command With Video	DIS_PTT_GROUP_CMD_VIDEO	Monthly	\$300.00
Dispatch Group Advance with LMR and Video	DIS_PTT_GROUP_ADV_LMR_VIDEO	Monthly	\$281.00
Dispatch Group Command with LMR and Video	DIS_PTT_GROUP_CMD_LMR_VIDEO	Monthly	\$306.00
Dispatch PTT+ with LMR and Video	DIS_PTT_LMR_VIDEO	Monthly	\$236.00
Dispatch Group Advance with Video	DIS_PTT_GROUP_ADV_VIDEO	Monthly	\$275.00
Dispatch PTT+ with Video	DIS_PTT_VIDEO	Monthly	\$230.00

**Note: Is there a note for the Sku's?? I can state that these are licenses that the customers can cancel at any time. Is there anything else you want to state? Command and advanced had paragraphs on how they worked etc. where is that for these?**

All lines must have a Group First Response compatible device with an active Push to Talk Plus feature to be eligible to purchase Group First Response Dispatch and Video Bundles. These features are available to National Security, Public Safety, and First Responder customers only as defined by the NAICS (formerly SIC) codes.

## Interoperability

### Mission Critical

Interoperability licenses are not eligible for any further discounts.

#### Software Sku's

Sku	Sku Description	Pricing Frequency	Price
U960-985-005-GOV	Public Safety IWS Edge Clients <sup>1</sup>	Monthly	\$139.95
U960-991-001-GOV	Public Safety Multimedia PTT Clients <sup>2</sup>	Monthly	\$7.95
U960-610-001-GOV	Public Safety Radio Gateway Interconnection <sup>3</sup>	Monthly	\$39.95
U960-240-001-GOV	Public Safety Video Gateway Interconnection <sup>4</sup>	Monthly	\$46.95
U960-260-001-GOV	Public Safety Telephone Interconnection <sup>5</sup>	Monthly	\$19.98
U961-985-001-GOV	Public Safety Soft Panic SW <sup>6</sup>	Monthly	\$112.50

#### Hardware Sku's One time charge

Sku	Sku Description	Pricing Frequency	Price
U980-100-001	All Network provisioning	One time	\$795.00
U990-800-001	All Staging Testing	One time	\$300.00
U500-614-001	4 PORT HW RADIO GATEWAY	One Time	\$3,000.00
U500-612-001	2 PORT HW RADIO GATEWAY	One Time	\$2,400.00
U500-610-001	1 PORT HW RADIO GATEWAY	One Time	\$1,995.00
M840-475	VIDEO STREAMING DEVICE	One Time	\$2,100.00
M400-351	SMART CABLE FOR VIDEO SCARPING	One Time	\$399.00

**Note:** Coverage includes the Verizon Wireless 4G network only. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing, which can be found at [www.verizonwireless.com/international](http://www.verizonwireless.com/international). Lines activating on these plans must be on 4G HD voice-capable smartphones.

Mutualink solution provides the interoperability required when an active incident occurs (robbery, shooting etc.), and there is a need for different public safety agencies, schools, or commercial establishments to work together. Specifically allow all parties to exchange video, files (e.g. floor plans), messages, in addition to instant Push To Talk for voice communication.

Interoperability – Mutualink solution improves collaboration (Audio, Video, Data) during emergencies in real-time. Overcome silos by enabling you to share information, between first responders, schools, and private security personnel, when you need it.

1. IWS Edge Client – Has a way of allowing drag and drop of participants and creating an active incident. Sharing audio/video data.
2. Multimedia PTT Client – Group communication to share audio/video data.
3. Radio Gateway Interconnection – Monthly charge for connecting the radio gateway to the hosted solution
4. Video Gateway Interconnection - Monthly charge for connecting the radio gateway to the hosted solution
5. Telephone Interconnection - Monthly charge for connecting the radio gateway to the hosted solution (Wireline)
6. Soft Panic SW – Allows customer to create an incident with predefined participants automatically

**\*\* The above Sku's are mutually exclusive from one another. They cannot be used on the same MDN at the same time\*\***



**Local Network Command –****National Security, Public Safety, and First Responders**

This feature is NOT eligible for monthly access fee discounts.

**Mission Critical**

<b>Monthly Access Fee for First Responders (88112)</b>	\$0.00	Customers may process an uplift that may auto renew within a 23 hr. period
<p><b>Notes:</b> Local Network Command (LNC) is a tool that provides on-demand local control of pre-selected users' network quality of service enhancement on a temporary basis. LNC requires each line to have Responder Private Core Internet Access (RPC IAC) on their lines to enable the feature. Below are the eligible NAICS codes:</p> <p>**Uplift will renew up to three (3) times after original uplift request, based on the length of time of the original uplift. Total uplift time (original and renewed) cannot exceed 23 hours.</p>		
<p><b>National Security/ First Responders / Public Safety</b></p> <ul style="list-style-type: none"> <li>• 485111 Mixed Mode Transit Systems (Rail &amp; Buses)</li> <li>• 485112 Commuter Rail Systems</li> <li>• 621910 Ambulance Services</li> <li>• 922110 Courts</li> <li>• 922120 Police Protection</li> <li>• 922130 Legal Counsel and Prosecution</li> <li>• 922140 Correctional Institutions</li> <li>• 922150 Parole Offices and Probation Offices</li> <li>• 922160 Fire Protection (except private)</li> <li>• 922190 Other Justice, Public Order, and Safety Activities</li> <li>• 923120 Administration of Public Health Programs</li> </ul>	<ul style="list-style-type: none"> <li>• 928110 National Security</li> <li>• 926120 Regulation and Administration of Transportation Programs</li> <li>• 926150 Regulation, Licensing, and Inspection of Commercial Sectors</li> <li>• 926130 Regulation and Administration of Comms, Electric, Gas, Utilities</li> <li>• 921150 American Indian and Alaska Native Tribal Governments</li> <li>• 921190 Other General Government Support</li> <li>• 921110 Executive Offices</li> </ul>	

**Local Network Command – Government Subscribers**

This feature is NOT eligible for monthly access fee discounts.

**Mission Critical**

<b>Monthly Access Fee for Government Agencies (88111)</b>	\$1.00	Customers may process an uplift that may auto renew within a 23 hr. period
<p><b>Notes:</b> Local Network Command (LNC) is a tool that provides on-demand local control of pre-selected users' network quality of service enhancement on a temporary basis. LNC requires each line to have Responder Private Core Internet Access (RPC IAC) on their lines to enable the feature. Below are the eligible NAICS codes:</p> <p>**Uplift will renew up to three (3) times after original uplift request, based on the length of time of the original uplift. Total uplift time (original and renewed) cannot exceed 23 hours.</p>		
<p><b>Water</b></p> <p>924110 Water Infrastructure 221320 Sewage Treatment Facilities 221310 Water Supply and Irrigation Systems</p> <p><b>Transportation</b></p> <p>482111 Railway Transportation 481111 Passenger Air Transportation 481112 Freight Air Transportation 483111 Shipping Transportation 491110 Postal Service</p> <p><b>Information Technology</b></p> <p>541512 Computer Integration 541519 Computer Disaster Recovery</p> <p><b>Chemical</b></p>	<p><b>Telecommunications</b></p> <p>238210, 334290 and 561620 Alarm Systems</p> <p><b>Critical Manufacturing</b></p> <p>237310 Highway, Street and Bridge Construction 811310 Industry Equipment Repair 236210 Industrial Building Construction 211113 Extraction; 236220 Construction Management</p> <p><b>Energy</b></p> <p>333611 Wind Turbine 221111 Hydroelectric Power Generation 221122 Electric Power Distribution 221118 Other Electric Power Generation 221210 Natural Gas Distribution 221113 Nuclear Electric Power Generation</p>	

561612 Protective Services 541330, 541690 Chemical Engineering and  <b>Consulting</b> 239210 Pharmaceutical  <b>Communications</b> 517110 Telecommunications, Wired 517212 Cellular and other Wireless	562211 Hazardous Waste Treatment and Disposal  <b>Healthcare and Public Health</b> 621112 Health Care Practitioners 923120 Public Health Programs
--	---

## Local Network Command – Enterprise Customers

This feature is NOT eligible for monthly access fee discounts.

### Mission Critical

<b>Monthly Access Fee for Enterprise/B2B Customers (NAICS Qualified) (8776)</b>	\$2.50	Customers may process an uplift that may auto renew within a 23 hr. period
<p><b>Notes:</b> Local Network Command (LNC) is a tool that provides on-demand local control of pre-selected users' network quality of service enhancement on a temporary basis. LNC requires each line to have Responder Private Core Internet Access (RPC IAC) on their lines to enable the feature. Below are the eligible NAICS codes:  **Uplift will renew up to three (3) times after original uplift request, based on the length of time of the original uplift. Total uplift time (original and renewed) cannot exceed 23 hours.</p>		

<p><b>Water</b>  924110 Water Infrastructure  221320 Sewage Treatment Facilities  221310 Water Supply and Irrigation Systems</p> <p><b>Transportation</b>  482111 Railway Transportation  481111 Passenger Air Transportation  481112 Freight Air Transportation  483111 Shipping Transportation  491110 Postal Service</p> <p><b>Information Technology</b>  541512 Computer Integration  541519 Computer Disaster Recovery</p> <p><b>Chemical</b>  561612 Protective Services  541330, 541690 Chemical Engineering and</p> <p><b>Consulting</b>  239210 Pharmaceutical</p> <p><b>Communications</b>  517110 Telecommunications, Wired  517212 Cellular and other Wireless</p>	<p><b>Telecommunications</b>  238210, 334290 and 561620 Alarm Systems</p> <p><b>Critical Manufacturing</b>  237310 Highway, Street and Bridge Construction  811310 Industry Equipment Repair  236210 Industrial Building Construction  211113 Extraction;  236220 Construction Management</p> <p><b>Energy</b>  333611 Wind Turbine  221111 Hydroelectric Power Generation  221122 Electric Power Distribution  221118 Other Electric Power Generation  221210 Natural Gas Distribution  221113 Nuclear Electric Power Generation  562211 Hazardous Waste Treatment and Disposal</p> <p><b>Healthcare and Public Health</b>  621112 Health Care Practitioners  923120 Public Health Programs</p>
---	--

## WIRELESS EQUIPMENT

### Equipment Pricing (NEW)

One (1) Basic voice device at no charge on rate plans with a monthly access fee of \$14.99 or higher per 24 months/ per line.

Make and model at Verizon Wireless sole discretion, subject to availability.

SOFL Approved  
Government Equipment Matrix devices.  
Verizon Wireless Government 10K 2yr matrix pricing only.

All devices shall include an AC charger at no additional cost with the initial purchase.  
Additional or replacement AC chargers may be purchased

Enterprise Network Extender at 25% off retail.  
25% discount applies to the non-discounted, full retail price only of qualifying equipment.

**Notes:** Verizon Wireless reserves the right to add or discontinue models. Equipment is subject to availability. Verizon Wireless' Government Equipment Matrix is updated at a minimum quarterly based upon equipment availability, changes in technology, and market conditions. Not eligible for any other promotional pricing offers. Equipment becomes eligible for upgrade after 24 months in service.

### Accessory Discount

Government Subscribers are eligible to receive a 25% discount from the non-discounted, retail price of qualifying accessories.

## Other Services and Fees

Non-recurring Verizon Wireless Fees	
Insufficient Funds Check	Waived
Bill Reprint	Waived
Late Fee	Waived
Record Change/Upgrade Fee	Waived

Fulfillment/Shipping	
Standard: 2-day (orders received before 4PM)	Waived
Urgent: Priority Overnight (delivery by 10:30 AM) (orders received before 4PM)	\$14.99
Saturday: (shipping by noon)	\$19.99

Directory Assistance: 411 Search <sup>SM</sup>	
Our wireless 411 Search <sup>SM</sup> is an enhanced directory assistance service with automatic connection. 411 Search offers phone numbers, addresses and information providing quick, safe and convenient service with up to three listings and one call connection per call or text.	
Voice call	\$1.99 (subject to change) per call plus applicable airtime, toll, wireless long distance and landline charges
Message Sent via text	With messaging bundle: \$1.99 plus airtime for the call, and the message will be subtracted from the monthly allowance
	Per text message: \$1.99 plus airtime for the call and \$0.20 for the text message

**Block all calls except local calls (as defined by call plan):** This is not permissible, but Flexible Business Plans are toll free nationwide. No blocking available to Canada or for premium calls such as 411. Toll charges may apply.

**Block spam and robocalls:** Verizon Call Filter helps you avoid unwanted callers with spam protection, and allows you to set up a spam filter by level of risk, preventing unsolicited calls by sending them directly to voicemail. The basics (spam detection, blocking and reporting) are available at no charge.

**Block inbound/outbound text messages:** Inbound and outbound text messaging can be blocked, including both at the same time at no charge.

**Block international calls to and from North America only:** International Services Enabled (ISE) is required to permit calls to Mexico. Blocking is available within the North America dialing pattern, which includes the U.S. and Canada. Toll charges may apply. Incoming calls can originate anywhere in the world.

Feature	Basic Voicemail	Basic Visual Voicemail	iPhone Visual Voicemail	Voicemail to Text for iPhone	Premium Visual Voicemail
Monthly Access Fee	Free	Free + Data	Free + Data	\$2.99 + Data	\$2.99 + Data
Storage Capacity (Messages)	20	20	40	40	40
Message Duration	3 minutes	3 Minutes	3 Minutes	3 Minutes	5 Minutes
Transcription	NA	NA	NA	X	X
Distribution Lists	15	15	NA	NA	20
Distribution Members	10	10	NA	NA	50
Call Return	NA	X	X	X	X
Save Voicemails to device	NA	X	NA	NA	X
Caller Dependent Greetings	NA	NA	NA	NA	20
Caller Dependent Greeting Members per group	NA	NA	NA	NA	50
Reply by Text and E-Mail	NA	X	X	X*	X
Forward by Text and E-Mail	NA	NA	NA	NA	X
Voicemail to Text	NA	NA	NA	X	X
Mobile Application**	NA	X	X	X	X
Reply by FaceTime**	NA	NA	X	X	NA

## Legacy Pricing

### LEGACY: Custom State of Florida Nationwide Push to Talk Plus (PTT) Per Line Calling Plan or Feature

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

Conventional (Basic) Device Plan		Smartphone Device Feature		
SOFL Plan Number	Monthly Access Charge Per Line	Tier Domestic Anytime PTT Plus Lines Per Month	Domestic Anytime Voice Allowance Minutes Per Month	
			Conventional (Basic) Device Plan	Smartphone Device Feature
2B.1 through 2B.18 (PTT+ 94976)	\$10.00	1 - 8,999	0	Per selected voice calling plan requirements
Mobile to Mobile Calling	Unlimited			
Data Sent/Received	Per the data package selected or Per the voice calling plan.			

PTT Plus service requires PTT Plus enabled device and coverage. Pricing is based on the current State of Florida, Department of Management Services' quarterly commitment selection and is subject to change. Please refer to the Mobile Communication Services (MCS) Contract DMS-10/11-008C for further details.

### Legacy: Custom State of Florida Nationwide Push to Talk Plus (PTT) Per Line Calling Plan or Feature (INTEROPERABILITY)

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

Conventional (Basic) Device Plan		Smartphone Device Feature		
SOFL Plan Number	Monthly Access Charge Per Line	Domestic Anytime PTT Plus Lines Per Month	Domestic Anytime Voice Allowance Minutes Per Month	
			As a plan:	As a feature:
2B.1 through 2B.18 (PTT+ 94976)	\$10.00	1 - 8,999	0	Per the voice calling plan
Mobile to Mobile Calling	Unlimited			
Data Sent/Received	Per the data package selected or Per the voice calling plan.			

PTT Plus service requires PTT Plus enabled device and coverage. PTT Plus Interoperability requires an Interoperability Gateway, PTT Plus enabled device, and coverage. Pricing is based on the current State of Florida, Department of Management Services' quarterly commitment selection and is subject to change. Please refer to the Mobile Communication Services (MCS) Contract DMS-10/11-008C for further details.

**LEGACY: Custom State of Florida SMS Per Message Feature**

The calling features below reflect the monthly access charge discount. No additional discounts apply.

**SMS (Text Messaging)**

SOFL Plan Number	Monthly Access Charge	Domestic Message Allowance	Domestic Messages Per Month	Per SMS Message Rate (Sent/Received)
3.1 through 3.13 (77847)	\$0.00	0	1 - 450,999	\$0.02

**SMS (Text) Messaging:** Text Messaging includes Short Message Service (SMS up to 160 characters) and Enhanced Messaging Service (EMS up to 1120 characters). Enhanced Text Messages sent to most SMS handsets will be delivered as multiple Text messages of up to 160 characters each. Subscribers have the option to have text messages disabled entirely without affecting voicemail or other related services. Text Messaging plans do not include Operator Assisted Messaging or International Messaging, which is available for 25¢ per message sent and 20¢ per message received see attached International services pricing for further details... Pricing is based on the current State of Florida, Department of Management Services' quarterly commitment selection and is subject to change. Please refer to the Mobile Communication Services (MCS) Contract DMS-10/11-008C for further details.

**LEGACY: Custom State of Florida MMS Per Message Feature**

The calling features below reflect the monthly access charge discount. No additional discounts apply.

**MMS (Picture and Video Messaging)**

SOFL Plan Number	Monthly Access Charge	Domestic Message Allowance	Domestic Messages Per Month	Per MMS Message Rate (Sent/Received)
3.1 through 3.25 (77848)	\$0.00	0	1 - 1,608,999	\$0.05

**Multi-Media Messaging (MMS):** Multi-Media Messaging (MMS) includes picture and video messaging and is only available within the National Enhanced Services Rate and Coverage Area. In addition, MMS messages are \$0.25 per message, per address. In addition to the MMS per message charges, MMS uses calling plan Anytime Minutes or kilobytes. Subscribers have the option to have text messages disabled entirely without affecting voicemail or other related services. Text Messaging plans do not include Operator Assisted Messaging or International Messaging, which is available for 25¢ per message sent and 20¢ per message received. Pricing is based on the current State of Florida, Department of Management Services' quarterly commitment selection and is subject to change. Please refer to the Mobile Communication Services (MCS) Contract DMS-10/11-008C for further details.

**LEGACY: Custom State of Florida SMS Broadcast Per Message Feature**

The calling features below reflect the monthly access charge discount. No additional discounts apply.

**SMS Broadcast (Text) Messaging**

SOFL Plan Number	Monthly Access Charge	Domestic Message Allowance	Domestic Messages Per Month	Per SMS Message Rate (Sent/Received)
3B.1 through 3B.25 (77847)	\$0.00	0	1 – 130,999	\$0.02

**SMS (Text) Messaging:** Text Messaging includes Short Message Service (SMS up to 160 characters) and Enhanced Messaging Service (EMS up to 1120 characters). Enhanced Text Messages sent to most SMS handsets will be delivered as multiple Text messages of up to 160 characters each. Subscribers have the option to have text messages disabled entirely without affecting voicemail or other related services. Pricing is based on the current State of Florida, Department of Management Services' quarterly commitment selection and is subject to change. Please refer to the Mobile Communication Services (MCS) Contract DMS-10/11-008C for further details.

**LEGACY: Custom State of Florida Voice Calling Plans**

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

## Unlimited Night &amp; Weekend Minutes

SOFL Plan Number	Domestic Anytime Minutes	Conventional and Smartphone Devices Monthly Access Charge	Overage Rate	Domestic Voice Roaming (Outside Florida)
6.1a (86192)	250	\$20.60	\$0.041	\$0.103
6.4a (86193)	600	\$30.90	\$0.041	\$0.103
Data Sent or Received		\$1.99 per MB or per Data Package		
Optional Feature				
Domestic Push-to-Talk Plus		\$0.00		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. 3G/4G Smartphones and 3G/4G Multimedia Phones require a data package. 4G service requires 4G equipment and 4G coverage. PTT Plus service requires PTT Plus enabled device and coverage.

**LEGACY: Custom State of Florida Unlimited Voice Calling Plan**

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

## No Domestic Long Distance Charges

SOFL Plan Number	Domestic Anytime Allowance Minutes*	Conventional and Smartphone Devices Monthly Access Charge	Overage Rate	Domestic Voice Roaming (Outside Florida)
6.6a(86194)	Unlimited	\$41.20	N/A	\$0.103 (includes PTT+)
Data Sent or Received		\$1.99 per MB or per Data Package		
Optional Feature				
Domestic Push-to-Talk Plus		\$0.00		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. \*Overage Rate applies after allowance. 3G/4G Smartphones and 3G/4G Multimedia Phones require a data package. 4G service requires 4G equipment and 4G coverage. PTT Plus service requires PTT Plus enabled device and coverage.

**LEGACY: Custom State of Florida Unlimited Nationwide Voice Calling Plan**

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

SOFL Plan Number	Domestic Anytime Allowance Minutes*	Conventional and Smartphone Devices Monthly Access Charge	Overage Rate	Voice Roaming (Canada and Mexico)
6.6a (86197)	Unlimited	\$51.50	N/A	\$0.69 (includes PTT+)
Data Sent or Received		\$1.99 per MB or per Data Package		
Optional Feature				
Domestic Push-to-Talk Plus		\$0.00		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. \*Overage Rate applies after allowance. 3G/4G Smartphones and 3G/4G Multimedia Phones require a data package. 4G service requires 4G equipment and 4G coverage. PTT Plus service requires PTT Plus enabled device and coverage.

**LEGACY: Custom State of Florida All Inclusive Unlimited Nationwide Voice & Messaging Plan**

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

## Conventional and Smartphone/BlackBerry Devices

SOFL Plan Number	Monthly Access Charge Per Line	Nationwide Voice Allowance	Domestic Tethering Allowance	Overate Rate	Unlimited Text, Picture, Video Messaging and Data
6.1d(86768-3G)	\$51.00	Unlimited	5GB	\$10.30/GB	Included

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Overage Rate applies after allowance. 4G service requires 4G equipment and 4G coverage.

**LEGACY: Custom State of Florida All Inclusive Unlimited Nationwide Voice & Messaging Plan (Hotspot)**

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

## Conventional and Smartphone/BlackBerry Devices

SOFL Plan Number	Monthly Access Charge Per Line	Nationwide Voice Allowance	4G Domestic Hotspot/Tethering	Overate Rate	Unlimited Text, Picture, Video Messaging and Data
6.1d (86769-4G)	\$51.00	Unlimited	5GB	\$10.30/GB	Included

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Overage Rate applies after allowance. 4G service requires 4G equipment and 4G coverage.

**LEGACY: Custom State of Florida BlackBerry Data Feature Packages**

The calling plans below reflect the monthly access charge discount. No additional discounts apply.

## Data for BlackBerry devices only

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Overage Rate	Unlimited Text and MMS Messaging
6.10b(77294 and 79789)	\$15.45	500MB	\$0.00849per MB	Included*
6.11b(77295 and 79790)	\$20.60	1,000MB		
Exhibit 6B(79740 and 79791)	\$23.69	2,000MB		

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. Overage Rate applies after allowance. 4G service requires 4G equipment and 4G coverage. \*Not included with the State of Florida Nationwide Custom Pooled Voice Services Plans

**LEGACY: Custom State of Florida BlackBerry Unlimited Data Feature Package**

The calling plan below reflects the monthly access charge discount. No additional discounts apply.

## Data for BlackBerry devices only

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Overage Rate	Unlimited Text and MMS messaging and tethering
6.12b(79407-4G and 79409-3G), (79781-4G and 79780-3G)	\$32.96	Unlimited*	N/A	Included**

**Notes:** See attached Plan and Feature Details for important information about calling plans, features and options. 4G service requires 4G equipment and 4G coverage. \*Verizon Wireless will limit the data throughput speeds should 25 GB of data usage be

reached in any given billing cycle on any line. Data throughput speeds for additional usage will be limited for the remainder of the then-current bill cycle for the line(s) that exceed the 25 GB high-speed data usage threshold. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB with prior written notice \*\*Not available when bundled with the State of Florida Nationwide Custom Pooled Voice Services Plans

### LEGACY: Custom State of Florida Mobile Broadband Connect Feature

The calling feature below reflects the monthly access charge discount. No additional discounts apply.

With a Mobile Broadband Connect capable Smartphone/BlackBerry devices only

SOFL Plan Number	Monthly Access Charge Per Line	Domestic Data Allowance	Per Minute Rate and Long distance
6.1f (76404-4G, 76405-3G)	\$10.00	Unlimited*	Per the Voice Plan

**Notes:** See attached Plan and Feature Details for important information about plans, features and options. Mobile Broadband Connect is currently available on select voice and data devices, and provides Mobile Broadband service utilizing the device as a modem. A mobile office kit, VZAccess Manager Software, a cable for tethering and/ or a software update may be required. Bluetooth® is not supported with Mobile Broadband Connect. Feature may only be added onto an eligible plan coupled with a Custom State of Florida Smartphone or BlackBerry Data Feature Package (SOFL Plans 6.6b, 6.7b, 6.10b, 6.11b and Exhibit 6B). Per Minute Rate applies to voice calls and other data usage in the United States. For optional features, the underlying calling plan determines the rates for voice airtime, and domestic long distance. \*Verizon Wireless will limit the data throughput speeds should 25 GB of data usage be reached in any given billing cycle on any line. Data throughput speeds for additional usage will be limited for the remainder of the then-current bill cycle for the line(s) that exceed the 25 GB high-speed data usage threshold. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB with prior written notice

### LEGACY: Custom 4G Unlimited Smartphone Plan for Public Sector

State of Florida - Government Subscribers Only

This plan is not eligible for additional monthly access fee discounts.

<b>Monthly Access Fee</b>	<b>\$50.00</b>
<b>Data Allowance<sup>1</sup></b>	Unlimited
<b>Mobile Hotspot<sup>2</sup></b>	Unlimited
<b>Monthly Anytime Minutes</b>	Unlimited
<b>Domestic Long Distance Toll Free</b>	Included
<b>Domestic and International Messaging Allowance<sup>3</sup></b>	Unlimited

**Notes:** No domestic roaming or long distance charges. Coverage includes the Verizon Wireless 4G network; and the 3G and 3G Extended networks, while available. Usage outside of the United States will be billed at the international travel feature rate, if applicable, or pay as you go pricing see attached International services pricing for further details.. Only a 4G smartphone can be activated on this plan.

<sup>1</sup>After 10 GB of data usage on a line during any billing cycle, usage may be prioritized behind other customers in the event of network congestion. To ensure users are able to maximize their high-speed data use for business applications, video applications will stream at up to 480p.

<sup>2</sup>Mobile Hotspot is available on all capable devices and allows the line to share data allowance with multiple Wi-Fi enabled devices. If 10 GB of Mobile Hotspot data usage is exceeded on any line in any given billing cycle, Verizon Wireless will limit the data throughput speeds for additional usage for the remainder of the then-current billing cycle for the line that exceeds the data usage.

<sup>3</sup>Unlimited messaging from within the United States to anywhere in the world where messaging services are available. See attached International services pricing for further details.

The "Custom 4G Unlimited Smartphone Plan for Public Sector – State of Florida Government" is eligible to use Travel Pass SPO code 383.

## Verizon Wireless Plan and Feature Details

**Plans and Associated Charges:** Billing, shipping and end-user address must be within an area where Verizon Wireless is licensed and provides service. Charges for calls will be based on the cell sites used, which may be outside the calling plan coverage area even when the subscriber is physically within the coverage area. Time of the call is based on the telephone switching office that carries the call, which may be different from the time of day shown on subscriber's phone. Unused monthly minutes and/or Megabytes are lost. On outgoing calls, charges start when subscriber first presses SEND or the call connects to a network, and on incoming calls, when the call connects to a network (which may be before it rings). A call may end several seconds after subscriber presses END or the call disconnects. Calls made on the Verizon Wireless network, are only billed if they connect (which includes calls answered by machines). Billing for airtime and related charges may sometimes be delayed. Calls to "911" and certain other emergency services are toll-free and airtime-free, Airtime may be charged when dialing toll-free numbers.

**Anytime Minutes:** Anytime Minutes apply when making or receiving calls from a calling plan's rate and coverage area. . Airtime is rounded up to the next full minute. Allowance minutes/Megabytes are not transferable except as may be available on plans with sharing. In order to gain access to coverage in newly expanding markets, subscribers must periodically dial \*228 to update roaming information from voice or Smartphone devices; from the VZAccess Manager, go into "Options" and click "Activation," while in the National Enhanced Services Rate and Coverage Area every three months. This may alter the rate and coverage area. Automatic roaming may not be available in all areas and rates may vary. Roaming charges may be delayed to a later bill.

**Long Distance:** Unlimited domestic long distance is included when calling from the calling plan's home rate and coverage area, unless otherwise specified in the calling plan.

**Unlimited Messaging:** Unlimited Messaging is included with select plans and is available in the National Enhanced Services rate and coverage area in the United States. Messaging applies when sending and receiving (i) text, picture and video messages to and from Verizon Wireless and Non-Verizon Wireless customers in the United States, (ii) Text, picture, and video messages sent via email, (iii) Instant messages, and (iv) Text messages with customers of wireless carriers in Canada, Mexico, Puerto Rico, and the U.S. Virgin Islands. Messaging is subject to Text, Picture, and Video Messaging Terms and conditions. Premium messages are not included.

**Mobile to Mobile Calling:** Mobile to Mobile Calling minutes apply when making calls directly to or receiving calls directly from another Verizon Wireless subscriber while in the Nationwide Rate and Coverage area. Mobile to Mobile calls must originate and terminate while both Verizon Wireless subscribers are within the Mobile to Mobile Calling area. Mobile to Mobile Calling is not available (i) with fixed wireless devices with usage substantially from a single cell site, (ii) for data usage including Push to Talk Plus calls, Picture or Video Messaging (iii) if Call Forwarding or No Answer/Busy Transfer features are activated, (iv) for calls to Verizon Wireless customers using any of the International services, (v) for calls to check Voice Mail, (vi) in those areas of Louisiana and Mississippi where the users roaming indicator flashes, (vii) in Canada and Mexico and (viii) to users whose current wireless exchange restricts the delivery of Caller ID And (viii) for incoming calls if Caller ID is not present or Caller ID Block is initiated. Mobile to Mobile Calling minutes will be applied before Anytime Minutes.

**Night and Weekend Minutes:** Apply to calls made in a calling plan's rate and coverage area only during the following hours: 12:00 am Saturday through 11:59 pm Sunday and 9:01 pm to 5:59 am Monday through Friday. If both Night and Weekend and Mobile to Mobile Calling minute allowances apply to a given call, Mobile to Mobile Calling minutes will apply before Night and Weekend minutes. However, if either allowance is unlimited, the unlimited allowance will always apply first.

**Push to Talk Plus:** Push to Talk Plus capable Equipment required. Push to Talk Plus capable Equipment can only be used with a Push to Talk Plus calling plan. **Subscribers switching from a Push to Talk Plus Calling Plan to another calling plan may not be able to use certain Push to Talk Plus capable Equipment with the new plan.** Push to Talk Plus calls may only be made with other Verizon Wireless Push to Talk Plus subscribers. Push to Talk Plus Subscribers may initiate or participate on a call, simultaneously, with as many as 250 total participants (total is limited to (50) if interoperating between 3G and 4G participants). Administrators can be designated to manage the Push to Talk contact lists via a single website interface with a single user name/password. Existing Push to Talk Subscriber Equipment may require a software upgrade to use Push to Talk Plus or replacement with a Push to Talk Plus capable device. Push to Talk Plus is only available within the National Enhanced Services Rate and Coverage Area and WiFi access points. There will be a delay from the time a Push to Talk Plus call is initiated until the Push to Talk Plus call is first received by the called party.. If an incoming voice call is received while on a Push to Talk Plus call the voice call may be answered and the Push to Talk Plus placed on hold. If an incoming Push to Talk Plus call is received while on a Push to Talk Plus call the PTT call icon can be selected to connect to the Push to Talk Plus call. If the incoming voice or Push to Talk Plus call is not answered a missed call alert will display. Network registration information will be sent to the Equipment each time it is powered on in the National Enhanced Services Rate and Coverage Area, each time the Subscriber travels into the National Enhanced Services Rate and Coverage Area, and every 12 hours if the Subscriber stays within the National Enhanced Services Rate and Coverage Area. While the updated network registration information is being sent to the Equipment, incoming voice calls will go directly to voice mail. Contact list cannot be modified from certain Equipment. Subscriber cannot prevent others who have the Subscriber's MTN from entering the MTN into their Push to Talk contact list. Only one person can speak at a time during a Push to Talk Plus call. . In-Call Talker Override (Talker Priority) allows a pre-determined user priority to take

the floor to communicate urgent message over participant. Push to Talk Plus services cannot be used for (i) access to the Internet, intranets or other data networks, except as the device's native applications & capabilities permit, (ii) any applications that tether Equipment to laptops, personal computers or other devices for any purpose. Please refer to the attached One Talk terms of service.

**International Long Distance:** You need International Eligibility to make international calls to most countries, but you can make calls to some North American destinations without it. Additional surcharges may apply when calling certain countries.

**International Roaming** Some services, such as premium text messaging, directory assistance, entertainment lines and third-party services, may be available, and charges for these services will be billed (along with applicable toll charges) in addition to roaming rates. Message-waiting-indicator service is not available where Text Messaging is not available. When using International Phone, or International Data services, or if you subscribe to a Nationwide Plus Canada or Nationwide Plus Mexico Plan, and you're roaming near country borders, calls may be carried by a cell site located in a neighboring country and billed at that country's rates. Verizon Wireless will terminate your service for good cause if less than half of your voice or data usage over three consecutive billing cycles is on the Verizon Wireless National Enhanced Services Rate and Coverage Area. International rates and destinations are subject to change without notice. You must add International Eligibility to your account to roam in many destinations. By using Equipment outside the United States, Subscriber is solely responsible for complying with all applicable foreign laws, rules and regulations ("Foreign Laws"), including Foreign Laws regarding use of wireless phones while driving and use of wireless camera phones. Verizon Wireless is not liable for any damages that result from subscriber's failure to comply with Foreign Laws.

**Roaming in GSM countries:** GSM International Phone, activated in the United States with compatible Subscriber Identity Module (SIM) card required. Rates terms and conditions apply only when roaming on participating GSM networks in published International Phone countries. Service may be available in additional countries, but airtime rates, availability of calling features, and ability to receive incoming calls (including return calls from emergency services personnel) may be restricted. Service in certain countries may be blocked without prior notice. Where Text messaging is available, Customer will be charged \$0.50 for each message sent and \$0.05 for each message received. Text messaging rates are subject to change. Text messages may be sent only to MTNs of (i) Verizon Wireless customers, and (ii) customers of foreign wireless carriers that participate in international text messaging. Ask your account manager for the most current list of participating foreign carriers.

## Data Services

**Data Services:** Verizon Wireless charges you for all data and content sent or received using our network (including any network overhead and/or Internet Protocol overhead associated with content sent or received), as well as resolution of Internet Protocol addresses from domain names. Sending or receiving data using a virtual private network (VPN) involves additional VPN overhead for which you will be charged. Please note that certain applications or widgets periodically send and receive data in the background, without any action by the user, and you will be billed for such data use. Applications may automatically re-initiate data sessions without you pressing or clicking the **SEND** or connect button. Data sessions automatically terminate after 24 hours. A data session is inactive when no data is being transferred. Data sessions may seem inactive while data is actively being transferred, or may seem active when the data is actually cached and data is not being transferred. If you have a Data Only plan and use voice service, domestic voice calls will be billed at \$0.25/minute.

Verizon Wireless is implementing optimization and transcoding technologies in our network to transmit data files in a more efficient manner to allow available network capacity to benefit the greatest number of users. These techniques include caching less data, using less capacity, and sizing the video more appropriately for the device. The optimization process is agnostic to the content itself and to the website that provides it. While Verizon Wireless invests much effort to avoid changing text, image, and video files in the compression process, and while any change to the file is likely to be indiscernible, the optimization process may minimally impact the appearance of the file as displayed on your device. For a further, more detailed explanation of these techniques, please refer to the Network Performance attachment. .

Verizon Wireless strives to provide customers with the best experience when using our network, a shared resource among tens of millions of customers. To further this objective, Verizon Wireless has implemented Network Optimization Practices designed to ensure that the overwhelming majority of data customers aren't negatively impacted by the inordinate data consumption of a few users. If you use an extraordinary amount of data and fall within the top 5% of Verizon Wireless data users, Verizon Wireless may reduce your data throughput speeds when connected to a congested cell site. The reduction can last for the remainder of the current bill cycle and the immediately following bill cycle to ensure high quality network performance for other users at locations and times of peak demand. For a further more detailed explanation of these techniques please refer to the Network Performance attachment.. Data transfer amounts will vary based on application. If you download an audio or video file, the file may be downloaded in sections or in its entirety; data charges will apply to the portion downloaded, regardless of whether you listen to or watch all of it. You may access and monitor your own data usage during a particular billing period, including during the Return Period, by accessing My Verizon online or by contacting Customer Service.

**Data Services: Permitted Uses:** You can use Verizon Wireless Data Services for accessing the Internet and for such uses as: (i) Internet browsing; (ii) email; (iii) intranet access (including accessing corporate intranets, email and individual productivity applications made available by your company); (iv) uploading, downloading and streaming of audio, video and games; and (v) Voice over Internet Protocol (VoIP).

**Data Services: Prohibited Uses.** You may not use our Data Services for illegal purposes or purposes that infringe upon others' intellectual property rights, or in a manner that interferes with other users' service, that violates trade and economic sanctions and prohibitions as promulgated by the Departments of Commerce, Treasury or any other U.S. government agency, that interferes with network's ability to fairly allocate capacity among users, or that otherwise degrades service quality for other users. Examples of prohibited usage include: (i) server devices or host computer applications that are broadcast to multiple servers or recipients such that they could enable "bots" or similar routines (as set forth in more detail (ii) below) or otherwise denigrate network capacity or functionality; (ii) "auto-responders," "cancel-bots," or similar automated or manual routines that generate amounts of net traffic that could disrupt net user groups or e-mail use by others; (iii) generating "spam" or unsolicited commercial or bulk e-mail (or activities that facilitate the dissemination of such e-mail); (iv) any activity that adversely affects the ability of other users or systems to use either Verizon Wireless' services or the Internet-based resources of others, including the generation of dissemination of viruses, malware, or "denial of service" attacks; (v) accessing or attempting to access without authority, the information, accounts or devices of others, or to penetrate, or attempt to penetrate Verizon Wireless' or another entity's network or systems; or (vi) running software or other devices that maintain continuous active Internet connections when a computer's connection would otherwise be idle or "any keep alive" functions, unless they adhere to Verizon Wireless' requirements for such usage, which may be changed from time to time.

Verizon Wireless further reserves the right to take measures to protect our network and other users from harm, compromised capacity or degradation in performance. These measures may impact your service, and Verizon Wireless reserves the right to deny, modify or terminate service, with or without notice, to anyone Verizon Wireless believes is using Data Services in a manner that adversely impacts the Verizon Wireless network. **Verizon Wireless may monitor your compliance, or other subscribers' compliance, with these terms and conditions, but Verizon Wireless will not monitor the content of the communications except as otherwise expressly permitted or required by law. [See the attached Verizon Full Privacy Policy]**

**Unlimited Data Plans and Features (such as Mobile Broadband, and Push to Talk Plus) may ONLY be used with wireless devices for the following purposes:** (i) Internet browsing; (ii) email; and (iii) intranet access (including access to corporate intranets, email, and individual productivity applications like customer relationship management, sales force, and field service automation). The Unlimited Data Plans and Features MAY NOT be used for any other purpose. Examples of prohibited uses include, without limitation, the following: (i) continuous uploading, downloading or streaming of audio or video programming or games; (ii) server devices or host computer applications, including, but not limited to, Web camera posts or broadcasts, automatic data feeds, automated machine-to-machine connections or peer-to-peer (P2P) file sharing; or (iii) as a substitute or backup for private lines or dedicated data connections. This means, by way of example only, that checking email, surfing the Internet, downloading legally acquired songs, and/or visiting corporate intranets is permitted, but downloading movies using P2P file sharing services and/or redirecting television signals for viewing on laptops is prohibited.

For individual use only and not for resale. We will protect our network from harm, which may impact legitimate data flows. We reserve the right to limit throughput or amount of data transferred exceeding 25 GB in any given billing cycle on any line, in any given billing cycle, for all additional usage for the remainder of the then-current bill cycle for the line that exceeds the data usage, and reserve the right to deny or terminate service, without notice, to anyone we believe is using an Unlimited Data Plan or Feature in any manner prohibited above or whose usage adversely impacts our network or service levels. Anyone using more than 25 GB per line in a given billing cycle is presumed to be using the service in a manner prohibited above, and we reserve the right to immediately terminate the service of any such person without notice. We reserve the right to adjust data throughput limitation thresholds to as low as 5GB in with prior written notice. We also reserve the right to terminate service upon notification to the customer.

Unlimited , Mobile BroadbandAccess, and InternationalAccess data sessions may be used for the following purposes: (i) Internet browsing, (ii) e-mail, and (iii) intranet access (including access to corporate intranets, e-mail and individual productivity applications like customer relationship management, sales force and field service automation). Unlimited Mobile BroadbandAccess and Push to Talk Plus services cannot be used (i) for uploading, downloading or streaming of movies, music or games, (ii) with server devices or with host computer applications, other than applications required for Wireless Sync service, including, but not limited to, Web camera posts or broadcasts, automatic data feeds, Voice over IP (VoIP), automated machine-to-machine connections, or peer-to-peer (P2P) file sharing, or (iii) as a substitute or backup for private lines or dedicated data connections. Additionally, Unlimited Mobile BroadbandAccess services cannot be used for, (i) access to the Internet, intranets or other data networks, except as the Equipment's native applications and capabilities permit, or (ii) for any applications that tether Equipment to laptops or personal computers other than for use of the Wireless Sync. Unlimited Mobile BroadbandAccess and data sessions automatically terminate after 2 hours of inactivity, unless Subscriber has Mobile IP (MIP) capable Equipment.

**Data Roaming:** International Eligibility is needed to roam in many destinations. See attached International services pricing for further details.

**International Data Optional Features:** International PC Card required for international use. International PC Cards will not work in the United States or Canada and GlobalAccess Subscribers will need a Mobile BroadbandAccess PC card for domestic use. The domestic and International PC Cards cannot be used at the same time. International Data Optional Features subscribers must activate and update their Preferred Roaming lists while in the National Enhanced Services Rate and Coverage Area every three months. Verizon Wireless reserves the right to terminate the service of any subscriber whose total usage is less than half on the Verizon Wireless National Enhanced Services Rate and Coverage Area over three consecutive billing cycles.

### M2M Data Plans and Feature Details

A data session is inactive when no data is being transferred, and may seem inactive while data is actively being transferred to a device, or seem active when actually cached and not transferring data. Customer must maintain virus protection when accessing the service and is responsible for all data sent and received including "overhead" (data that is in addition to user-transmitted data, including control, operational and routing instructions, error-checking characters as well as retransmissions of user-data messages that are received in error) whether or not such data is actually received. Verizon Wireless will not be liable for problems receiving Service that result from Customer's device.

**Megabyte (MB) Data Plans:** M2M data usage is rounded to next full kilobyte at end of each billing cycle. Any unused portion of the megabyte allowance is lost. Equipment will not indicate kilobyte usage.

**Data Roaming:** International eligibility is needed to roam in many destinations. Only the Canadian Broadband Rate and Coverage Area supports EV-DO. Please refer to the attached international services pricing for additional details.

#### *M2M Data Plan Share Options:*

**Share Options:** Sharing is available only among Government Subscribers on applicable M2M Low Usage and High Usage calling plans.

**Account Share:** Customer may activate up to 15 share groups per account. Sharing is available only among M2M Lines on the Mobile Broadband M2M Account Share Plans on the same billing account, in the same usage group (e.g. Low Usage and High Usage plans cannot share with each other). Unused allowance will be distributed to M2M Lines with an overage on an as needed basis to M2M Lines on the same billing account that have exceeded their allowance during the same monthly billing period. At the end of each bill cycle any unused allowances will be applied to the overages of the other M2M Lines on the same account beginning with the line with the lowest overage need until depleted. Customers subscribing to Mobile Broadband M2M Account Share Plans will be billed on separate billing accounts and invoices from Subscribers to the Mobile Broadband M2M Profile Share Plans.

**Profile Share:** Customer may activate one (1) share group per profile (e.g. Low Usage and High Usage plans cannot share with each other); however, customer may have multiple bill accounts on the same profile. Sharing is available only among M2M Lines on the Mobile Broadband M2M Profile Share Plans **on the same profile, in the same usage group**. Each sharing M2M Lines unused KBs will pass to other sharing M2M Lines that have exceeded their data allowance during the same monthly bill cycle. Unused KBs will be distributed proportionally as a ratio of the KBs needed by each applicable M2M Line to the total KBs needed by all sharing M2M Lines **on the same profile**. Customers subscribing to Mobile Broadband M2M Profile Share Plans will be billed on separate billing accounts and invoices from Subscribers to the Mobile Broadband M2M Account Share Plans.

**Note:** <sup>1</sup>A profile is defined as a Customer's overarching account of record under which Customer may have multiple billing accounts

### One Talk<sup>SM</sup> and Message+ from Verizon - Government Terms of Service

One Talk from Verizon, together with its related devices, software and applications ("Service" or "One Talk"), is a commercially available business telephone solution that brings together the functions of office phones and mobile devices (smartphones and tablets) into a unified system, with all devices sharing the same communication features. Please refer to the One Talk Features as attached hereto for a listing of features currently available with the Service.)

The following terms of service apply to the One Talk Service. "Customer" means the eligible entity purchasing the One Talk service under the Contract along with any Customer end users using the Service.

- Customer Agreement.** Customer's use of the Service is subject to all Contract terms. This applies regardless of whether the end user device is on the Customer's account or paid for by the end user (e.g. a Bring Your Own Device arrangement between Customer and end user).
- How the Service Works.** For the Service to work on wireless devices, Customer must select the line on your agency's profile to which you wish to add the One Talk feature. Each One Talk phone number can be shared with up to eight (8) devices (which can include one (1)

smartphone using One Talk in Basic Dialer mode (if available), five (5) smartphones and/or tablets using the One Talk Mobile App, and two (2) desk phones. (Note that desk phones are not required for the Service.) You may only make voice and/or video calls with up to three (3) devices per One Talk phone number at the same time. The Service is not compatible with all price plans and desk phones are not available under all contracts. Check with your sales representative for plan compatibility with the Service and the availability of desk phones under the Contract.

Customer is solely responsible for managing its end user access to the One Talk Service, management of end user devices and management of information transmitted via the Service. Addition of devices and associated Service features is managed and administered by the Customer through Verizon Wireless' web portal.

### A. One Talk Components

**One Talk Basic Dialer.** If available, the One Talk Basic Dialer adds various business features to a compatible device's native dialer, which on a compatible smartphones.) With One Talk in Basic Dialer mode, Customer's One Talk phone number will be the same as its Verizon Wireless phone number. Other devices that you select will share the same One Talk phone number.

**One Talk Mobile App.** The One Talk Mobile App is available for smartphone and tablets either from the Google Play™ Store for devices with Android™ 5.0 or higher or from the Apple® App Store for devices with iOS 9.0 or higher. To use the Service, Customer must add a One Talk phone number to the Mobile App and end users must use the Mobile App to make voice and video calls and to send and receive messages. You can also obtain access to One Talk features through the Mobile App. With the Mobile App, the device will have two phone numbers – one for its original native dialer (if available), and the other for the One Talk number. Other associated devices will share the same One Talk number. Users may install the One Talk Mobile App on a compatible device, including devices receiving service from other carriers. In such circumstances, One Talk phone numbers must be added to their devices, and the users will be Verizon Wireless subscribers for purposes of the Service only, even if they continue to use a different carrier for their original mobile telephone numbers. In order to use messaging through the One Talk Mobile App, the customer also must add the Message + App.

**Message+ App.** The Message+ App provides an integrated and customized messaging experience across an end user's mobile phone, tablet, PC, and other devices, and an integrated calling experience across a user's mobile phone and tablet. (Note that integrated calling is not part of the One Talk Service.) An end user can also send group, location and other multimedia messages ("MMS") in addition to traditional text messages. The Message+ App includes an Integrated Messaging feature that lets users send and receive text and multimedia messages on an end user's smartphone, tablet, computer or the web using a user's Verizon One Talk mobile telephone number. The service syncs up to 90 days of messages across an end user's devices.

**One Talk Desk Phones.** One Talk desk phones are Voice-over-Internet Protocol (VoIP) devices that must be purchased from Verizon Wireless. At your location, you will need separate broadband service (from Verizon or another ISP), either Ethernet or Wi-Fi connectivity, and AC power. Check with your Verizon Wireless sales representative for the availability of desk phones under the Contract.

**Auto Receptionist; Hunt Group.** In order to utilize either of these features, Customer must activate a new Verizon Wireless line or port in a line from another carrier. The settings for the line must be configured using the One Talk section of the My Business web portal.

### B. Charges

For each One Talk line, you will be charged a monthly recurring fee for the Service, in addition to the charges for data, voice, and messaging based on your service plan. Charges for international use may apply. You may be assessed additional 911 surcharges if required by law, for up to a maximum of three devices on each mobile phone number during the applicable billing cycle.

**Desk Phones.** Voice and video calls to and from One Talk desk phones will consume data on your existing broadband, cellular, or Wi-Fi connection. The following applies if you use the VZW network to connect to the Service:

**One Talk Basic Dialer.** Adding the One Talk feature to a smartphone does not consume any data. If you have a device that supports video calling, the voice portion will be billed as minutes of use and the video portion will be billed as data. Voice calls will be billed as minutes of use only.

**One Talk Mobile App.** Your download of the One Talk Mobile App will consume approximately 30 MB of data. Your use of the Service (including your download of the One Talk Mobile App) will be billed as data.

**Auto Receptionist; Hunt Group.** You will be charged a monthly recurring fee for each Auto Receptionist and Hunt Group line in your company's profile.

3. **Integrated Calling Charges (Message+).** Integrated Calling does not have a separate monthly service fee, but data usage charges will be incurred in accordance with Customer's service plan. If a call is transferred among connected devices, each transfer will be billed as a separate call. Also, depending on the service address, Customer may be assessed an additional 911 charge if required by law. Any call made from a tablet to a U.S. number will be treated as a domestic call, no matter where the call originates. Any call made from a tablet to a non-U.S. number will be treated as an international long distance call that originates in the U.S., which is subject to U.S. taxes, fees and Verizon surcharges, no matter where the call actually originates. These calls will be billed in accordance with Customer's international calling plan and/or international Contract rates.

4. **Emergency 911 Calls.** End users can make a 911 call over a Wi-Fi connection when using the Service, but whenever possible, end users

should avoid doing so because 911 calls over a WiFi connection will not work if there is a failure of your broadband connection or electrical power, or if the 911 system doesn't recognize the address. In addition, when using a One Talk desk phone, voice functionality (including the ability to make and receive 911 calls) will not be available during a power outage, broadband connection failure or other service disruption. Before any desk phone can be activated or the Service can be activated on any device, Customer must enter the U.S. address where Customer wants emergency services to be sent if end users call 911. It is not necessary to use the same address for all devices. It is very important that Customer updates its 911 address whenever Customer changes its location for any of these devices because this is the location that will be given to emergency services when end users dial 911. End users can go to their mobile device's Settings and change their 911 address at any time. Customer can change the 911 address for a desk phone on the One Talk section of the My Business web portal. (Note: With a smartphone using the One Talk Mobile App, emergency services will use the 911 address only if you use Wi-Fi to make the 911 call. If end users are using the Verizon Wireless Network, their smartphone's built-in capabilities will provide the location of the end user's device.)

5. **Integrated Messaging Text Message Feature.** To send and receive SMS messages, Mobile devices associated with either One Talk Basic Dialer (if available) or One Talk Mobile App must download the Message+ App to the device. The Integrated Messaging functionality of Message+ enables you to synchronize messages across multiple devices, including smartphones, tablets and the web. Text messages sent and received while using the Service are separate from the native texting app (dual numbers) and are only temporarily retained on the One Talk message platform in the cloud. End users with access to the Service on a Smartphone or the Mobile Client can retrieve/download any text message sent or received using the Service.

6. **HIPAA.** Integrated Messaging is not designed for secure transmission or storage of personal healthcare information. Therefore, Customer agrees not to use Service to store or transmit Protected Health Information (PHI) as defined in the Health Insurance Portability & Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 and accompanying regulations (collectively "HIPAA"). Covered Entities and Business Associates (as defined by HIPAA) will not use Integrated Messaging to store or transmit PHI. Customers that do not want its end users to save messages to the cloud (including all Covered Entities and Business Associates, as defined by HIPAA), must have an authorized representative block Integrated Messaging. For further information One Talk Verizon Messages terms of service.. To learn more about HIPAA, go to: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>.

7. **Service Limitations.** The Service is not compatible with fax machines, credit card machines or certain security systems. Your Verizon Wireless representative can suggest other possible solutions for some of these functions. Please check with your provider to confirm the compatibility requirements of your security system.

8. **Important Service Disclosures.** CUSTOMER ACKNOWLEDGES AND AGREES THAT THE SERVICE IS IMPLEMENTED WITHOUT SPECIFIC CONTROLS THAT MAY GENERALLY BE REQUIRED OR CUSTOMARY FOR CUSTOMERS IN ANY PARTICULAR INDUSTRY AND ARE NOT DESIGNED TO SATISFY ANY SPECIFIC LEGAL OBLIGATIONS. CUSTOMER IS SOLELY RESPONSIBLE FOR DETERMINING THAT THE SERVICE SATISFIES ANY LEGAL, REGULATORY OR CONTRACTUAL OBLIGATIONS CUSTOMER MAY HAVE. CUSTOMER AGREES TO USE THE SERVICES IN ACCORDANCE WITH ALL APPLICABLE LAWS AND NOT TO USE THE SERVICES IN ANY MANNER THAT MAY IMPOSE LEGAL, REGULATORY OR CONTRACTUAL OBLIGATIONS ON VERIZON WIRELESS, OTHER THAN THOSE WITH WHICH WE HAVE EXPRESSLY AGREED TO COMPLY IN THIS ADDENDUM.

CUSTOMER IS ON NOTICE THAT ANY TEXT MESSAGES DELIVERED TO A DEVICE USING THE SERVICE WILL REMAIN ON THAT DEVICE, EVEN AFTER THE MESSAGING FEATURE IS REMOVED OR END USER IS DEREGISTERED AND NO LONGER HAS ACCESS TO THE SERVICE. END USERS CONTROL THE DELETION OF MESSAGES RECEIVED ON THEIR DEVICES.

9. **Software.** In connection with the Service, Verizon Wireless will provide software that is owned by us, our affiliates or third-party licensors ("Software"). Verizon Wireless may update the Software from time to time and Customer and/or end user failure to install any update may affect Customer's Service and/or use of the Software. Customer may use the Software only as part of, or for use with, the Service as authorized in this Addendum.

Verizon Wireless grants Customer a limited, non-exclusive, non-transferable license to use the Service and the Software solely as authorized in this Addendum. All rights regarding use of the Service and Software not expressly granted in this Addendum are reserved by Verizon Wireless and/or any third-party licensors. The Software contains some programming, scripts, tools, modules, libraries, components, or other items that were developed using "Open Source" code; which are available for review in the One Talk attachments.

Software was developed solely at private expense, and Customer has no other rights in software than those set forth herein. As such, customer may not adapt, alter, modify, reverse engineer, de-compile, disassemble, translate, attempt to derive source code from or create derivative works of the Service or Software, or otherwise tamper with or modify any security features or other Service components for any reason (or allow or help anyone else to do so). Customer also agrees to follow all rules and policies applicable to the Service, including the installation of required or automated updates, modifications and/or reinstallations of Software and obtaining available patches to address security, interoperability and/or performance issues.

10. **Disclaimer of Warranty.** THE SERVICE AND SOFTWARE ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTIES, EXPRESS OR IMPLIED, OF ANY KIND BY EITHER VERIZON WIRELESS, OUR AFFILIATES, OFFICERS, EMPLOYEES, LICENSORS, CONTRACTORS, AND AGENTS (TOGETHER, THE "VERIZON PARTIES"), INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE, NON- INFRINGEMENT OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE VERIZON PARTIES AND ANY THIRD PARTY MOBILE APPLICATION STORE

OPERATORS FROM WHICH YOU DOWNLOAD THE ONE TALK MOBILE APP WILL NOT BE LIABLE TO YOU OR ANYONE ELSE FOR ANY LOSSES OR DAMAGES OF ANY KIND OR ANY SECURITY ISSUES THAT MAY RESULT FROM YOUR USE OF THE SERVICE. NO ADVICE OR INFORMATION GIVEN BY THE VERIZON PARTIES SHALL CREATE ANY WARRANTY HEREUNDER.

## Networkfleet Terms and Conditions

**1. DEFINITIONS.** In these Terms and Conditions, the following terms, when capitalized, shall have the meaning set forth below:

"Customer Website Pages" means the web pages on the Networkfleet Website designated by Networkfleet for use by Customer.

"Devices" means the Networkfleet wireless device(s) identified on an accepted order.

"Networkfleet Services" means the services ordered hereunder including, but not limited to: (a) collection of diagnostic and/or location information from a Vehicle; (b) any proprietary data feed or elements thereof or any APIs provided by Networkfleet; (c) analysis, delivery and posting of Vehicle information to the Networkfleet Website; (d) notification to Customer and/or a designated third party by e-mail of certain events or Vehicle information; (e) Customer access and usage of Customer Website Pages; and (f) Device installation services.

"Networkfleet Website" means the Networkfleet website currently located at [www.networkfleet.com](http://www.networkfleet.com).

"Network Fleet" is a wholly owned subsidiary of Verizon Communications, Inc, and an affiliate of Cellco Partnership, d/b/a Verizon Wireless which is the "Contractor" under the Verizon Wireless State of Florida Contract DMS-10/11-008C

"Service Partners" means the entities that Verizon Wireless works with, from time to time, to provide the Networkfleet Services, including, but not limited to, installers, website operators, mapping data providers and licensors.

"Vehicle" means any vehicle equipment equipped with a Device and owned or under the control of Customer.

**2. NETWORKFLEET LICENSE.** During the time that Customer is entitled to receive Networkfleet Services hereunder, the Customer shall have a non exclusive, non transferable license to (i) use the Networkfleet Services in the United States and such other countries as may be approved by Verizon Wireless in writing, (ii) access and use the Customer Website Pages, and (iii) use the firmware and software included in the Devices, solely for use in connection with the Networkfleet Services, and as provided in these Terms and Conditions. Redistribution or resale of this information by the Customer is prohibited without prior written consent.

**3. INSTALLATION SERVICES.** If Verizon Wireless accepts an order for Device installation services, such services may be performed by Service Partners who will install the Device at a mutually agreed location, in accordance with Networkfleet's Installation Policy, located at in the Networkfleet attachments., as it may be amended from time to time, which is available at the Networkfleet Website. Customer acknowledges and agrees that installation of the Device may involve drilling holes, rewiring and other similar alterations to the Vehicle and that Verizon Wireless is not obligated to restore the Vehicle after removal of the Device.

**4. CUSTOMER OBLIGATIONS.** Customer shall limit its use of the Devices, Networkfleet Services, Networkfleet Website, and Customer Website Pages to their intended purposes and shall comply, and cause its employees and agents to comply with all applicable laws and regulations and with Networkfleet's Website Acceptable Use Policy, Privacy Policy and all other policies that Networkfleet may establish from time to time, which are, or will be available, on the Networkfleet Website. Customer shall inform its drivers of Vehicles that such Vehicle has been enabled for Networkfleet Services and that the Networkfleet Services include the collection of data points associated with the Vehicle's location and manner of operation.

**5. LIMITED WARRANTY.** (a) Verizon Wireless warrants to Customer that a Device purchased hereunder (other than an Asset Tracker device) will be free from defects in material and workmanship that prevent the Device from functioning in accordance with its specifications for a period of three (3) years following the initial activation of a Device. The period may be extended though the same period of time as the Customer has continuously paid for Networkfleet Services for the Device;

(b) Verizon Wireless warrants to Customer that an Asset Tracker device which has been purchased new from Networkfleet by Customer, will be free from defects in material and workmanship that prevent it from functioning in accordance with its specifications for a period of three (3) years from initial activation, excluding the battery.

(c) Verizon Wireless warrants to Customer that all accessories that are purchased new from Networkfleet by Customer will be free from defects in material and workmanship that prevent them from functioning in accordance with their specifications for a period of one (1) year from the date of shipment,

(d) Verizon Wireless warrants to Customer that installation services will be free from defects in workmanship for a period of one (1) year from completion of any such installation services (unless Customer has purchased an extended installation warranty). Verizon Wireless warrants that extended warranty

installation services will be free from defects in workmanship for a period of one (1) year following completion of such services. The period may be extended through the same period of time as the Customer has continuously paid for such extended warranty installation service.

(e) Warranty claims must be made by notifying Verizon Wireless in writing promptly after Customer learns of the facts supporting a warranty claim, as specified in Networkfleet's current applicable warranty policy as attached hereto. Verizon Wireless will, at its discretion, either repair or replace any non-complying Device with a Device of equivalent functionality, and if applicable, remedy any defects in installation of the Device.

(f) THE REMEDIES IN THIS SECTION ARE THE SOLE OBLIGATIONS AND REMEDY FOR BREACH OF ANY WARRANTY.

**6. EXCLUSIONS.** The Limited does not cover repair, replacement or correction of any defect, damage or malfunctions caused by: (i) failure to properly install the Devices as described in the Networkfleet installation guides (if installation is not performed by Networkfleet); (ii) accident, negligence, theft, vandalism, operator error, misuse or acts of Nature; (iii) failure of the facilities Customer uses to access the Networkfleet Website or to conform to Networkfleet specifications; (iv) modifications, attachments, repairs or unauthorized parts replacements performed by Customer or any third party not authorized by Networkfleet; or (v) use by Customer of hardware or software not provided or approved by Networkfleet. Customer will be responsible for the cost of Support Services provided by Networkfleet caused by any of the foregoing.

**7. DISCLAIMER OF WARRANTIES.** EXCEPT FOR THE LIMITED WARRANTY SET FORTH IN SECTION 5, VERIZON WIRELESS MAKES NO WARRANTY OR GUARANTEE OF ANY KIND WITH RESPECT TO THE DEVICES AND THE NETWORKFLEET SERVICES. TO THE FULLEST EXTENT PERMISSIBLE BY APPLICABLE LAW, VERIZON WIRELESS DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO: IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE. VERIZON WIRELESS DOES NOT WARRANT THAT THE RECEIPT OF DATA, MAPPING INFORMATION, AND OTHER CONTENT FROM THE DEVICES WILL BE AVAILABLE AT ALL TIMES, AT ALL GEOGRAPHIC LOCATIONS, UNINTERRUPTED OR ERROR-FREE, OR THAT THE TRANSMISSION OF DATA, MAPPING INFORMATION, AND OTHER CONTENT FROM NETWORKFLEET TO CUSTOMER OR TO THE CUSTOMER WEBSITE PAGES WILL ALWAYS BE ACCURATE, TIMELY OR COMPLETE.

**8. LIMITATION OF LIABILITY.** (a) NEITHER PARTY WILL BE LIABLE FOR CONSEQUENTIAL, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF THAT PARTY IS INFORMED THAT THOSE DAMAGES MAY OCCUR. VERIZON WIRELESS' CUMULATIVE LIABILITY UNDER ANY LEGAL THEORY SHALL NOT EXCEED THE AMOUNT PAID TO VERIZON WIRELESS. (b) WITHOUT LIMITING THE FOREGOING, VERIZON WIRELESS AND THE SERVICE PARTNERS ARE NOT RESPONSIBLE FOR LIABILITIES OF ANY KIND RESULTING FROM DELAYS IN DELIVERY, INSTALLATION OR PROVIDING NETWORKFLEET SERVICES OR OTHER SERVICES, REGARDLESS OF THE CAUSE OF THE DELAY. CUSTOMER UNDERSTANDS AND AGREES THAT VERIZON WIRELESS SHALL NOT BE LIABLE FOR ANY DAMAGES OF ANY KIND RESULTING FROM AN ALLEGED OR ACTUAL LACK OF SECURITY RELATING TO CUSTOMER'S USE OF THE NETWORKFLEET SERVICES. (c) CUSTOMER UNDERSTANDS AND AGREES THAT: (i) THE DEVICE IS A WIRELESS DEVICE AND THAT WIRELESS COMMUNICATIONS NETWORKS ARE USED TO CONNECT THE DEVICES WITH NETWORKFLEETS DATA CENTER AND BY USING GPS (GLOBAL POSITIONING SYSTEM) TO DETERMINE A VEHICLE'S LOCATION; (ii) THE NETWORKFLEET SERVICES WILL NOT OPERATE UNLESS A VEHICLE IS IN AN AREA THAT HAS ADEQUATE WIRELESS COMMUNICATIONS COVERAGE AND, EVEN IF A VEHICLE IS IN SUCH AREA, THE NETWORKFLEET SERVICE IS SUBJECT TO WIRELESS SERVICE NETWORK AND TRANSMISSION LIMITATIONS AND MAY BE ADVERSELY AFFECTED BY TERRAIN, SIGNAL STRENGTH, WEATHER AND ATMOSPHERIC CONDITIONS, OR OTHER THINGS THAT VERIZON WIRELESS DO NOT CONTROL; AND (iii) INFORMATION ABOUT A VEHICLE'S LOCATION WILL NOT BE AVAILABLE UNLESS THE DEVICE IN THE VEHICLE IS ABLE TO RECEIVE GPS SIGNALS.

**9. PROPRIETARY RIGHTS.** Customer acknowledges and agrees that the Devices, the Networkfleet Service and the Networkfleet Website may include patent, copyright, trademark, service mark, trade secrets, or other intellectual property rights (collectively "Proprietary Rights") of Networkfleet, its affiliates or the Service Partners (including, with respect to the Networkfleet Website, materials that may be proprietary to Service Partners and suppliers, and that Networkfleet, its affiliates, including Verizon Wireless and/or the Service Partners retain title to and ownership of those Proprietary Rights and any and all improvements, modifications, fixes or enhancements made by or for Networkfleet, its affiliates and/or the Service Partners to the Devices, the Networkfleet Service or the Networkfleet Website and grant such Customers a limited license for purposes of utilizing the services for the purposed outlined in this agreement. Customer will not copy, modify, reverse-engineer, disassemble or decompile any software or firmware included in any Device or the Networkfleet Website or otherwise provided to Customer by or on behalf of Networkfleet, and will not disclose such software or provide access to the Devices, such software or any Networkfleet Services to any third party for such a purpose. Customer agrees that with respect to the Networkfleet Services, it shall not, nor shall it permit any third party to (a) assign, transfer, lease, rent, sell, distribute or import such Networkfleet Services to any third party; (b) except with the express written consent of Verizon Wireless, combine, embed or incorporate the Networkfleet Services into any other product or service other than any Customer-owned or developed interface for purposes of receiving the data feed delivered from the Networkfleet Devices; (c) reverse engineer, translate, convert, decompile the Networkfleet Services; (d) remove or alter any proprietary notices in the Networkfleet Services; (e) use the Networkfleet Services in connection with the transmission, sale, license, or delivery of any infringing, defamatory, offensive, or illegal products, services, or materials; (f) use the Networkfleet Services in any manner that threatens the integrity, performance, or availability of the Networkfleet Service; or (g) use the Networkfleet Service in any manner that violates local, state or federal laws, regulations or orders. The Networkfleet Website includes aerial, satellite imagery from Digital Globe, one of the Service Partners, as a mapping option. If Customer uses such mapping option, Customer agrees to comply with the terms of use contained in Digital Globe's End User License Agreement reference Networkfleet MAXAR DigitalGlobe attached hereto.

May 14, 2021

**10. MODIFICATIONS; WEBSITE MAINTENANCE.** Networkfleet may alter or modify all or part of the Devices, the Networkfleet Services or the Networkfleet Website from time to time; provided such changes do not materially adversely affect Customer's use of the Networkfleet Services or Networkfleet Website. Subject to the foregoing, such changes may include, without limitation, the addition or withdrawal of features, information, products, services, software or changes in instructions. Networkfleet reserves the right to perform scheduled maintenance for the Networkfleet Services and Networkfleet Website from time to time. This may include application and database maintenance as well as general website maintenance and may or may not involve Networkfleet Website and Networkfleet Services unavailability.

**11. DATA.** Customer represents and warrants that it has all rights and authority with respect to the data Verizon Wireless, Networkfleet, and the Service Partners acquire and transmit through Customer's use of the Devices, the Networkfleet Services and the Networkfleet Website ("Business Data") and grant the rights and approvals set forth in this Agreement and further grants to Verizon Wireless, Networkfleet, its affiliates and the Service Partners the nonexclusive, license and right to collect, access and use Business Data, and to access, copy and use the Business Data in the course of performing the Networkfleet Services and to analyze, measure and optimize the performance of the Devices and the Networkfleet Services and to develop new offerings for Customer and others and for other purposes of Networkfleet and its affiliates, including the development of data products for sale, licensing and distribution to third parties during the term of its contract with the Customer; provided, however, that except as may be required under law or court order, Networkfleet will not disclose or distribute Business Data to a third party in a form that permits identification of Customer.

**12. EXPORT CONTROL.** Customer understands and agrees that: (i) the software used in connection with the Service is controlled by US export control laws; (ii) further transfer or export of the software may be subject to US export control laws or similar laws of other countries; (iii) Customer will abide by such laws; and (iv) Customer will not re-export or divert the software to a country or activity in contravention of U.S. law. Customer represents and warrant that: (i) Customer is not now located in, does not maintain an office or residence in, is not a citizen of, nor does Customer intend to travel to (without agreeing to follow any specific federal regulatory parameters on such travel), any of the following countries: Cuba, Iran, North Korea, Sudan, Syria, or other locations where the United States or other governments may have restrictions; and (ii) Customer is not, nor does Customer anticipate being, listed on any U.S. Government, United Nations or other country's prohibited parties list (including, but not limited to the U.S. Department of Commerce Denied Persons List or Entity List and the U.S. Treasury Department's Specially Designated Nationals, Terrorists or Narcotics Traffickers List).

**13. OWNERSHIP AND ACCEPTANCE.** Title transfer and acceptance of products and services occur upon shipment or provision of service.

**14. GENERAL.** (a) No amendment, change, modification or waiver to any provision of any accepted order or these Terms and Conditions will be binding unless signed by an authorized representative of each party. (b) The parties' respective rights and obligations under Sections 7. DISCLAIMER OF WARRANTIES, 9. PROPRIETARY RIGHTS, and 11. DATA survive termination of an order.

## Call Filter Service Attachment to Verizon Wireless Agreement: Government Terms of Service

This Call Filter Service Attachment ("Call Filter Attachment") to the Agreement between Customer and Verizon Wireless sets forth the terms and conditions specific to the Call Filter Service (described below) to be provided by Verizon Wireless to Customer hereunder. If there are any inconsistencies between this Call Filter Attachment and the Agreement, this Call Filter Attachment shall control with respect to the Call Filter Service functionality or operation. Any capitalized but undefined terms used in this Call Filter Attachment shall have the meanings given such terms in the Agreement.

- 1. Call Filter Service Overview.** Verizon Wireless's Call Filter Service allows Customer to take manage its calls (the "Service").
- 2. Call Filter and Call Filter Plus Service Description.** Call Filter is available to Customer for no additional monthly charges, and provides spam protection (spam alerts, blocking and reporting). Call Filter Plus provides added protection with caller ID and other premium features for a monthly charge, which are set forth in the Call Filter Plus Service Fees exhibit attached hereto. Call Filter utilizes network-based functionality to provide spam alerts and caller ID information on Customer's devices, and will not require the Call Filter application for these features. Spam blocking and other enhanced spam protection tools require the Call Filter application and a compatible device. Availability of certain features will vary depending on the device. Basic phones will receive network-based spam protection. Call Filter requires Verizon Wireless's 4G LTE network; limited features of the Service may be available if Customer is roaming on a VoLTE network outside of Verizon Wireless's 4G coverage area.
- 3. Call Filter Limitations.** Call Filter is not available for incoming calls from restricted or unlisted numbers. Call Filter does not detect spam calls from international numbers, but Customer may choose to block calls from international numbers. Call Filter

utilizes analytics and databases that are continually evolving, including spam reporting by customers. Call Filter may not work with some of our other services like NumberShare or eSIM lines.

4. **Spam Protection and the Call Filter Application.** Call Filter will alert Customer when Customer receives potential spam calls and allows Customer to turn on the spam filter to automatically block (send directly to voicemail) spam calls based on Customer's preferred risk level (as determined by Customer in the Call Filter application). If Customer enrolls in Call Filter through the Call Filter application, Verizon will automatically turn on Customer's spam filter to block all high-risk spam calls, but Customer can always turn off or adjust the blocking within the Call Filter application. Call Filter Plus, provides additional protection with caller ID for unknown numbers, access to a risk assessment meter for each spam call, reverse spam number lookup, and additional categories of spam alerts including "Robo Caller" or "Potential Fraud." With Call Filter Plus, depending upon Customer's device, Customer may also be able to view a list of callers that have been identified as spam or blocked, and block and un-block specific numbers. Call Filter's spam detection and block management may inadvertently mislabel or block legitimate callers including those to whom Customer may have given consent to communicate with via Customer mobile number. Customer should check Customer voicemail to determine if the caller is legitimate (if they left a voice message and if Customer have voicemail enabled). Verizon Wireless does not guarantee that all calls that are spam will be detected. Customer's spam settings such as spam filters and personal block and spam lists will be permanently deleted once Customer changes devices, uninstalls the Call Filter application, unsubscribes or downgrades the Service, or in the case of Android users, disables the Call Filter application or clear application cache or data.
5. **Caller ID.** Caller ID, available with Call Filter Plus, displays the name, phone number, city and state of a caller's phone number, if these details are available and supported by Customer's device. Some devices may only display the caller's name as the Call Filter may not be available on all devices. Some devices also allow identification of text messages when using an eligible messaging application. Android users may also see the caller's uploaded photo if available.
6. The caller's identity may not show if they are labelled as Robo Caller, Potential Spam or Potential Fraud on certain operating systems. Customer's saved contact names will show instead of the caller identification (so if a call would normally show as a Robo Caller with the Service, but is in Customer's list of contacts, that contact name will show instead). If Customer uploads a photo, Customer's photo will be seen by other Verizon Wireless customers that use the Service but will not override a Customer's contact photo (uploading is not available for all devices).
7. **Data Charges.** Subject to the Agreement, data charges may apply for download of the application and use of the Service. Call Filter does not operate on Wi-Fi, so data charges may apply when using the Service even if Customer device is also connected to Wi-Fi. If Customer's device is eligible for the uploading or receiving of a picture, data charges apply to such uploading and also for receiving pictures. Such data charges will be billed to Customer's Verizon Wireless account according to Customer's data plan. The Service will automatically renew every month unless canceled. For Call Filter Plus, Customer will be billed a Monthly Access Fee as specified in the Call Filter Plus Service Fees exhibit.
8. **Privacy.** Verizon Wireless may use information about Customer's activity in the Service, subject to our Privacy Policy, please refer to the attached Verizon Full Privacy Policy. In order to provide the Service to Customer, Verizon Wireless will access the following information: MTN, contacts, call log, and messages (Android devices only). Verizon Wireless does not share information for any other purposes other than to render the Service. While a Customer end user can review or turn off these permissions at any time in the device settings, without access to that information, the Service will not be provided to that device.
9. **Licenses and Restrictions.** Call Filter is the property of Verizon Wireless or its licensors. Call Filter software and any application installed on Customer devices are licensed and not sold to Customer. Verizon Wireless and its licensors grants to Customer a limited, non-exclusive, revocable, non-transferable, personal, non-commercial license to use the Service for its intended use, in the United States.
10. **Restrictions on Use.** Customer will not, or permit anyone else to, sell, resell, distribute, sublicense, loan, lease, otherwise transfer, alter, modify, merge, adapt, copy, delete, record, translate, publish, upload, transmit, export, create derivative works of, make any commercial use of, reverse engineer, decompile, attempt to derive the source code, or disassemble the Service of any software that forms part of the Service. Customer may not use the Service or any part of it for any improper use (including infringement of copyright or other intellectual property rights) and must follow all laws. Customer will not alter, disable, or circumvent any features embedded in the software. All rights not expressly granted to Customer herein are reserved. Verizon Wireless may revoke this license at any time without notice.

11. **Branding.** All trademarks, service marks, trade names, logos, domain names, and any other features of Verizon Wireless's brand are the sole property of Verizon Wireless and Verizon Wireless does not grant any rights to such branding to Customer for any use at all. Customer may not remove or alter any copyright, trademark, or other intellectual property notices of the Service.
12. **User Content.** For certain eligible devices, the Service allows Customer to upload a photo to display. Customer may choose to attach a photo from Customer own photo gallery, a new photo that Customer take, or a photo available for use from an Internet search that Customer conducts. Customer is responsible for any content that Customer uploads to the Service. Verizon Wireless does not monitor or control the content Customer chooses to send via the Service and, Verizon Wireless disclaims all responsibility for such content. Photos that Customer did not take may be subject to copyright protection which limits or prohibits their copying, transmission and/or use. Customer agrees that Customer will not attach copyrighted content in a way that infringes any copyright, and that Customer is wholly responsible for any copyright infringement resulting from Customer's conduct. If Customer is unsure about whether Customer's conduct is lawful, Customer should not attach the content.
13. **Digital Millennium Copyright Act Notice.** If Customer believe that Customer content has been improperly used in the Service in a way that constitutes copyright infringement please contact Verizon at the address below. Pursuant to Title II of the DMCA, all claims alleging copyright infringement for material that is believed to be residing on Verizon's system or network should be promptly sent in the form of written notice to Verizon's Designated Agent. The Designated Agent for DMCA Notice is:

Verizon Copyright Department  
 1320 North Courthouse Road, Floor 9  
 Arlington, Virginia 22201, U.S.A.  
 Fax 703.351.3669  
 Email [DMCA@verizon.com](mailto:DMCA@verizon.com)

**NOTE:** No other notices or communications should be sent to the Designated Agent, who is appointed solely for the purpose of receiving notices of claims alleging copyright infringement under the DMCA. Specific requirements for proper notification of claimed infringement are set forth in the DMCA (see 17 U.S.C. § 512(c)(3)). Valid notification must be a written communication that includes all of the following elements:

1. Signature of copyright owner or person authorized to act on behalf of the owner;
2. Identification of copyrighted work claimed to be infringed;
3. Identification of the material claimed to be infringing or to be the subject of infringing activity and information reasonably sufficient to permit the service provider to locate the material;
4. Information reasonably sufficient to permit the service provider to contact the complaining party (address, phone number and, if available, email address);
5. A statement that the complaining party has a good faith belief that use of the material in the manner complained is not authorized by the copyright owner, its agent, or the law; and
6. A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of the exclusive right allegedly being infringed.

It is the policy of Verizon that upon receipt of a valid DMCA notice Verizon will remove or disable access to allegedly infringing material. There are substantial penalties for false claims (see 17 U.S.C. § 512(f)).

14. **Open Source and Third Party Licenses.** Customer's use of the Service is subject to open source licenses that form part of the Service. Certain software or technical information is licensed from third parties, and may be covered by one or more U.S. Patents, pending U.S. patent applications, and pending counterpart European and international patents. The open source licenses that form part of the Service. Please refer to the Call Filter open source licenses attached hereto. :
- [This link is broken. Our technical team reached out to the vendor and that vendor is working on the links, but it has not yet been resolved.
  - 
  - This link is broken. Our technical team reached out to the vendor and that vendor is working on the links, but it has not yet been resolved.

15. **Termination.** Subject to the dispute resolution provision in the Agreement, Verizon may limit, suspend, terminate or discontinue the Service, or certain features or functions of the Service, at any time without notice, including if Customer breaches this Call Filter Attachment. Customer may terminate Customer's use of the Service at any time by unsubscribing to the Service.
16. **DISCLAIMER OF WARRANTIES.** THE SERVICE AND ANY INCLUDED APPLICATION IS PROVIDED BY VERIZON OR ITS LICENSORS 'AS IS', WITHOUT WARRANTIES, EXPRESS OR IMPLIED, OR CONDITIONS OF ANY KIND, INCLUDING FOR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CUSTOMER USES THE SERVICE AT ITS OWN RISK. VERIZON WIRELESS AND ITS LICENSORS, AND VENDORS MAKE NO WARRANTY, EITHER EXPRESS OR IMPLIED, AS TO THE ACCURACY, AVAILABILITY, COMPLETENESS, USEFULNESS, SECURITY, RELIABILITY, INTEROPERABILITY, OR THAT THE SERVICE WILL BE UNINTERRUPTED, VIRUS FREE, OR COMPATIBLE WITH YOUR DEVICE OR THAT THE SERVICE WILL MEET YOUR EXPECTATIONS AT ALL OR AS TO THE IDENTIFICATION, LABELING, SPAM OR BLOCK MANAGEMENT, OR BLOCKING OF CALLS. VERIZON WIRELESS AND ITS LICENSORS, AND VENDORS DO NOT PROVIDE ANY WARRANTY (EXPRESS OR IMPLIED) OR GUARANTEE THAT ALL SPAM, ROBOCALLER AND FRAUDULENT CALLERS WILL BE IDENTIFIED, LABELED CORRECTLY OR BLOCKED. THE SERVICE COULD CAUSE DAMAGE TO CUSTOMER, ITS DATA, DEVICES, SOFTWARE OR HARDWARE.
17. **LIMITATIONS OF LIABILITY.** TO THE MAXIMUM EXTENT ALLOWED BY LAW, THE LIABILITY OF VERIZON WIRELESS OR ITS LICENSORS, AND VENDORS FOR MONETARY DAMAGES FOR ANY CLAIMS, THAT CUSTOMER MAY HAVE UNDER THESE TERMS ARE LIMITED TO NO MORE THAN THE PROPORTIONATE AMOUNT OF THE SERVICE CHARGES ATTRIBUTABLE TO THE AFFECTED PERIOD, AND THE MAXIMUM IN DAMAGES RECOVERABLE SHALL BE TEN (\$10) U.S. DOLLARS. UNDER NO CIRCUMSTANCES ARE VERIZON WIRELESS, ITS LICENSORS, AND VENDORS LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, PUNITIVE, MULTIPLE, OR SPECIAL DAMAGES OF ANY NATURE WHATSOEVER INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOST DATA, REPUTATION, LOSS OF BUSINESS, OR COST OF REPLACEMENT PRODUCTS AND SERVICES ON ANY THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE SERVICE OR THE INABILITY TO USE THE SERVICE IN ANY WAY WHETHER FORESEEABLE OR NOT OR WHETHER ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. VERIZON WIRELESS SHALL NOT BE LIABLE FOR ANY DAMAGES, COSTS OR PENALTIES (DIRECT OR INDIRECT) AS A RESULT OF MIS-IDENTIFICATION, MIS-MANAGEMENT OR BLOCKING OF A CALLER OR FAILURE TO PROPERLY IDENTIFY, MANAGE OR BLOCK A CALLER.
18. **[Reserved]**
19. **Export Control.** Use of the Service may be subject to the export and import laws of the United States and other countries. Customer agrees to comply with all applicable export and import laws and regulations. By using the Service and/or by downloading the applicable Application, Customer agrees that Customer are not located in, under the control of, or a resident or national of any country, or person, on the United States Treasury Department's list of Specially Designated Nationals or the United States Commerce Department Table of Deny Orders. Customer also agrees that Customer are not located in a country that is subject to the U.S. government embargo, or that is designated by the U.S. as a terrorist supporting country and Customer are not listed on any U.S. government list of prohibited or restricted parties. Customer agrees also not to attempt to export or import any encrypted information, materials, hardware or software.
20. **Safety.** Customer must not endanger either Customer or others by using the Service while driving or engaging in any other activity that requires Customer's full attention.

### Verizon Push to Talk Responder (PTT Responder) Terms and Conditions

This Agreement is between you, as our Customer or End User, and Verizon Wireless ("VZW") and it sets forth the terms and conditions under which you agree to use and we agree to provide PTT Responder, a mission-critical push to talk solution (also known as the "Service"). By using or accessing PTT Responder, you accept these Terms & Conditions. VZW may change these terms and conditions from time to time as permitted by applicable law. By continuing to use the Service after VZW has notified you of changes, you are accepting those changes.

1. **Customer Agreement.** For business customers, PTT Responder is subject to your company's major account agreement with VZW.

2. **How the Service Works.** You can access PTT Responder in the following ways: (i) through a mobile application (the "**Mobile App**"), or (ii) by downloading computer software from the VZW website (the "**Computer Client**"). Not all PTT Responder service features are available through all access methods.
3. **Charges.** Your download of PTT Responder will be billed according to the applicable data plan. Your use of PTT Responder will be billed according to the monthly recurring fee that you agreed to pay, and use on certain devices will be billed according to the applicable data plan. For a list of those devices that will be billed according to your data plan, please see the Public Safety Services document attached
4. **Privacy.** VZW may use information about your activity in PTT Responder, subject to our Privacy Policy and applicable law attached hereto. .
5. **Licenses.** Mobile App, Computer Client, or any other executable associated with your access or use of PTT Responder is referred as "PTT Responder Software". You have a limited, non-exclusive, non-transferable license to use PTT Responder in the U.S. and the object code version of PTT Responder Software solely for the purposes for which it is provided and only in accordance with all documentation provided by VZW or its licensors or suppliers and, for the sake of clarity, is not for resale and is not sublicensable. The PTT Responder Software contains some programming, scripts, tools, modules, libraries, components, or other items that were developed using "Open Source" code, and information about these items is available in the attached Open Source document. . Nothing in this Agreement will be construed to limit any rights granted under such open source licenses.
6. **Maps.** If you are using PTT Responder Dispatcher Request Location from Client and PTT Responder Dispatch with MAP Integration as standalone products (not in conjunction with Push to Talk Plus), such use will require use of OpenStreetMap (© OpenStreetMap contributors). Use of OpenStreetMap within PTT Responder is subject to the Open Data Commons Open Database License (ODbL) licensed by the OpenStreetMap Foundation (OSMF). Please refer to the attached Open Street map document. . The ODbL may be updated from time to time and are incorporated into these Terms and Conditions by reference, as if set forth fully herein. If you do not accept the ODbL including all limitations and restrictions therein as may be updated by OpenStreetMap from time to time, you may not use PTT Responder. Your use of the OpenStreetMap service within PTT Responder will constitute your acceptance of the ODbL. If there is a conflict between these Terms and that license, the ODbL license terms will control.
7. **Consent to Share Location Information.** PTT Responder Dispatcher Request Location from Client and PTT Responder Dispatch with MAP require sharing of your "Location Information" (data that can be used to describe, determine or identify the location of the mobile device you use while accessing PTT Responder). With your consent, your Location Information will be shared with your employer, for business purposes only.
8. **Additional Terms for Device Call Logging and Recording.** For PTT Responder, the Device Call Logging and Recording feature within PTT Responder permits your employer to log and record your calls while you are using a mobile device with PTT Responder. By using PTT Responder, you consent to calls on your mobile device being logged and recorded by your employer, and you consent to any person authorized by your employer listening to your conversation(s) for training and other legitimate business purposes. Employers shall restrict access to the Device Call Logging and Recording feature of PTT Responder to only authorized employees, who shall only use the feature during business hours for training and other legitimate business purposes.
9. **Restrictions on Use.** You may not, or allow others to (i) transfer, assign or sublicense its license rights to any other person or entity or use the PTT Responder Software on any equipment other than the equipment on which it was originally installed, and You acknowledges that any attempted transfer, assignment, sublicense or use shall be void; (ii) make error corrections to or otherwise modify or adapt the PTT Responder Software, create derivative works based upon the PTT Responder Software, or permit third parties to do the same; (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the PTT Responder Software to human-readable form or attempt to reconstruct or discover the source code, underlying ideas or algorithms of any components of the PTT Responder Software, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction; (iv) use or permit the PTT Responder Software to be used to perform services for third parties, whether on a service bureau or time-sharing basis or otherwise, without the express written authorization of Verizon; (v) remove or obscure any proprietary notices from the PTT Responder Software, documentation or other materials furnished or made available hereunder; (vi) disclose, provide, or otherwise make available trade secrets contained within the PTT Responder Software and documentation in any form to any third party without the prior written

consent of Verizon; (vii) enable any PTT Responder Software features or capacity (e.g., additional storage hours, agents, ports or mailboxes) which is licensed as separate products without Verizon's prior written consent; and/or (viii) permit or encourage any third party to do any of the foregoing. Customer shall implement reasonable security measures to protect such trade secrets.

10. **Termination.** VZW may terminate or discontinue PTT Responder at any time without notice, including if you breach these Terms and Conditions, subject to the applicable contracts disputes act if you are a government entity.
11. **Disclaimer of Warranty; Limitation on Liability.** PTT RESPONDER AND ANY INCLUDED SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTIES, EXPRESS OR IMPLIED, OF ANY KIND BY EITHER VZW OR ITS LICENSORS OR SUPPLIERS. VZW'S LIABILITY SHALL BE LIMITED AS SET FORTH IN THE CUSTOMER AGREEMENT (AND THE LIABILITY OF EACH VZW LICENSOR AND SUPPLIER SHALL BE LIMITED TO THE SAME EXTENT).
12. **Export Control.** You shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and not export, or allow the export or re-export of PTT Responder in violation of any such restrictions, laws or regulations. By downloading or using PTT Responder, you agree to the foregoing and you represent and warrant that you are not located in, under the control of, or a national or resident of any restricted country or on any restricted parties list.
13. **Safety.** Please do not endanger yourself and others by using PTT Responder while driving or engaging in any other activity that requires your full attention.

## Verizon Local Network Command Terms and Conditions

1. GENERAL
  - 1.1 Service Definition
  - 1.2 Service Availability
2. SUPPLEMENTAL TERMS
  - 2.1 Customer Agreement
  - 2.2 Privacy
  - 2.3 Licenses
  - 2.4 Consent to Share Location Information
  - 2.5 Disclaimer of Warranty; Limitation of Liability
3. CUSTOMER RESPONSIBILITIES
  - 3.1 Restrictions on Use
4. FINANCIAL TERMS
  - 4.1 Responsibility for Charges

### 1. GENERAL

- 1.1 **Service Definition.** Local Network Command is a local control solution allowing for temporary uplift of mobile devices to enhanced network performance (also known as the "Service").
- 1.2 **Service Availability.** You can access the Service through a web-based tool hosted at the VZW MyBiz portal. The account single point of contact (SPOC) must preselect the users for uplift through the Service. The account SPOC can preselect users individually or as part of a group. The account SPOC must also create and designate specific users as Incident Commanders. Incident Commanders will have the ability to create incidents using the Service and uplift preselected users during an incident.

### 2. SUPPLEMENTAL TERMS

- 2.1 **Customer Agreement.** For enterprise customers, the Service is subject to your organization’s major account agreement with VZW.
- 2.2 **Privacy.** VZW may use information about your activity in using the Service, subject to our Privacy Policy and applicable law, which are attached hereto
- 2.3 **Licenses.** You have a limited, non-exclusive, non-transferable license to use the Service solely for the purposes for which it is provided and only in accordance with all documentation provided by VZW or its licensors or suppliers.

For Location Information (defined below), the Service requires use of MapQuest. Use of MapQuest within the Service is subject to:

- the MapQuest Terms of Service attached hereto
- the MapQuest 3rd Party Notices and Licenses MapQuest Attributions attached hereto.,
- the Mapbox Notices MapQuest Mapbox as attached hereto, and
- the MapQuest Privacy Policy MapQuest System1 Privacy Policy as attached hereto

The MapQuest Terms of Service, MapQuest 3rd Party Notices and Licenses, Mapbox Notices and MapQuest Privacy Policy may be updated from time to time and are incorporated into these Terms and Conditions by reference, as if set forth fully herein. If you do not accept the MapQuest Terms of Service, MapQuest 3rd Party Notices and Licenses, Mapbox Notices or MapQuest Privacy Policy, including all limitations and restrictions therein as may be updated by MapQuest from time to time, you may not use the Service. Your use of MapQuest within the Service will constitute your acceptance of the MapQuest Terms of Service, MapQuest 3rd Party Notices and Licenses, Mapbox Notices and MapQuest Privacy Policy

- 2.4 **Consent to Share Location Information.** The Service will require sharing of “Location Information” (data that can be used to describe, determine or identify the location of all mobile devices subject to the Service). In using the Service, you represent and warrant that you have obtained all necessary consent(s) from individual users whose mobile devices will be subject to the Service, and that VZW has no responsibility to obtain such consent(s).
- 2.5 **Disclaimer of Warranty; Limitation of Liability.** THE SERVICE IS PROVIDED ‘AS IS’, WITHOUT WARRANTIES, EXPRESS OR IMPLIED, OF ANY KIND BY EITHER VZW OR ITS LICENSORS OR SUPPLIERS. VZW’S LIABILITY SHALL BE LIMITED AS SET FORTH IN THE CUSTOMER AGREEMENT (AND THE LIABILITY OF EACH VZW LICENSOR AND SUPPLIER SHALL BE LIMITED TO THE SAME EXTENT).

### 3. CUSTOMER RESPONSIBILITIES

- 3.1 **Restrictions on Use.** You may not, or allow others to, adapt, alter, modify, de-compile, reverse engineer, translate, or create derivative works of the Service. The Service is intended for those devices with a clear need for temporary uplift to enhanced network improvement. You agree not to abuse the Service as determined by the sole discretion of Verizon. “Abuse” may include, but not be limited to, the indiscriminate uplift of all devices within a specific geographic area where such action adversely affects the Verizon wireless network.

### 4. FINANCIAL TERMS

- 4.1 **Responsibility for Charges.** Your use of the Service will be billed according to the monthly recurring fee that you agreed to pay, and use on certain devices will be billed according to the applicable data plan. For a list of those devices that will be billed according to your data plan

## VERIZON DNS SAFEGUARD for PUBLIC SAFETY

### 1. GENERAL

#### 1.1 Service Definition

- 1.2 Service Features for DNS Service Plus
- 1.3 Service Features for DNS Service Advanced
- 2. SUPPLEMENTAL TERMS
  - 2.1 Service Activation and Implementation
  - 2.2 Services Agreement Flow Down Terms
  - 2.3 Customer Responsibilities
  - 2.4 Warranties
  - 2.5 Use of Data
  - 2.6 Term and Termination
- 3. FINANCIAL TERMS
  - 3.1 General
- 4. DEFINITIONS

## 1. GENERAL

**1.1 Service Definition.** Verizon DNS Safeguard for Public Safety (DNS Service) is a cloud-based security platform intended to provide a first line of defense against threats on the Internet by detecting and blocking inappropriate and malicious sites and content before the Internet Protocol (IP) connections are established. DNS Service is enhanced with threat intelligence feeds from the Verizon Threat Research Advisory Center which, learning from internet activity patterns, automatically uncovers current and emerging threats to continually keep the network safe.

The DNS Service platform operates as a DNS resolver that converts domain names to IP addresses which allows the platform to prevent IP connections to known malicious sites. When a legitimate domain is resolved, the DNS Service returns the actual IP address.

The DNS Service consists of two offerings: DNS Service Plus and DNS Service Advanced.

**1.2 Service Features for DNS Service Plus.** The following service features are included with DNS Service Plus:

**1.2.1 DNS Layer of Breach Protection.** DNS Service is able to detect and block malicious sites and content before they reach the network as a DNS request is made before IP connections are established. Malware, ransomware, phishing, spyware, botnets, and command & control call-backs are blocked over any port or protocol before such threats can reach users and network.

**1.3 Service Features for DNS Service Advanced.** The following service features are included with DNS Service Advanced.

- 1.3.1 **Premium Threat Feeds.** DNS Service Advanced includes the Basic Threat Feeds described in the DNS Service Plus and additional threat feeds from the Verizon Threat Research Advisory Center's display of threat analytics and intelligence it gathers from third party proprietary and open source data.

## 2. SUPPLEMENTAL TERMS

### 2.1 Service Activation and Implementation

- 2.1.1 **Service Activation.** The DNS Service will begin Activation Date is 10 Business Days following the Order Confirmation Date.
- 2.1.2 **Offshore Support.** Customer agrees that the DNS Service may be provided by, and all related information (including data) accessed and/or stored by, resources located within and outside the United States. Customer consents to such performance of services, including access and storage of data, from outside the United States.

### 2.2 Services Agreement Flow Down Terms

- 2.2.1 **Acceptance of Terms.** From time to time, Verizon may update the functionality, add new features to the DNS Service, and/or change the access configuration for the DNS Services. In such event, these terms shall also apply to any upgrades or updates subsequently provided by Verizon for the DNS Services.
- 2.2.2 **Use of the DNS Services.** Customer accepts the non-assignable, non-transferable, non-sublicensable, and non-exclusive right to access and use the DNS Service only as authorized in this Agreement and related documentation for the duration of the Service Commitment and for the number of licenses purchased by and allocated to Customer.

### 2.3 Customer Responsibilities

- 2.3.1 **Internet Access.** Customer must have wireless internet access in place to use DNS Service. **Customer must have a subscription to Verizon's Responder Private Core in place to use DNS Service.**
- 2.3.2 **Prohibited Use.** Customer will not: (i) use the Services for any unlawful, unauthorized, fraudulent or malicious purpose, (ii) modify, adapt, sublicense, translate, sell, reverse engineer, decompile or disassemble any portion of the Services (except to the limited extent applicable laws specifically prohibit such restriction); (iii) bypass any measures Verizon may use to prevent or restrict access to the Services or otherwise interfere with any other party's use and enjoyment of the Services; or (iv) use Customer's account or the Services to infringe any intellectual property or other right of any other third party. Verizon may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Subject to Verizon's Privacy Policy, Verizon reserves the right at all times to disclose any information as Verizon deems necessary to satisfy any applicable law, regulation, legal process or governmental request, or to edit, refuse to post or to remove any information or materials, in whole or in part, in Verizon's sole discretion.

### 2.4 Warranties

- 2.4.1 **Verizon's Disclaimer of Warranties.** Verizon does not warrant that any network, computer systems, or any portions thereof, are secure. Verizon does not warrant that use of DNS Service will be uninterrupted or error-free or that any defect in DNS Service will be correctable or that incidents will be fully contained. Customer acknowledges that impenetrable security

cannot be attained in real-world environments and that Verizon does not guarantee protection against breaches of security, or the finding or successful prosecution of individuals obtaining unauthorized access. Verizon does not warrant the accuracy of information provided to Customer hereunder.

CUSTOMER'S USE OF THE DNS SERVICES IS AT CUSTOMER'S SOLE RISK. ALL DNS SERVICES ARE PROVIDED ON AN AS IS OR AS AVAILABLE BASIS, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERIZON EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND SATISFACTORY QUALITY. VERIZON, ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, OR SUPPLIERS MAKE NO WARRANTY THAT THE SERVICES ARE ACCURATE, TIMELY, UNINTERRUPTED, VIRUS-FREE OR ERROR-FREE, OR THAT ANY PROBLEMS ENCOUNTERED WILL BE CORRECTED. THE WARRANTIES AND REMEDIES SET FORTH IN THIS SERVICE ATTACHMENT ARE VERIZON'S EXCLUSIVE WARRANTIES AND CUSTOMER'S SOLE REMEDIES FOR BREACH OF WARRANTY, IF ANY, BY VERIZON.

2.4.2 **Customer Warranty.** Customer represents and warrants that Customer (a) will use the DNS Safeguard services, including all reporting, deliverables, documentation, and other information provided in connection with DNS Service solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including public internet service provided by Verizon and Customer will not market, sell, distribute, lease, license or use any such deliverables, documentation or information for any other purposes; and (b) will comply with all applicable laws and regulations.

2.4.3 **Third Party Warranties.** For any third party products and/or services incorporated as part of Service, Customer will receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

2.5 **Use of Data.** As part of Customer's use of the Services, Customer will be providing certain (i) Network Data, (ii) User Data and/or Feedback. Some Network Data is necessary for the essential use and functionality of the Services. Network Data is also used to provide associated services such as technical support and to continually improve the operation, security, efficacy and functionality of the Services.

2.5.1 **User Data.** Customer grants Verizon a worldwide, royalty-free, sublicensable license to use, modify, reproduce, publicly display, publicly perform, and distribute the User Data only as reasonably required to provide the Service.

2.5.2 **Network Data.** Customer hereby grants to Verizon a non-exclusive, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use (i) the Network Data that is aggregated and de-identified so that it does not identify Customer for the purpose of enhancement of the Services, and (ii) any information that Verizon learns in evaluating Network Data to create the Statistical Data for the purpose of enhancing, developing, and/or promoting the Services.

2.5.3 **Feedback.** De-identified Feedback may be incorporated into the Services, and Customer hereby grants Verizon a non-exclusive, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use de-identified Feedback for any purpose whatsoever, including, without limitation, for purposes of enhancing, developing and/or promoting products and services, including the Services.

## 2.6 **Term and Termination**

2.6.1 **Service Commitment.** The Service Commitment is for the terms specified in the Customer's purchase order as accepted by Verizon.

2.6.2 **Service Cancellation.** If Customer requests cancellation of Service, or Verizon cancels Service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision such Service, Customer will pay any set-up fees and other amounts accrued for such Service through the date of such termination, plus an amount equal to any applicable annual third party license fee, which Customer acknowledges are liquidated damages reflecting a reasonable measurable of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

### 3. FINANCIAL TERMS

3.1 **Responsibility for Charges.** Your use of the Service will be billed according to the monthly recurring fee that you agreed to pay, and use on certain devices will be billed according to the applicable data plan. For a list of those devices that will be billed according to your data plan.

## Verizon Wireless Private Network Terms and Conditions

1. **Verizon Wireless Private Network Service ("Private Network"):** Private Network extends Customer's IP network to its wireless equipment by segregating the data between such devices and Customer's servers from the public Internet (the "Internet"). Customer's use of Private Network is subject to the Private Network Roles and Responsibilities Customer Guidelines, which are available from your Sales representative.

2. **Customer Minimum Line Requirement:** Customer must maintain a minimum of 100 Machine-to-Machine lines at all times during the term of its Agreement in order to remain eligible for Private Network. If Customer falls below the 100-line minimum, Verizon Wireless reserves the right to discontinue Private Network for non-use.

3. **Connection to Verizon Wireless Facility:** Customer must establish a direct-connect circuit from its facilities to Verizon Wireless's facilities by the use of Virtual Private Network, Verizon Private IP, or Fixed End System connections. Customer is solely responsible for making arrangements with a local access provider for installation and ongoing maintenance of such a connection, with sufficient data throughput to meet Customer's anticipated data needs. Customer is also responsible for all charges incurred directly or through a third party associated with establishing the connection, as well as for accessing Private Network, including Internet access fees, hardware, software, license fees, and telecommunications charges.

4. **Customer Provided Equipment ("CPE"):** Customer must procure routers and any other CPE that meet Verizon Wireless requirements for Private Network connectivity. Customer is responsible for ensuring any CPE meets its data capacity and throughput needs.

5. **IP Addresses:** Customer is responsible for procuring private IP addresses, which must be communicated to Verizon Wireless during implementation. Private Network supports static and dynamic addressing for 1X service and/or EVDO service; 4G LTE service; and Internet addressing system Internet Protocol version 4. Direct Internet access requires static IP addressing.

6. **Dynamic Mobile Network Routing ("DMNR"):** DMNR allows configuration of Private Network for dynamic routing to the subnets it serves (up to eight) to other devices on Customer's network and as support for mobile or stationary routers. DMNR is based off Mobile IPv4-based Network Mobility protocol and requires the router to be configured to support this capability. Customer is responsible for any charges associated with the customization of its CPE to support DMNR.

7. **Service Based Access ("SBA"):** SBA is an optional configuration of Private Network that enables customers to access Verizon's Visual Voice Mail; multimedia messaging services; and 3G location-based services assisted Global Positioning System. Customer is responsible for any charges associated with the customization of its CPE to support SBA.

## Verizon Wireless Private Network Traffic Management

8. **Private Network Traffic Management (PNTM):** PNTM allows Customer to configure its Private Network to allow differentiated Quality of Service (QoS) by application over Verizon Wireless's LTE network using standards-based IP packet marking. Customer can identify applications on its 4G LTE devices to get priority QoS over its Private Network. Verizon Wireless makes no guarantee of PNTM bandwidth allocations, which are subject to the limitations of wireless service availability as detailed in the Agreement. Customer is responsible for any charges associated with the customization of its CPE to support PNTM.

- a. **PNTM for Public Safety:** Eligible public safety accounts can take advantage of priority access to a data channel over the Wireless Service for its data traffic during times of heavy network demand. While PNTM for Public Safety enables a dedicated data channel, Verizon Wireless makes no guarantee of Wireless Service availability, which is subject to the limitations of wireless service availability as detailed in the Agreement. PNTM for Public Safety is only available to Customers approved by Verizon Wireless that qualify as Public Safety Entities classified by the following Qualifying Public Safety NAICS codes a) 621910 Ambulance Services; b) 922110 Courts; c) 22120 Police Protection; d) 922130 Legal Counsel and Prosecution; e) 922140 Correctional Institutions; f)

922150 Parole Offices and Probation Offices; g) Fire Protection; h) 922190 Other Justice, Public Order, and Safety Activities or i) National Security.

**9. Customer Private Network Contact:** Customer must designate a Private Network representative and provide contact information, including a phone number and email address. The Private Network contact will work with the Verizon Wireless solution engineer through the Private Network implementation and testing processes detailed below. The contact shall be available during business hours and any other time period that Customer utilizes Private Network for the purpose of assisting to resolve service problems and trouble shooting.

**10. Private Network Implementation and Testing:** Verizon Wireless will implement Customer's Private Network, which requires Customer to a) provide any information (e.g., account numbers, IP address ranges, router/CPE information) necessary to complete the Private Network Connectivity Form; b) participate in a Private Network turn-up call to ensure that CPE is properly configured to support the Private Network connection; and c) participate in a Solution Validation call to confirm that Private Network is working properly from Verizon Wireless to Customer's applications.

**11. Wireless Devices/Network Access:** Customer must use Private Network-compatible end-user Equipment and at Customer's expense must submit any devices not identified as Private Network compatible to Verizon Wireless, for network testing and Private Network certification. Private Network functionality is available on the Verizon Wireless 3G and 4G data network, subject to the limitations defined in this Addendum. While Private Network functionality may also be available on the networks of Verizon Wireless's domestic and international roaming partners, Verizon Wireless makes no representation of Private Network availability or reliability on such networks.

**12. Permitted Use/Fraud:** Customer shall use Private Network only for lawful purposes and shall not send or enable via the Private Network connection, by way of example, any SPAM, viruses, worms, trap doors, back doors or timers, nor shall Customer engage in any mail-bombing or spoofing via Private Network. Customer is responsible for the security of its network and end-user devices and is responsible for any unauthorized access to the Private Network. Verizon Wireless will treat any traffic over the Private Network as authorized by Customer. Verizon Wireless reserves the right but is not obligated to filter fraudulent usage.

**13. Maintenance/Service Changes/Termination of Private Network Service:** Verizon Wireless may limit access to Private Network in order to perform maintenance to the service and will use reasonable efforts to provide Customer with prior notice of such maintenance. With reasonable advance notice, Verizon Wireless has the right to modify and reconfigure Private Network as it deems necessary to enhance Customer's experience or to safeguard the Verizon Wireless network. In addition, VERIZON WIRELESS CAN WITHOUT NOTICE LIMIT, SUSPEND OR CANCEL CUSTOMER'S ACCESS TO OR USE OF PRIVATE NETWORK IF CUSTOMER VIOLATES THE RESTRICTIONS OF THIS ADDENDUM OR FOR GOOD CAUSE. Good cause includes (a) breach of the terms of this Addendum or the Agreement; (b) unlawful use of Private Network; (c) using Private Network in a way that adversely affects the Verizon Wireless network or Verizon Wireless's customers; (d) breach of an obligation of Customer to comply with any applicable federal, state and local government laws, rules and regulations, industry practices, third-party guidelines, or other applicable policies and requirements; (e) the suspension or termination by any governmental body of competent jurisdiction of Customer's service or the institution of a requirement, ruling or regulation that conflicts with this Addendum; or (f) for operational or governmental reasons.

**14. No Warranties:** Verizon Wireless makes no warranties, express or implied, with respect to Private Network, which it provides to Customer on an "AS IS" basis "WITH ALL FAULTS" and "AS AVAILABLE." The accuracy, timeliness, completeness, suitability, or availability of any aspect of Private Network cannot be guaranteed. THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE HEREBY EXPRESSLY DISCLAIMED IN THEIR ENTIRETY. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law. Verizon Wireless makes no representation that it supports any service levels with respect to the availability, performance, capacity, uptime or any similar metrics of Private Network.

**15. NO RESELLING:** Customer cannot resell Private Network /Private Network Traffic Management service(s) or allow third parties to use Private Network/Private Network Traffic Management service(s) or access Private Network/Private Network Traffic Management service(s) without prior written permission from Verizon Wireless.

**16. Subject to the Customer's Government Agreement:** The terms of this Addendum supplement the Customer's Government Agreement. The terms of the Agreement are applicable to Customer's use of Private Network. If there are any inconsistencies between the terms of this Addendum and the Customer's Government Agreement, the terms of this Addendum shall control with respect to Private Network.

Revision History		
Version	Date	Description
1.0	2/12/21	Pricing Offer
2.0	5/14/21	Best and Final Offer

**Employee Discount Supplement**

It is Verizon's intent to continue offering its Employee Program consistent with the terms and conditions provided under the current DMS 1011-008C contract, Exhibit 7.

<b>Individual-Liable Service Pricing Discount</b>	
<b>Category</b>	<b>% Discount</b>
Equipment	0
Services	19
Accessories	25*
Activation Fees	Waived
*Individual-Liable Subscribers are eligible to receive a 25% discount from the non-discounted, retail price of qualifying accessories.	



*\*Click Verizon logo from any page to return to table of contents*

## **State of Florida Contract Pricing**

**TABLE OF CONTENTS** *Click topic below*

### **Equipment:**

[\*\*SMARTPHONES\*\*](#)

[\*\*TABLETS & INTERNET DEVICES\*\*](#)

[\*\*BASIC & ONE TALK DESKPHONES\*\*](#)

[\*\*PLANS - CODES - USAGE TIERS\*\*](#)

[\*\*One Talk Plans\*\*](#)

[\*\*PUBLIC SAFETY PLANS\*\*](#)

[\*\*INTERNATIONAL RATES - Travel Pass\*\*](#)

[\*\*NUMBER SHARE\*\*](#)

[\*\*VERIZON CONNECT\*\*](#)

[\*\*MOBILE IRON\*\*](#)

[\*\*CANVAS\*\*](#)

[\*\*SAMSUNG KNOX\*\*](#)

[\*\*MAAS360\*\*](#)

[\*\*ASAVIE\*\*](#)

[\*\*LTE Vehicle Internet\*\*](#)

[\*\*Netmotion\*\*](#)

## Attachment D, Exhibit 2 - Vendor's Device List

<b>verizon</b> <sup>✓</sup>			
<i>*Click Verizon logo from any page to return to table of contents</i>			
State of Florida DMS 10/11-008C Price Plans			
CODES	DESCRIPTION	ACCESS	GUIDELINES & OPTIONAL PLAN FEATURES
<b>Nationwide Per Minute</b>			
86680	\$.049 Per Minute <b>Nationwide</b> Voice Plan-includes 600 M2M and 600 N&W	<b>\$0.00</b>	N/A on feature codes 77294, 77295, and 79740, 79407, and 72409. Must use 79789, 79790, 79791, 79780, or 79781. Please see smartphone feature codes below
80245	200 Text/Pix/Flix Messages- <b>Optional on price plan 86680 only</b>	<b>\$0.00</b>	
94976 (All current PTT)	Unlimited Push to Talk w/ Unlimited Mobile 2 Mobile .049 per min rate	<b>\$10.00</b>	<b>PTT Plus-</b> (auto attaches-81814)
<b>Smartphone Standalone Nationwide Per Minute</b>			
93445	Unlimited Nationwide Blackberry/ Smartphone Data / Unlimited Domestic Text.Pix, Flix Messaging, Unlimited Mobile 2 Mobile & Nights/Weekends (\$.052 Per Minute Nationwide Voice Plan)/Mobile Hotspot-5GB)	<b>\$35.99</b>	<b>Mobile Hotspot (5 GB auto attached)-</b> 76404 and 79048 <b>Block Mobile Hotspot-</b> 78485 <b>Optional-PTT Plus-</b> \$5 (80598 for all smartphones, 80590 for Kyocera Brigadier) <b>TXT Block -</b> 73572
<b>Smartphone All Inclusive Nationwide Price Plan</b>			
86769	Unlimited Nationwide Calling w/ Unlimited Domestic Text/Pix/Flix Messaging; Email and Data, 5GB of data hotspot/Tethering	<b>\$51.00</b>	<b>4G Smartphone -\$0 Hotspot-</b> 76065 (auto attached built into the price plan) <b>Optional-PTT Plus-</b> \$5 (80598 for all smartphones, 80590 for Kyocera Brigadier)
<b>Nationwide</b>			
86195	Nationwide 250 Anytime Min (\$.052 per min overage rate) w/ Unlimited Mobile 2 Mobile, Push 2 Talk, Nights/Weekends	<b>\$25.75</b>	<b>PTT Plus-</b> (auto attaches-81814)
86196	Nationwide 600 Anytime Min (\$.052 per min overage rate) w/ Unlimited Mobile 2 Mobile, Push 2 Talk, Nights/Weekends	<b>\$36.05</b>	<b>PTT Plus-</b> (auto attaches-81814)
86197	Unlimited Nationwide Calling w/ Unlimited Push 2 Talk	<b>\$51.50</b>	<b>PTT Plus-</b> (auto attaches-81814)
22901	4G Custom Nationwide Unlimited Mins+Msg Unlimited Data +Email MHS	<b>\$50.00</b>	<b>TravelPass compatible.</b>
<b>Features</b>			
<b>Smartphone Data Features</b>			
77294	500 MB Data allowance (\$.00849 per MB overage rate) Unlimited Domestic Text/Pix/Flix Messaging	<b>\$15.45</b>	Cannot be used with 86680 \$.049 plan. Required to be used with a minimum \$9.99 access
79789	500 MB Data allowance (\$.00849 per MB overage rate)	<b>\$15.45</b>	Avl on all plans. Does not include Txt, Pix, or Flix. Use block code 54307 to block SMS
77295	1,000 MB Data allowance (\$.00849 per MB overage rate) Unlimited Domestic Text Messaging	<b>\$20.60</b>	Cannot be used with 86680 \$.049 plan. Required to be used with a minimum \$9.99 access
79790	1000 MB Data allowance (\$.00849 per MB overage rate)	<b>\$20.60</b>	Avl on all plans. Does not include Txt, Pix, or Flix. Use block code 54307 to block SMS
79740	2,000 MB Data allowance (\$.00849 per MB overage rate) Unlimited Domestic Text Messaging	<b>\$23.69</b>	Cannot be used with 86680 \$.049 plan. Required to be used with a minimum \$9.99 access
79791	2000 MB Data allowance (\$.00849 per MB overage rate)	<b>\$23.69</b>	Avl on all plans. Does not include Txt, Pix, or Flix. Use block code 54307 to block SMS
79407	Unlimited MBB Data Plan w/ Unlimited Domestic Text Messaging	<b>\$32.96</b>	Cannot be used with 86680 \$.049 plan. Required to be used with a minimum \$9.99 access
79781	Unlimited MBB Data Plan	<b>\$32.96</b>	Avl on all plans. Does not include Txt, Pix, or Flix. Use block code 54307 to block SMS
<b>Messaging Features</b>			
77847/77848	\$0.02 Per SMS messaging rate/\$0.05 Per MMS messaging rate	<b>\$0.00</b>	
77328	300 SMS/MMS Messages (.05 Per Message overage rate)	<b>\$2.00</b>	
77341	500 SMS/MMS Messages (.05 Per Message overage rate)	<b>\$3.00</b>	
77329	Unlimited SMS/MMS Messages	<b>\$7.00</b>	
<b>Aircard/Tablet Data Packages</b>			
86226	500 MB Data allowance (\$.00849 per MB overage rate) Unlimited Domestic Text	<b>\$20.60</b>	
86227	1,000 MB Data allowance (\$.00849 per MB overage rate) Unlimited Domestic Text Messaging	<b>\$25.75</b>	
86228	2,000 MB Data allowance (\$.00849 per MB overage rate) Unlimited Domestic Text Messaging	<b>\$30.90</b>	
86229	Unlimited MBB Data Plan w/ Unlimited Domestic Text Messaging	<b>\$36.05</b>	\$0 Text Messaging code 47309 is avl to add if needed
90237	5GB Public Sector Mobile Broadband Share Plan	<b>\$34.99</b>	\$8.00 per GB overage charge and \$.002 per kilobyte National Access Roaming. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account, beginning with the line with the lowest overage need.
90240	10GB Public Sector Mobile Broadband Share Plan	<b>\$59.99</b>	\$8.00 per GB overage charge and \$.002 per kilobyte National Access Roaming. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account, beginning with the line with the lowest overage need.

## Attachment D, Exhibit 2 - Vendor's Device List

90241	20GB Public Sector Mobile Broadband Share Plan	<b>\$99.99</b>	\$8.00 per GB overage charge and \$.002 per kilobyte National Access Roaming. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account, beginning with the line with the lowest overage need.
<b>Machine to Machine</b>			
86693	\$.099 Per MB data rate for Machine to Machine or Customer provided equipment	<b>\$0.00</b>	**Do not offer for note books, tablets, ipads, etc. Must be CPE certified device or Jetpack/MiFi at MTM pricing in Equip Guide
87640	1MB Machine to Machine Share (\$1.00 per MB overage rate) Tier 1	<b>\$5.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87641	5MB Machine to Machine Share (\$1.00 per MB overage rate) Tier 1	<b>\$7.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87642	25MB Machine to Machine Share (\$1.00 per MB overage rate) Tier 1	<b>\$10.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87643	50MB Machine to Machine Share (\$1.00 per MB overage rate) Tier 1	<b>\$15.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87644	150MB Machine to Machine Share (\$1.00 per MB overage rate) Tier 1	<b>\$18.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87645	250MB Machine to Machine Share (\$.015 per MB overage rate) Tier 2	<b>\$20.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87646	1GB Machine to Machine Share (\$.015 per MB overage rate) Tier 2	<b>\$25.00</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87647	5GB Machine to Machine Share (\$.015 per MB overage rate) Tier 2	<b>38.50 (25%)</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
87648	10GB Machine to Machine Share (\$.015 per MB overage rate) Tier 2	<b>61.60 (25%)</b>	If using a tablet for this plan, finance approval must be obtained and special price plan codes must be conditioned for profile (non standard device has to have non standard plan)
90231	5GB Public Sector M2M Share Plans	<b>\$34.99</b>	\$8.00 per GB overage charge and \$.002 per kilobyte National Access Roaming. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account, beginning with the line with the lowest overage need.
90234	10GB Public Sector M2M Share Plans	<b>\$59.99</b>	\$8.00 per GB overage charge and \$.002 per kilobyte National Access Roaming. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account, beginning with the line with the lowest overage need.
90235	20GB Public Sector M2M Share Plans	<b>\$99.99</b>	\$8.00 per GB overage charge and \$.002 per kilobyte National Access Roaming. At the end of each bill cycle, any unused data allowances for lines sharing on the same account will be applied to the overages of the other lines on the same account, beginning with the line with the lowest overage need.
86847 (3G)	25MB Machine to Machine 3G Backup Router Plan 25MB \$10/GB \$10	<b>\$10.00</b>	Overage rate is \$10 per GB
86848 (4G)	25MB Machine to Machine 4G Backup Router Plan 25MB \$10/GB \$10	<b>\$10.00</b>	Overage rate is \$10 per GB

\*\*\*If you are on the \$35.99 (93445) plan or (86769) \$51.00 plan with unl Text, Pix, Flix, you can block text with code 73572. If you remove block later, add code 73502 to re-add unlimited

**Disclaimer:** Information contained in this document is provided for review purposes only and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this document. In the event of any ambiguities or inconsistencies between the information in this spreadsheet and the pricing contained in the Verizon Price Sheet for State of Florida DMS-10/11-008C, the latter shall prevail.

verizon													
SOFL Equipment Matrix-Smartphones													
Samsung Galaxy													
Model	A42 5G	A51	XCover Pro	A71 5G UW	S10e	Galaxy S20	Galaxy S20 Ultra 5G	Samsung Galaxy S20 FE 5G UW	Samsung Galaxy Z Fold 2 5G UW	Galaxy S21 5G	Galaxy S21+ 5G	Galaxy S21 Ultra 5G	
SKU	128GB (SM-A425DUZ) / 128GB (SM-A425DUZ)	SM-A515DUZ / 5G UW (SM-A515DUZ)	SM-T715DUZV	SM-A715DUZV	128GB (SM-G970FDKAM)	SM-N970LZAV	128GB (SM-N970LZAV) / 512GB (SM-N970LZAV)	SM-N971VZBV	SM-F916DUZV	128GB (SM-G981DUZV) / 256GB (SM-G981DUZV)	128GB (SM-G982DUZV) / 256GB (SM-G982DUZV)	128GB (SM-G983DUZV) / 256GB (SM-G983DUZV) / 512GB (SM-G983DUZV)	
Retail Price	\$399.99	\$399.99 / \$549.99	\$499.99	\$649.99	\$529.99	\$999.99	\$1,299.99 / \$1,449.99	\$699.99	\$1,999.99	\$799.99 / \$949.99	\$999.99 / \$1,249.99	\$1,199.99 / \$1,249.99 / \$1,379.99	
Contract Price	\$159.99	\$149.99 / \$249.99	\$199.99	\$299.99	\$69.99	\$499.99	\$799.99 / \$949.99	\$359.99	\$1,499.99	\$319.99 / \$369.99	\$499.99 / \$549.99	\$699.99 / \$749.99 / \$879.99	
Operating System	Android 11	Android 10	Android 10	Android 10	Android 10	Android 10	Android 10	Android 10	Android 10	Android 11	Android 11	Android 11	
Camera	48MP/12MP front	48MP/12MP front	25MP/5MP front	64MP/ No front	12 MP/10 MP front	64MP/12MP front (2.2)	108MP/10MP front (2.2)	12MP / 12MP front	12MP / 10MP front	64MP / 10MP front	64MP / 10MP front	64MP / 10MP front	
Removable Memory	1TB capable	512GB capable	512GB capable	512 GB capable	512 GB capable	N/A	1 TB capable	1TB capable	None-Int Only	None-Int Only	None-Int Only	None-Int Only	
Hearing Aid Compatible	M3/T3	M4/T4	M3/T3	M3/T3	M3/T3	M3/T3	M3/T3	M3/T3	M3/T3	M3/T3	M3/T3	M3/T3	
Mode	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	
Field Force Manager	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Other Features	Processor: Octa-Core (Dual Quad Core Processors) 2.2 GHz x 4 / 1.8 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.3 GHz x 4 / 1.7 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.3 GHz x 4 / 1.7 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 64 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.4 GHz x 4 / 2.2 GHz x 1 / 1.7 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.3GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	5.8 inch screen FHD 402-compliant government grade encryption for Email, Calendar, and Contacts All three models have dual rear cameras Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 3 / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 3 / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.8GHz / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 256 Gigabyte Onboard RAM Memory 12 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.8GHz / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 256 Gigabyte Onboard RAM Memory 12 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.8GHz / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 256 Gigabyte Onboard RAM Memory 12 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.8GHz / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 256 Gigabyte Onboard RAM Memory 12 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.8GHz / 2.2GHz / 1.8GHz Onboard Memory (Actual available/formatted amount may be less) 256 Gigabyte Onboard RAM Memory 12 Gigabyte RAM

Apple, Blackberry, Google & Sonim																
Model	iPhone SE (2020)	iPhone 11 (2020)	iPhone 11 (2020)	iPhone 11 Pro	iPhone 11 Pro Max	iPhone 12 Mini 5G	iPhone 12 5G	iPhone 12 Pro 5G	iPhone 12 Pro Max 5G	BlackBerry KEY2 LE	Google Pixel 4a 5G UW	Google Pixel 4a	Google Pixel 4	Google Pixel 5 5G UW	Sonim XP6 64GB	
SKU	4408 (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 128GB (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 128GB (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A) / 512GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A) / 512GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 128GB (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 128GB (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A) / 512GB (MNP0LL2LL/A)	4408 (MNP0LL2LL/A) / 256GB (MNP0LL2LL/A) / 512GB (MNP0LL2LL/A)	BBK72LEVZV	GA01738-US	GA01738-US	GA01738-US	GA01955-US	99900543	
Retail Price	\$399.99 / \$449.99	\$649.99	\$649.99	\$799.99	\$849.99	\$599.99	\$699.99	\$999.99	\$1,099.99	\$449.99	\$399.99	\$799.99	\$799.99	\$899.99	\$649.99	
Contract Price	\$99.99 / \$499.99	\$49.99 / \$599.99	\$49.99 / \$599.99	\$149.99 / \$699.99	\$149.99 / \$799.99	\$299.99 / \$599.99	\$349.99 / \$699.99	\$549.99 / \$899.99	\$649.99 / \$1,099.99	\$99.99	\$79.99	\$79.99	\$349.99 / \$449.99	\$349.99	\$249.99	
Operating System	iOS 13	iOS 13	iOS 13	iOS 12	iOS 12	iOS 14	iOS 14	iOS 14	iOS 14	Android 8.1 / One	Android 11	Android 10	Android 10	Android 10	Android 8.1 One	
Camera	12MP / 7MP front	12MP / 12MP front	12MP / 12MP front	12MP / 7MP front	12MP / 7MP front	12MP / 12MP front	12MP / 12MP front	12MP / 12MP front	12MP / 12MP front	13 MP / 8 front	12 ZMP / 8MP front	12 ZMP / 8MP front	12 ZMP / 8MP front	12 ZMP / 8MP front	12 MP / 8 MP front	
Removable Memory	None-Int Only	None-Int Only	None-Int Only	None-Int Only	None-Int Only	None-Int Only	None-Int Only	None-Int Only	None-Int Only	25GB capable	Internal only	Internal only	Internal only	Internal only	64GB	
Hearing Aid Compatible	M4/T3	M3/T4	M3/T4	M3/T4	M3/T4	M3/T4	M3/T4	M3/T4	M3/T4	M4/T3	M4/T4	M4/T4	M4/T4	M4/T3	M4/T3	
Mode	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	
Field Force Manager	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Other Features	Processor: Dual Core Apple A13 Bionic 64 bit M11 Motion Coprocessor 4.7" Liquid Retina HD Display. Offering Multi-Touch, Display Zoom, and True Tone display/fitness charging / No charging dock or earbuds	Apple A13 Bionic 64 bit Quad Core. The dual camera system captures higher quality photos in a smartphone. No charging dock or earbuds	Apple A13 Bionic 64 bit Quad Core. A transformative mobile camera system that sets the bar in capability without complexity	All-new Liquid Retina display, the most advanced LCD in the industry. 11 inch screen size.	All-new Liquid Retina display, the most advanced LCD in the industry. 11 inch screen size.	Onboard Memory (Actual available/formatted amount may be less) 4 Gigabyte RAM	Processor: Hexa-Core A14 Bionic chip with 4th generation Neural Engine / Onboard RAM Memory 4 Gigabyte RAM	Processor: Hexa-Core A14 Bionic chip with 4th generation Neural Engine / Onboard RAM Memory 4 Gigabyte RAM	Processor: Hexa-Core A14 Bionic chip with 4th generation Neural Engine / Onboard RAM Memory 4 Gigabyte RAM	Processor: Hexa-Core A14 Bionic chip with 4th generation Neural Engine / Onboard RAM Memory 4 Gigabyte RAM	Octa-Core (Dual Quad Core Processors) 2.2 GHz x 4 / 1.8 GHz x 4 Type C charging port	Processor: Octa-Core (Dual Quad Core Processors) 2.2 GHz x 4 / 1.8 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 6 Gigabyte	Processor: Octa-Core (Dual Quad Core Processors) 2.2 GHz x 4 / 1.8 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 64 Gigabyte Onboard RAM Memory 4 Gigabyte	Processor: Octa-Core 2.84 GHz x 1 / 2.42 GHz x 3 / 1.8 GHz x 4 / Onboard Memory (Actual available/formatted amount may be less) 64 Gigabyte Onboard RAM Memory 8 Gigabyte	Processor: Octa-Core (Dual Quad Core Processors) 2.4 GHz x 1 / 2.2 GHz x 1 / 1.8 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte	Processor: Octa-Core (Dual Quad Core Processors) 2.2 GHz Octa core. Push-to-Talk Plus (PTT)

LG, Motorola & Kyocera													
Model	LG K51	LG V50 ThinQ 5G	LG Wing 5G	motor g power	motor g stylus	Motorola one 5G UW	Motorola edge 5G	Motorola razor	Durafone Ultra 5G	Durafone Pro 2			
SKU	LM-A500BMT	LM-V5000M	LM-W5000M	MOT7204K7	MOT7204S5	MOT7202A7	MOT720811	MOT720505	KYOCER110	KYOCER10			
Retail Price	\$149.99	\$649.99	\$549.99	\$249.99	\$299.99	\$299.99	\$499.99	\$299.99	\$699.99	\$444.00			
Contract Price	\$69.99	\$449.99	\$549.99	\$69.99	\$79.99	\$299.99	\$499.99	\$299.99	\$399.99	\$179.99			
Operating System	Android 10	Android 10	Android 10	Android 10	Android 10	Android 10	Android 10	9.0 - Android Pie & Android 10	Android 10	Android 10			
Camera	13 MP front only	64MP /12MP front	64MP /12MP front	13MP / 5 front	48 MP / 16 front	48 MP / 16 front	108 MP / 25 front	48MP / 16MP front	24 MP / 8MP front	13 MP / 8 front			
Removable Memory	2TB capable	2TB capable	2TB capable	512GB capable	512GB capable	1TB capable	Internal only	N/A	1TB capable	512 capable			
Hearing Aid Compatible	M3/T3	M4/T3	M4/T3	M3/T3	M3/T3	M3/T3	M3/T3	N/A	M3/T4	M3/T4			
Mode	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global	All Digital (Quad Band) Global			
Field Force Manager	x	NA	NA	NA	NA	NA	NA	NA	x	x			
Other Features	Processor: Octa-Core (Dual Quad Core Processors) Quad 2.0 GHz / Quad 1.5 GHz Onboard Memory (Actual available/formatted amount may be less) 32 Gigabyte USB Mass Storage Onboard RAM Memory 3 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) Octa Core 1.8 GHz (3.1) / 1.8 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) Octa Core 1.8 GHz (3.1) / 1.8 GHz x 4 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 8 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.4 GHz x 1 / 2.2 GHz x 2 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.4 GHz x 1 / 2.2 GHz x 2 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.4 GHz x 1 / 2.2 GHz x 2 Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte Onboard RAM Memory 4 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.2 GHz Octa core / ML-Standard 8104	Processor: Octa-Core (Dual Quad Core Processors) 2.2 GHz Octa core / ML-Standard 8104 Shock/Dust/Water Resistant		

Attachment D, Exhibit 2 - Vendor's Device List



\*Click Verizon logo from any page to return to table of contents

SOFL Equipment Matrix- Tablets & Internet Devices												
Tablets & Books												
<b>Make &amp; Model</b>	Samsung Galaxy Tab A 8.4 32GB	Samsung Galaxy Tab S5e 64GB	Samsung Galaxy Tab S7 5G UW	Samsung Galaxy Tab S7+ 5G UW	Apple iPad Mini 7.9	Apple iPad 10.2 (8th Gen)	iPad Air 10.9 (4th Gen)	iPad Pro 11 Inch (2nd Gen)	Apple iPad Pro 12.9 (4th Gen)	iPad Pro 11 Inch (3rd Gen 2021) 5G	iPad Pro 12.9 Inch(5th Gen 2021) 5G	
<b>SKU</b>	SMT307U2NA	SMT727V2SA	SMT878UZKA	SMT978UZKA	64GB: MUY12LLA / 256GB: MLV82LLA	32GB: MYH22LLA / 128 GB: MYM22LLA	64GB: MHY82LLA / 256GB: MVY122LLA	128GB: MY2X2LLA / 256GB: MXED2LLA / \$120GB: MXEF2LLA / 1TB: MXEH2LLA	128GB: MY3F2LLA / 256GB: MXFF2LLA / \$120GB: MXFH2LLA / 1TB: MXFH2LLA	128GB: MHMT3LLA / 256GB: MHMV3LLA / \$120GB: MHMX3LLA / 1TB: MHN33LLA	128GB: MHN33LLA / 256GB: MHNW3LLA / \$120GB: MHNW3LLA / 1TB: MHP13LLA / 2TB: MHP43LLA	
<b>Retail Price</b>	\$279.99	\$479.99	\$849.99	\$1,049.99	\$529.99 / \$679.99	\$459.99 / \$559.99	\$729.99 / \$879.99	\$949.99 / \$1,049.99 / \$1,249.99 / \$1,449.99	\$1,149.99 / \$1,249.99 / \$1,449.99 / \$1,699.99	\$999.99 / \$1,099.99 / \$1,299.99 / \$1,699.99 / \$2,099.99	\$1,299.99 / \$1,399.99 / \$1,599.99 / \$1,999.99 / \$2,399.99	
<b>Contract Price (2yr)</b>	\$279.99	\$479.99	\$849.99	\$1,049.99	\$529.99 / \$679.99	\$459.99 / \$559.99	\$729.99 / \$879.99	\$949.99 / \$1,049.99 / \$1,249.99 / \$1,449.99	\$1,149.99 / \$1,249.99 / \$1,449.99 / \$1,699.99	\$899.99 / \$999.99 / \$1,199.99 / \$1,599.99 / \$1,999.99	\$1,199.99 / \$1,299.99 / \$1,499.99 / \$1,899.99 / \$2,299.99	
<b>Operating System</b>	Android 9.0 Pie	Android 8.1 Oreo	Android 10	Android 10	iPadOS 13 / 14	iPadOS 14	iPadOS 14	iOS 13	iOS 13	iPadOS 14	iPadOS 14	
<b>Camera</b>	Rear (13 MP) and front facing (8.0MP)	Rear (13 MP) and front facing (8.0MP)	Rear (13 MP) and front facing (8.0MP)	Rear (13 MP) and front facing (8.0MP)	Rear (8 MP) and front facing (7.0MP)	Rear (8.0MP) and front facing (1.2MP)	Rear (12 MP) and front facing (7.0MP)	Rear (12 MP) and front facing (7.0MP)	Rear (12 MP) and front facing (7.0MP)	Rear (12 MP) and front facing (12MP Ultra Wide)	Rear (12 MP) and front facing (12MP Ultra Wide)	
<b>Removable Memory</b>	Up to 400 GB	Up to 400 GB	Up to 512GB	Up to 512GB	Internal only	Internal only	Internal only	Internal only	Internal only	Internal only	Internal only	
<b>Other Features</b>	Processor: Octa-Core (Dual Quad Core Processors) 1.8 GHz x 2 / 1.6 GHz x 6 Octa core // Onboard Memory (Actual available/formatted amount may be less) 32 Gigabyte Onboard RAM Memory 3 Gigabyte RAM	Processor: Hexa-Core (Dual Quad Core Processors) 2.0 GHz x 2 / 1.7 GHz x 6 Hexa-Core CPU // Onboard Memory (Actual available/formatted amount may be less) 64 Gigabyte USB Mass Storage Onboard RAM Memory 4 Gigabyte RAM	Processor: Octa-Core (Dual Quad Core Processors) 2.4GHz x3 / 1.8GHz x4 // Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte USB Mass Storage Onboard RAM Memory 6 Gigabyte	Processor: Octa-Core (Dual Quad Core Processors) 2.4GHz x3 / 1.8GHz x4 // Onboard Memory (Actual available/formatted amount may be less) 128 Gigabyte USB Mass Storage Onboard RAM Memory 6 Gigabyte	Processor Dual Core Apple A12 Bionic 64 bit neural engine with Embedded M12 coprocessor	Processor Dual Core Apple A12 Bionic 64 bit neural engine with Embedded M12 coprocessor	Onboard Memory (Actual available/formatted amount may be less) 64 Gigabyte	Processor: Octa-Core (Dual Quad Core Processors) Apple A12Z Bionic chip with 64-bit architecture Embedded M12 coprocessor	Dual core processor: Apple A12X Bionic 64 bit neural engine with Embedded M12 coprocessor	Processor: Octa-Core (Dual Quad Core Processors) Apple M1 8 Core CPU 4 performance cores/4 efficiency cores	Processor: Octa-Core (Dual Quad Core Processors) Apple M1 8 Core CPU 4 performance cores/4 efficiency cores	Processor: Octa-Core (Dual Quad Core Processors) Apple M1 8 Core CPU 4 performance cores/4 efficiency cores
Internet Devices												
<b>Make &amp; Model</b>	5G MIFI M1000	MIFI 8800L	Ellipsis Jetpack 900LS	USB730L	Orbic Speed	Inseego MIFI M2100 5G UW	Skyyus 160					
<b>SKU</b>	INSGM1000	MIF8800L	MH900LS	USB730L	ORB400LBVZRT	INSGM2100	SK160-VZ					
<b>Retail Price</b>	\$649.99	\$199.99	\$79.99	\$249.99	\$99.99	\$399.99	\$249.99					
<b>Contract Price</b>	\$499.99	\$99.99	\$29.99	\$79.99	\$99.99	\$249.99	\$99.99					
<b>4G LTE</b>	5G	X	X	X	X	5G	X					
<b>Rev A</b>	No	X	No	No	No	No	No					
<b>Form Factor</b>	Hotspot	Hotspot	Hotspot	Aircard	Hotspot	Hotspot	Router					
<b>Mac Compatible</b>	X	X	X	X	X	X						
<b>External Antenna</b>	No	No	No	No	No	No	N/A					
<b>Vista Compatible</b>	No	No	X	No	No	No	N/A					
<b>Mode</b>	All Digital (Ultra Wide Band XLTE Band 13)	All Digital (Quad Band) Global	4G LTE	All Digital (Quad Band) Global	4G LTE / XLTE Band 13 / 4 (700/1700 MHz)	All Digital (Ultra Wide Band XLTE Band 13)	4G LTE					
<b>Other Features</b>	5G Mobile Hotspot up to 15 devices. VPN Client Capable USB 3.0 Support -Ultra Wide Band (UWB): n261 (27.5-28.35 GHz); n260 (37-40 GHz)	4G Mobile Hotspot up to 15 devices. VPN Capable USB 3.0 Support -Ultra Wide Band (UWB): n261 (27.5-28.35 GHz); n260 (37-40 GHz)	4G Mobile Hotspot up to 8 devices. VPN Capable 1.4 GHz Dual Core Processor Battery life up to 24 hours	One Step Access Easy to adjust Type A USB Port compatibility	Processor Quad Core 1.3 GHz Quad-Core Processor // Onboard Memory (Actual available/formatted amount may be less) 512 Megabyte Onboard RAM Memory 256 Megabyte RAM	5G Mobile Hotspot up to 15 devices. VPN Client Capable USB 3.0 Support -Ultra Wide Band (UWB): n261 (27.5-28.35 GHz); n260 (37-40 GHz)	Processor: Qualcomm MDM230 // Onboard Memory (Actual available/formatted amount may be less) 8 Gigabyte Onboard RAM Memory 1 Gigabyte RAM					

Attachment D, Exhibit 2 - Vendor's Device List

 *Click Verizon logo from any page to return to table of contents <b>SOFL Equipment Matrix - Basic &amp; One Talk Phones</b>										
One Talk Desk phones										
										
<b>Yealink Deskphone</b>	<b>T41S IP</b>	<b>T41SW IP</b>	<b>T42S IP</b>	<b>T46S IP</b>	<b>T46SW IP</b>	<b>T49G IP</b>	<b>VZP59 IP</b>	<b>W60 DECT</b>	<b>CP920 IP Conference Phone</b>	<b>CP960 IP Conference Phone</b>
<b>SKU</b>	T41S	T41SW	T42S	T46S	T46SW	T49G	VZP59	W60	CP920	CP960
<b>Retail Price</b>	\$85.00	\$115.00	\$115.00	\$145.00	\$170.00	\$349.00	\$399.00	\$169.00	\$395.00	\$499.00
<b>Number of contacts</b>	1000	1000	1000	1000	Memory Dependent	1000	1000	1000	1000	1000
<b>Accessibility</b>	PoE support 6 Way conferencing support	PoE support 6 Way conferencing support	PoE support 6 Way conferencing support	Multi-Language 6 Way conferencing support	Multi-Language 6 Way conferencing support	6 Way conferencing support	6 Way conferencing support	Indoor Range 150 Feet / Outdoor range 900 Feet Tactile-discernible number, feature, and navigation keys	Multi-Language Supports connection to a mobile phone or PC for conference calls 6 Way conferencing support	Multi-Language Supports connection to a mobile phone or PC for conference calls 6 Way conferencing support
<b>Form Factor</b>	Integrated stand with 2 adjustable angles Wall Mountable Message Waiting Indicator (MWI) 2 x RJ45 10/100 Ethernet Ports 1xRJ9 (4P4C) handset port 1xRJ9 (4P4C) handset port Power over Ethernet (IEEE 802.3af), Class 2 1XRJ12 (6P6C) EHS port 1 x USB 2.0 port Desk Phone	Integrated stand with 2 adjustable angles Wall Mountable Message Waiting Indicator (MWI) 2 x RJ45 10/100 Ethernet Ports 1xRJ9 (4P4C) handset port 1xRJ9 (4P4C) handset port Power over Ethernet (IEEE 802.3af), Class 2 1XRJ12 (6P6C) EHS port Desk Phone	Integrated stand with 2 adjustable angles Wall Mountable Message Waiting Indicator (MWI) 2 x RJ45 10/100 Ethernet Ports 1xRJ9 (4P4C) handset port 1xRJ9 (4P4C) handset port Power over Ethernet (IEEE 802.3af), Class 2 1XRJ12 (6P6C) EHS port Desk Phone	Integrated stand with 2 adjustable angles Wall Mountable Message Waiting Indicator (MWI) 1xRJ9 (4P4C) handset port 1xRJ9 (4P4C) handset port Power over Ethernet (IEEE 802.3af), class 0 1 x USB 2.0 port Desk Phone	Integrated stand with 2 adjustable angles Wall Mountable Message Waiting Indicator (MWI) 1xRJ9 (4P4C) handset port Power over Ethernet (IEEE 802.3af), class 0 1 x USB 2.0 port Desk Phone	HDMI Port Integrated stand with 2 adjustable angles HDMI output for connection to Monitor/Storage Applications Message Waiting Indicator (MWI) 1xRJ9 (4P4C) handset port 1xRJ9 (4P4C) handset port 1 x USB 2.0 port Desk Phone	HDMI Port Integrated stand with 2 adjustable angles HDMI output for connection to Monitor/Storage Applications Message Waiting Indicator (MWI) 1xRJ9 (4P4C) handset port 1xRJ9 (4P4C) handset port 1 x USB 2.0 port Desk Phone	Headphone Port 3.5mm Wall Mountable Message Waiting Indicator (MWI) Power over Ethernet (IEEE 802.3af), Class 2 Desk Phone	1 x RJ45 10/100 Ethernet port Power over Ethernet (IEEE 802.3af), class 0 1 x USB 2.0 port 1x Mobile phone/PC port: 3.5mm Desk Phone 20 feet and 360 degree voice pickup	Headphone Port 3.5mm Power over Ethernet (IEEE 802.3af), class 0 1x Mobile phone/PC port: 3.5mm Desk Phone 20 feet and 360 degree voice pickup Built-in three-microphone array Available expansion microphones (wired or wireless sold separately)
<b>Technology</b>	Yealink Optima HD voice SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 IP assignment: static/DHCP USB 2.0 Supported	Wi-Fi 802.11 n - 2.4 and 5GHz only 802.11 a/b/g/n/ac Yealink Optima HD voice SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 IP assignment: static/DHCP USB 2.0 Supported	Wi-Fi 802.11 n - 2.4 and 5GHz only 802.11 a/b/g/n/ac Yealink Optima HD voice SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 IP assignment: static/DHCP USB 2.0 Supported	Yealink Optima HD voice Dual Port Gigabit Ethernet PoE(802.3af) class support Supports Bridging that allows T41P, T46G, T46GW and T49G to monitor incoming calls IPv6 OpenVPN, IEEE802.1X IP assignment: Static / DHCP / PPPoE	Wi-Fi 802.11 b/g/n 802.11 n - 2.4 and 5GHz only Yealink Optima HD voice Up to 16 SIP accounts Dual Port Gigabit Ethernet Supports Bridging that allows T41P, T46G, T46GW and T49G to monitor incoming calls SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 OpenVPN, IEEE802.1X IP assignment: Static / DHCP / PPPoE USB 2.0 Supported	Wi-Fi 802.11 n - 2.4 and 5GHz only Yealink Optima HD voice Up to 16 SIP accounts Dual Port Gigabit Ethernet Supports Bridging that allows T41P, T46G, T46GW and T49G to monitor incoming calls SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 OpenVPN, IEEE802.1X IP assignment: Static / DHCP / PPPoE USB 2.0 Supported	Wi-Fi 802.11 n - 2.4 and 5GHz only Yealink Optima HD voice Up to 16 SIP accounts Dual Port Gigabit Ethernet Supports Bridging that allows T41P, T46G, T46GW and T49G to monitor incoming calls SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 OpenVPN, IEEE802.1X IP assignment: Static / DHCP / PPPoE USB 2.0 Supported	Auto Answer Function Yealink Optima HD voice SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 SRTP security encryption Noise Reduction System SIP v1 (RFC2543) SIP v2 (RFC3261) SIP v1 (RFC2543), v2 (RFC3261) Out-of-band DTMF(RFC 2835) In-band DTMF SIP INFO DTMF Report (RFC3581) Digest/basic authentication Peer-to-peer SIP link mode Loose routing and strict routing support PRACK (RFC3262) Error-information support Reliability of provisional responses (RFC3262) Offer/answer (RFC3264) Message Waiting Indication (RFC3842) Subscription for MWI events (RFC3265) Dialog-state monitoring(RFC 4235) Event list subscription support (RFC4662) REFER (RFC3515)	SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 IP assignment: static/DHCP OpenVPN, IEEE802.1X Background Noise Suppression Call Recording via local USB	Wi-Fi 802.11 n - 2.4 and 5GHz only 802.11 b/g/n/ac SIP v1 (RFC2543), v2 (RFC3261) Transport Layer Security (TLS) IPv6 IP assignment: static/DHCP OpenVPN, IEEE802.1X Background Noise Suppression Call Recording via local USB USB 2.0 Supported Noise Proof Technology Five-way conference call capability
Standard Voice & PTT devices										
										
<b>Make &amp; Model</b>	Alcatel Go Flip V	Orbic Journey V	Kazana eTalk	Sonim XP5s	Sonim XP3	DuraXV Extreme				
<b>SKU</b>	ALCATEL-4051S	ORB2200LBVZ	KAZF119VWQ	999000144	999000389	KYOE4810				
<b>Retail Price</b>	\$99.99	\$99.99	\$79.99	\$288 - \$648	\$199.99	\$240.00				
<b>Contract Price</b>	\$49.99	\$49.99	\$29.99	\$149.99	\$99.99	\$99.99				
<b>Camera</b>	2.0 MP	2.0 MP	2.0 MP	5.0 MP	5.0 MP	5.0 MP				
<b>Bluetooth</b>	X	X	X	X	X	X				
<b>Removable Memory</b>	Up to 32GB	2.0 MP	Up to 32GB	Up to 64GB	Up to 128GB	Up to 512GB				
<b>Hearing Aid Compatible</b>	X (M3/T3)	X (M3/T3)	X (M4/T4)	X (M3/T4)	X (M3/T4)	X (M3/T4)				
<b>Mode</b>	All Digital (Quad Band) Global	X	All Digital (Quad Band) Global	All Digital (Quad Band)	All Digital (Quad Band)	X				
<b>Field Force Manager</b>	X	X	X	X	X	X				
<b>Other Features</b>	1.1 Ghz Quad Core Processor HD Voice capable 2.8 Inches LCD display and large keys Not CDMA compatible	Processor Quad Core 1.1 Ghz Quad CoreScreen Resolution TFT QVGA 320 x 240 / 142.8 PPI Screen Size 2.8 Inches	1.1 Ghz Quad Core Processor HD Voice capable 2.8 Inches display and large keys Not CDMA compatible	3-year warranty Gorilla Glass 3 by Corning Ghz Quad Core Processor PTT compatible Meets MIL-Standard 8100 standards for Dust, Shock, Water Resistance.	Processor Quad Core 1.1 Ghz Quad Core, HD Voice capable Push-to-Talk Plus (PTT+)	Screen Resolution: QVGA TFT (240 x 320 pixels) / Screen Size: 2.8 inches/ 1. G102 Ghz Quad Core / Push-to-Talk Plus (PTT+)				

For specific product functionality and features, device and calling plan/feature compatibility, and for the latest equipment pricing, see your Verizon Government Account Manager. The above Equipment prices are effective as of 04-01-19 and are subject to change. Customer may purchase at the then current State of Florida Government Equipment Matrix pricing or Government promotional pricing, whichever is less at the time of purchase. Verizon may make certain equipment available at no charge, however, Verizon does not guarantee that we will always be able to offer equipment at no charge through the term of the resulting agreement. Government Subscriber Equipment Pricing listed in this matrix is not available for activations or upgrades on Verizon Telephony plans. Camera phone use or possession may be prohibited in some locations based on privacy, security, or other restrictions. Verizon's Government Equipment Matrix is updated at a minimum quarterly, based upon equipment availability, changes in technology and market conditions. Equipment is promotional and subject to availability. Verizon reserves the right to add or discontinue models. Pricing above is at the 2 yr price point. Existing customers can upgrade at this price 20 months into their current contract.

**STATE OF FLORIDA**

**DEPARTMENT OF MANAGEMENT SERVICES**

**ITN NO: DMS-19/20-006 MOBILE COMMUNICATION SERVICES (MCS-2)**

**REQUEST FOR BEST AND FINAL OFFER**

**DUE: May 14, 2021 BY 11:59 PM ET**

---

**INTRODUCTION**

Pursuant to the Mobile Communication Services ITN Sections 4.4.3., Revised Replies and Best and Final Offers, and 4.4.4, Other Department Rights During Negotiations, the Department requests a Best and Final Offer. Please submit the Best and Final Offer by 11:59 PM ET on May 14, 2021, to the Procurement Officer, Caitlen Boles, at [Caitlen.Boles@dms.fl.gov](mailto:Caitlen.Boles@dms.fl.gov)

Respondents must email the Best and Final Offer with files attached as a .pdf or in their native format (.docx or .xlsx where applicable) to the Procurement Officer. If the Best and Final Offer exceeds the file limit to submit via email, the Respondent must submit its Best and Final Offer on a thumb drive to the Procurement Officer by the above-stated deadline.

Best and Final Offers are expressly understood to be for the provision of services and features with no minimum guaranteed purchase of services or features.

All revisions made by the Department to the attachments provided with this Request for Best and Final Offer are reflected in track changes; track changes reflect changes made to the original documents posted with the ITN, and as modified by Addendum No. 2. Any Respondent-proposed edits not reflected in the attachments were deemed not acceptable to the Department. Do not make any changes, revisions, exceptions, or deviations to the Department's language in the provided documents.

**BEST AND FINAL OFFER SUBMISSION**

The Best and Final Offer must include the following requested documents:

**A. ATTACHMENT A – FINAL STATEMENT OF WORK**

Please submit a response to each subsection in Attachment A – Final Statement of Work where a response is requested, including Section 4 Public Safety if the Respondent is proposing public safety services. Identify all modifications and/or revisions, if any, to the responses provided in the Statement of Work from Respondent's initial ITN Reply via track changes.

**B. ATTACHMENT B – FINAL CONTRACT**

By submitting a Best and Final Offer, the Respondent confirms acceptance of Attachment B – Final Contract, as is; ***do not make any changes, revisions, exceptions, or deviations.***

**C. ATTACHMENT C – FINAL SERVICE LEVEL AGREEMENTS**

By submitting a Best and Final Offer, the Respondent confirms acceptance of Attachment C – Final Service Level Agreements, as is; ***do not make any changes, revisions, exceptions, or deviations.***

#### D. FINAL VENDOR'S DEVICE LIST AND VENDOR'S SERVICES AND DISCOUNTS PRICING (EUPL)

Please submit Vendor's Device List and Vendor's Services and Discounts Pricing. If the Respondent is proposing public safety plans and devices, these shall be included within these documents.

The Respondent is required to submit a Vendor's Device List and Vendor's Services and Discounts Pricing that includes the Respondent's best pricing for the Department's consideration based on the revisions contained in the Request for Best and Final Offer and attachments. Given these revisions made by the Department, the Department is anticipating reductions in the Respondent's pricing.

The Vendor's Device List and Vendor's Services and Discounts Pricing must comply with ITN Section 3.10, Respondent's Pricing. Pricing in either document shall not include State of Florida and Federal Taxes. Taxes are defined here to include payments that the Contractor is required to collect by law and pay to public entities.

#### E. WIRELESS SERVICE GUIDES

Please submit the plans and features government terms of service with the terms agreed upon in negotiations. If awarded a contract, the intent is for these terms to be incorporated into the EUPL.

#### **SUPPLEMENTAL INFORMATION**

The Best and Final Offer shall constitute the Respondent's final Reply to this ITN and should be reflective of all terms and conditions applicable to the Respondent's proposed services.

Should the Respondent's BAFO response contain website references, that are external to the documents, the information referenced on the website should be provided in the BAFO response. However, if the information has been previously supplied to the negotiation team in the information request in January and no changes have been made, it is not necessary to resubmit.

The Respondent is under no obligation to submit a Best and Final Offer; however, the Respondent will no longer be considered for an award if the Department does not receive a Best and Final Offer.

By the submission of its Best and Final Offer, the Respondent certifies that, if awarded a Contract, it will comply with all terms and conditions found in the aforementioned documents included with this Request for Best and Final Offer.

#### **REDACTED COPY**

If the Respondent considers any portion of the documents, data, or records submitted to the Department to be trade secret or otherwise exempt from public inspection or disclosure pursuant to Florida's Public Records Law, the Respondent must provide the Department with a separate, electronic redacted copy of the Best and Final Offer in accordance with Section 3.8 of the ITN.

#### **STATE OF FLORIDA EMPLOYEE DISCOUNTS**

If the Respondent intends to offer any discounted pricing to State of Florida employees (including state agencies, OEU's, or their retirees), please provide the discount percentage in the Best and Final Offer.

Please note that the decision to offer discounted rates is wholly within the Respondent's discretion and will NOT be considered as part of the State's best value determination (see ITN Section 4.5, Final Selection and Notice of Intent to Award Contract).



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

**Ron DeSantis, Governor**  
Jonathan R. Satter, Secretary

**INVITATION TO NEGOTIATE  
FOR  
MOBILE COMMUNICATION SERVICES  
ITN NO: DMS-19/20-006  
THE STATE OF FLORIDA  
DEPARTMENT OF MANAGEMENT SERVICES**

Procurement Officer: Caitlen Boles  
Departmental Purchasing  
Florida Department of Management Services  
4050 Esplanade Way, Suite 335.3Y  
Tallahassee, FL 32399-0950  
Phone: (850) 410-1423  
Email: [DMS.Purchasing@dms.myflorida.com](mailto:DMS.Purchasing@dms.myflorida.com)

Failure to file a protest within the time prescribed in section 120.57(3), Florida Statutes, or failure to post the bond or other security required by law within the time allowed for filing a bond shall constitute a waiver of proceedings under Chapter 120, Florida Statutes.

Any protest concerning this agency decision or intended decision must be timely filed with the Agency Clerk. Protests may be filed by courier, hand delivery, or regular mail at: Department of Management Services, Office of the General Counsel, Attention: Agency Clerk, 4050 Esplanade Way, Suite 160, Tallahassee, Florida 32399-0950. Protests may also be filed by fax at 850-9226312, or by email at [agencyclerk@dms.myflorida.com](mailto:agencyclerk@dms.myflorida.com). It is the filing party's responsibility to meet all filing deadlines.

**NOTICE PURSUANT TO SECTION 287.057(23), FLORIDA STATUTES**

Respondents to this solicitation or persons acting on their behalf may not contact, between the release of the solicitation and the end of the 72-hour period following the agency posting the notice of intended award, excluding Saturdays, Sundays, and state holidays, any employee or officer of the executive or legislative branch concerning any aspect of this solicitation, except in writing to the procurement officer or as provided in the solicitation documents. Violation of this provision may be grounds for rejecting a response.

**TABLE OF CONTENTS**

SECTION 1. INTRODUCTION .....	4
1.1 Solicitation Objective .....	4
1.2 Background.....	4
1.3 Term.....	4
1.4 Questions Being Explored .....	4
1.5 Goals of the ITN.....	4
1.6 Special Accommodations .....	5
1.7 Procurement Officer.....	5
1.8 Timeline of Events .....	5
SECTION 2. SOLICITATION PROCESS.....	7
2.1 General Overview .....	7
2.2 Questions and Answers.....	8
2.3 Addenda to the Solicitation.....	8
2.4 Receipt of Replies.....	8
2.5 Respondent Firm Offer .....	9
SECTION 3. GENERAL INSTRUCTIONS.....	9
3.1 General Instructions to Respondents (PUR 1001 Form).....	9
3.2 MFMP Registration .....	10
3.3 Florida Substitute Form W-9 Process .....	11
3.4 Website References .....	11
3.5 How to Submit a Reply .....	11
3.6 Mandatory Responsiveness Requirements .....	12
3.7 Contents of Reply .....	12
3.8 Public Records, Respondent’s Confidential Information, and Redacted Replies .....	14
3.9 Additional Information.....	16
3.10 Respondent’s Pricing.....	16
SECTION 4. SELECTION METHODOLOGY .....	19
4.1 Responsiveness and Responsibility .....	19
4.2 Evaluation Process – General Overview.....	20
4.3 Evaluation of the Reply.....	20
4.4 Negotiations .....	21
4.5 Final Selection and Notice of Intent to Award Contract .....	24
SECTION 5. AWARD .....	24
5.1 Rights for Award .....	24
5.2 Agency Decision .....	25

5.3 Other Reserved Rights.....25  
5.4 No Contract until Execution.....25

**Attachments:**

- Attachment A – Statement of Work
- Attachment B – Draft Contract
- Attachment C – Service Level Agreements
- Attachment D – Business Case
- Attachment E – Definitions and Acronyms

**Forms:**

- FORM 1 – CONTACT INFORMATION
- FORM 2 – NOTICE OF CONFLICT OF INTEREST
- FORM 3 – NON-COLLUSION STATEMENT
- FORM 4 – STATEMENT OF NO PRIOR DISQUALIFYING INVOLVEMENT
- FORM 5 – MANDATORY RESPONSIVENESS REQUIREMENTS
- FORM 6 – BUSINESS EXPERIENCE

## SECTION 1. INTRODUCTION

### 1.1 Solicitation Objective

The State of Florida (State), Department of Management Services (Department or DMS) is seeking to establish, through this Invitation to Negotiate (ITN), a contract or contracts (Contract) for cellular voice and data services, secure access to MyFloridaNet (through 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). MCS is part of the DMS SUNCOM group of contracts providing voice and data services to SUNCOM Customers. The Department intends to award multiple Contracts but reserves the right to award to one Respondent or to make no award.

The resulting Contract(s), if any, will be used by State agencies and other authorized entities, collectively referred to as "Customers," in accordance with Chapter 282, Florida Statutes.

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

### 1.2 Background

Prior to issuance of this solicitation, the Department contracted with a private vendor to assist in the development of a business case for MCS, in accordance with section 287.0571, Florida Statutes. The business case examined options for the future path of MCS and recommended that the Department issue an ITN for the services. That Mobile Communication Services Business Case is attached to this procurement as Attachment D – Business Case for background informational purposes only and does not contain specifications for this solicitation.

The Department has estimated that the annual total enterprise expenditures on the Contract resulting from this solicitation will be approximately \$85 million. This estimate is for informational purposes only. Under no circumstances should this estimate be construed as representing actual, guaranteed, or minimum spend under any new Contract.

### 1.3 Term

The term of the Contract will be five (5) years. Upon written agreement, the Department and the Contractor may renew the Contract in whole or in part for up to five (5) additional years. Renewals are contingent upon satisfactory performance evaluations by the Department and are subject to the availability of funds (see section 287.057(13), Florida Statutes).

### 1.4 Questions Being Explored

- a) What is the best model for delivery of cost-efficient and high-quality MCS, including nationwide coverage?
- b) What service options meet a variety of Customer needs?
- c) How we the Department maintain competitive pricing throughout the initial and renewal year of the Contract?
- d) What is the best model for the Department to achieve the objectives state in Attachment A – Statement of Work (SOW), Subsection 1.3?

### 1.5 Goals of the ITN

The goals of this ITN are to establish:

- a) The delivery of cost-efficient and high-quality MCS, including nationwide coverage;
- b) Service options to meet a variety of Customers' needs;

- c) Competitive pricing throughout the initial and any renewal years of the Contract; and
- d) The objectives stated in Attachment A - Statement of Work (SOW), Subsection 1.3.

### 1.6 Special Accommodations

Any person requiring a special accommodation due to a disability should contact the Department's Americans with Disabilities Act (ADA) Coordinator at (850) 922-7535 or [ADA.Coordinator@dms.fl.gov](mailto:ADA.Coordinator@dms.fl.gov). Requests for accommodation for meetings must be made at least five (5) Business Days prior to the meeting. A person who is hearing or speech impaired can contact the ADA Coordinator by using the Florida Relay Service at (800) 955-8771 (TDD).

### 1.7 Procurement Officer

The Procurement Officer is the **sole point of contact** for this procurement. Direct all contact with the Department to the Procurement Officer in writing by email.

Caitlen Boles  
 Departmental Purchasing  
 Florida Department of Management Services  
 4050 Esplanade Way, Suite 335.3Y  
 Tallahassee, FL 32399-0950  
 Phone: (850) 410-1423  
 Email: [dms.purchasing@dms.myflorida.com](mailto:dms.purchasing@dms.myflorida.com)

**\*\*\*PLACE THE SOLICITATION NUMBER IN THE SUBJECT LINE OF ALL EMAILS TO THE PROCUREMENT OFFICER\*\*\***

If a Respondent is claiming that any portion of an email is trade secret under section 812.081, Florida Statutes, or otherwise confidential under Florida or Federal Law, the Respondent is to place the word "Confidential" in the subject line. (See Subsection 3.8.4, How to Claim Trade Secret or Other Exemptions, of this ITN for more information on confidential information.)

Any contact with the Department by an affiliate, a person with a relevant business relationship with a Respondent, or an existing or prospective subcontractor to a Respondent is assumed to be on behalf of a Respondent unless shown otherwise.

### 1.8 Timeline of Events

The table below contains the anticipated Timeline of Events for this solicitation. The dates and times within the Timeline of Events are subject to change. It is the Respondent's responsibility to check the VBS for any changes. The Respondent is responsible for ensuring the Department receives all required documentation by the dates and times (Eastern Time) specified below (or as revised by addenda).

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
ITN posted on the VBS.		October 7, 2020
Deadline to submit questions to the Procurement Officer.	3:00 PM	October 28, 2020

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
Department's anticipated posting of answers to Respondent's questions on the VBS.		November 9, 2020
Deadline to submit Reply and all required documents to the Procurement Officer.	2:00 PM	November 23, 2020
<p>Public Opening. Conference Room 101 4050 Esplanade Way Tallahassee, Florida 32399-0950</p> <p><b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/198062149">https://global.gotomeeting.com/join/198062149</a></p> <p><b>You can also dial in using your phone.</b> United States (Toll Free): <a href="tel:18773092073">1 877 309 2073</a> United States: <a href="tel:+16467493129">+1 (646) 749-3129</a></p> <p><b>Access Code:</b> 198-062-149</p> <p><b>Join from a video-conferencing room or system.</b> Dial in or type: 67.217.95.2 or inroomlink.goto.com Meeting ID: 198 062 149 Or dial directly: 198062149@67.217.95.2 or 67.217.95.2###198062149</p> <p>New to GoToMeeting? Get the app now and be ready when your first meeting starts: <a href="https://global.gotomeeting.com/install/198062149">https://global.gotomeeting.com/install/198062149</a></p>	3:00 PM	November 23, 2020
Anticipated Evaluations Phase.		December 1, 2020 to December 30, 2020
Anticipated Negotiations Phase.		January 4, 2021 to April 12, 2021
<p>Negotiation Team Public Meeting Conference Room 101 4050 Esplanade Way</p> <p><b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/432429477">https://global.gotomeeting.com/join/432429477</a></p>	10:00 AM	April 19, 2021

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
<p><b>You can also dial in using your phone.</b>            United States (Toll Free): <a href="tel:18773092073">1 877 309 2073</a>            United States: <a href="tel:+16467493129">+1 (646) 749-3129</a></p> <p><b>Access Code:</b> 432-429-477</p> <p><b>Join from a video-conferencing room or system.</b>            Dial in or type: 67.217.95.2 or inroomlink.goto.com            Meeting ID: 432 429 477            Or dial directly: 432429477@67.217.95.2 or            67.217.95.2##432429477</p> <p>New to GoToMeeting? Get the app now and be ready when your first meeting starts:  <a href="https://global.gotomeeting.com/install/432429477">https://global.gotomeeting.com/install/432429477</a></p>		
Anticipated date to post Notice of Intent to Award on the VBS.		April 26, 2021
Anticipated Contract Execution.		May 2021

## SECTION 2. SOLICITATION PROCESS

### 2.1 General Overview

The ITN is a method of competitively soliciting contractual services under section 287.057(1)(c), Florida Statutes. This solicitation will be administered through the Vendor Bid System (VBS). Vendors interested in submitting a Reply are to comply with all terms and conditions described in this solicitation. The Department will hold a public opening of the Replies at the date, time, and location provided in the Timeline of Events.

The ITN process is divided into two (2) phases: the evaluation phase and the negotiation phase. The evaluation phase involves the Department's evaluation of Replies in accordance with this ITN. During this phase, the Department evaluates all Responsive Replies using the assessment scale against all evaluation criteria to establish a competitive range of Replies reasonably susceptible of award. The Department then selects one (1) or more Respondents within the competitive range with which to commence negotiations.

The negotiation phase involves negotiations between the Department and one or more Respondents whose evaluated Replies were determined to be within the competitive range, in accordance with this ITN. During this phase, the Department may request revised Replies and best and final offers (BAFOs) based on the negotiations.

Once negotiations have concluded and BAFO(s) have been received and reviewed, the Department will hold a negotiation team public meeting to recommend Contract award(s). The Department intends to post a notice of Intent to Award Contract(s), identifying the responsive and responsible vendor(s) that provide the best value to the State based on the selection criteria set forth in Subsection 4.5, Final Selection and Notice of Intent to Award Contract, of the ITN.

Any reservation or listing of reservations of the Department’s rights provided in this ITN is not intended to be exhaustive and shall not be construed to limit the rights of the Department in conducting this procurement.

**2.2 Questions and Answers**

Respondents will submit all questions during the Question and Answer period in writing to the Procurement Officer via email. The deadline for submission of questions is reflected in Subsection 1.8, Timeline of Events.

The Department requests that all questions have the solicitation number in the subject line of the email and be submitted in the following format:

Question #	Respondent Name	Section	Page #	Question

Questions will not constitute a formal protest of the specifications of the solicitation. Department answers to written questions will be issued by addendum via the VBS.

**2.3 Addenda to the Solicitation**

The Department reserves the right to modify this solicitation by issuing addenda posted on the VBS. It is the responsibility of the Respondent to check the VBS for information and updates.

**2.4 Receipt of Replies**

**2.4.1 Reply Deadline**

The Respondent is responsible for ensuring the Department receives the Reply no later than the date and time provided in Subsection 1.8, Timeline of Events, of this ITN (or as revised by addenda). Address the Reply to the Procurement Officer at:

Caitlen Boles  
 Departmental Purchasing  
 Florida Department of Management Services  
 4050 Esplanade Way, Suite 335.1X  
 Tallahassee, FL 32399-0950  
 Phone: (850) 410-1423  
 Email: [DMS.Purchasing@dms.myflorida.com](mailto:DMS.Purchasing@dms.myflorida.com)

All methods of delivery or transmittal to the Procurement Officer are exclusively the responsibility of Respondents, and the risk of non-receipt or delayed receipt shall be borne exclusively by the Respondents.

#### **2.4.2 Clarifications to Replies**

No changes, modifications, or additions to the Replies will be allowed after the Replies have been opened, except as negotiated during the negotiation phase. However, the Department reserves the right to seek clarifications from any Respondent at any time.

#### **2.5 Respondent Firm Offer**

The Department may enter into a Contract within three hundred and sixty-five (365) calendar days after the date the Notice of Intent to Award is posted, during which period Replies shall remain firm and shall not be withdrawn. If a Contract is not executed within three hundred and sixty-five (365) days, the Replies shall remain firm until either the Contract is executed or the Department receives from a Respondent written notice that the Reply is withdrawn.

### **SECTION 3. GENERAL INSTRUCTIONS**

#### **3.1 General Instructions to Respondents (PUR 1001 Form)**

The PUR 1001 Form, General Instructions to Respondents, is incorporated by reference into this solicitation but is superseded to the extent set forth herein. The form can be accessed at: [http://www.dms.myflorida.com/business\\_operations/state\\_purchasing/documents\\_forms\\_references\\_resources/purchasing\\_forms](http://www.dms.myflorida.com/business_operations/state_purchasing/documents_forms_references_resources/purchasing_forms).

**Sections 3, 5, 9, and 14 of the PUR 1001 Form are inapplicable and are replaced as follows:**

#### **Section 3. Electronic Submission of Offers**

Replies shall be submitted in accordance with Subsection 3.5, How to Submit a Reply.

#### **Section 5. Questions**

Submit questions in accordance with Subsection 2.2, Questions and Answers.

#### **Section 9. Respondent's Representation and Authorization.**

In submitting a Reply, the Respondent understands, represents, and acknowledges the following:

- The Respondent is not currently under suspension or debarment by the State or any other governmental authority.
- The Respondent, its affiliates, subsidiaries, directors, officers, and employees are not currently under investigation by any governmental authority and have not in the last ten (10) years been convicted or found liable for any act prohibited by law in any jurisdiction involving conspiracy or collusion with respect to bidding on any public contract.
- The Respondent currently has no delinquent obligations to the State, including a claim by the State for liquidated damages under any other contract.
- The submission is made in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive Reply.
- The prices and amounts have been arrived at independently and without consultation, communication, or agreement with any other Respondent or potential Respondent; neither the prices nor amounts, actual or approximate, have been disclosed to any Respondent or potential Respondent, and they will not be disclosed before the solicitation opening.
- The Respondent has fully informed the Department in writing of all convictions of the firm, its affiliates (as defined in section 287.133(1)(a), Florida Statutes), and all directors, officers, and employees of the firm and its affiliates for violation of state or federal antitrust laws with respect to a public contract for violation of any state or federal law involving fraud, bribery,

collusion, conspiracy or material misrepresentation with respect to a public contract. This includes disclosure of the names of current employees who were convicted of contract crimes while in the employ of another company.

- Neither the Respondent nor any person associated with it in the capacity of owner, partner, director, officer, principal, investigator, project director, manager, auditor, or a position involving the administration of funds:
  - Has within the preceding three (3) years been convicted of or had a civil judgment rendered against them or is presently indicted for or otherwise criminally or civilly charged for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state, or local government transaction or public contract; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; or
  - Has within a three-year period preceding this certification had one (1) or more federal, state, or local government contracts terminated for cause or reason of default that would impair the Respondent's ability to deliver the commodities or contractual services of the resultant contract.
- The commodities or contractual services offered by the Respondent will conform to the specifications without exception.
- The Respondent has read and understands the Contract terms and conditions, and the submission is made in conformance with those terms and conditions.
- If an award is made to the Respondent, the Respondent agrees that it intends to be legally bound to the Contract that is formed with the State.
- The Respondent has made a diligent inquiry of its employees and agents responsible for preparing, approving, or submitting the Reply, and has been advised by each of them that he or she has not participated in any communication, consultation, discussion, agreement, collusion, act or other conduct inconsistent with any of the statements and representations made in the Reply.
- The Respondent shall indemnify, defend, and hold harmless the Department and Customers, and their employees, against any cost, damage, or expense which may be incurred or be caused by any error in the Respondent's Reply.
- All information provided by, and representations made by, the Respondent are material and important and will be relied upon by the Department in awarding the Contract. Any misstatement shall be treated as fraudulent concealment from the Department of the true facts relating to submission of the Reply. A misrepresentation shall be punishable under law, including, but not limited to, Chapter 817, Florida Statutes.
- If at any point during the course of the procurement, circumstances change so that any of the above acknowledgements are no longer true, the Respondent will notify the Procurement Officer as soon as practicable.

#### **Section 14 – Firm Response**

The offer will be held firm in accordance with Subsection 2.5, Respondent Firm Offer.

#### **3.2 MFMP Registration**

The awarded Respondent(s), if any, must have completed this process prior to Contract execution. For additional information, please visit: <https://Respondent.myfloridamarketplace.com/>.

The awarded Respondent(s) will be required to pay the required MFMP transaction fee(s) as specified in Subsection 3.7, MyFloridaMarketPlace Transaction Fee, of Attachment B - Draft

Contract, unless an exemption has been requested and approved pursuant to Rule 60A-1.031, Florida Administrative Code.

### 3.3 Florida Substitute Form W-9 Process

A State of Florida contractor **must** have registered and completed an electronic Florida Substitute Form W-9. The Internal Revenue Service (IRS) receives and validates the information Respondents provide on the Form W-9.

For instructions on how to complete the Florida Substitute Form W-9, please visit: <http://www.myfloridacfo.com/Division/AA/StateAgencies/W-9Instructions022212.pdf>

The awarded Respondent(s), if any, must have completed this process prior to Contract execution.

### 3.4 Website References

Respondents should not incorporate or reference dynamic links that are external to the Reply documents. Provide screen shots in lieu of references to websites. References to dynamic links (Universal Resource Locators) will not be considered as part of the Respondent's Reply.

### 3.5 How to Submit a Reply

Respondents are responsible for submitting their Replies by the date and time specified in the Timeline of Events of this solicitation. Respondents are to submit the Reply in a sealed package containing the following:

**3.5.1** One (1) hard copy of a cover letter as specified in Section 3.7, Contents of Reply.

**3.5.2** One (1) electronic Reply in Adobe (.pdf) on a USB flash drive (CD/DVD format is also acceptable). Files are to be organized in accordance with Section 3.7, Contents of Reply. The Vendor's Device List; Vendor's Services and Discounts Pricing; and Vendor's Services and Discounts Pricing, Public Safety (if submitting), should be submitted in either Adobe (.pdf) or Microsoft Excel.

**3.5.3** If applicable, one (1) electronic redacted copy of the entire Reply on a USB flash drive (CD/DVD format is also acceptable), as described in Subsection 3.8, Public Records, Respondent's Confidential Information, and Redacted Replies, of this ITN. Large files should be scanned as separate files.

All electronic documents are to be searchable to the fullest extent practicable.

**Clearly mark on the outside of the sealed package the solicitation number, company name, and Procurement Officer name.**

Submit Replies to the Procurement Officer at the address listed in Subsection 1.7, Procurement Officer.

Prepare Replies simply and economically, providing a straightforward, concise delineation of the Respondent's capabilities to satisfy the requirements of this solicitation. The emphasis of each Reply should be on completeness and clarity of content.

**Replies that are not timely submitted with all required information may be deemed nonresponsive. The risk of submitting a blank or unreadable USB flash drive or CD/DVD rests with the Respondent.**

### 3.6 Mandatory Responsiveness Requirements

**The Department will not evaluate Replies that do not meet the minimum mandatory requirements listed below.** Responses to the SOW will be scored at the evaluation phase. Responses to the SOW and evaluator scores will not be used to determine the responsiveness of the Replies.

The Department reserves the right to waive any minor irregularity, technicality, or omission if the Department determines that doing so will serve the best interest of the State.

- 3.6.1** The Respondent must be, at the time of Reply submittal, a facilities-based mobile wireless service provider with a network that covers at least 90% of the nation's non-rural population. A Respondent which has been determined by the Federal Communications Commission (FCC) to be a "nationwide service provider" in the Consolidated Communications Marketplace Report – 2018, paragraph 6, page 4, and paragraph 44, page 37, is presumed to meet this coverage requirement. A Respondent not listed in the above-mentioned FCC report as a nationwide service provider must submit documentation showing that it has been independently verified by a government entity as meeting these coverage requirements. The report is located here:  
<https://docs.fcc.gov/public/attachments/FCC-18-181A1.pdf>

**The certifications required in Subsections 3.6.2 through 3.6.4 must be accomplished through the execution of Form 5, Mandatory Responsiveness Requirements, below. A Reply will be deemed nonresponsive if it fails to contain a signed Form 5.**

- 3.6.2** The Respondent must certify that it is in compliance with Subsection 3.1, General Instructions to Respondents (PUR 1001 Form), of this ITN.
- 3.6.3** The Respondent must certify that neither it, nor its affiliates, is a convicted vendor or a discriminatory vendor as described in sections 287.133 and 287.134, Florida Statutes, respectively.
- 3.6.4** The Respondent must certify that it is not on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List, and is not participating in a boycott of Israel.
- 3.6.5** The Respondent must certify that it is currently authorized to do business with the State, or will obtain authorization through the Department of State, Division of Corporations, should the Respondent be awarded the Contract, prior to Contract execution. Website:  
[www.sunbiz.org](http://www.sunbiz.org)

### 3.7 Contents of Reply

All Replies are to be organized in sections as directed below. Submit the sections of the Reply in one (1) sealed package to the Procurement Officer, organized as follows:

- 1. A cover letter on the Respondent's letterhead with the following information:**
  - a. Company name and physical address;
  - b. Primary location from where the work will be performed;

- c. Contact information for primary point of contact, including phone number and email address; and
- d. Federal Employer Identification (FEID) Number.

**2. Completed forms:**

FORM 1 – CONTACT INFORMATION  
FORM 2 – NOTICE OF CONFLICT OF INTEREST  
FORM 3 – NON-COLLUSION STATEMENT  
FORM 4 – STATEMENT OF NO PRIOR DISQUALIFYING INVOLVEMENT  
FORM 6 – BUSINESS EXPERIENCE

**3. Mandatory Responsiveness Requirements:**

A signed FORM 5 – MANDATORY RESPONSIVENESS REQUIREMENTS.

**4. Respondent's Reply to the Statement of Work (Technical Reply)**

Respondent will provide a response to each subsection in the SOW, where it is requested, by either inserting a narrative in the response blocks below the text of the numbered subsection (preferred method) or by attaching a narrative with a reference to the corresponding SOW subsection.

Note: It is the Respondent's responsibility to ensure responses are properly aligned with the corresponding SOW sections. The Department will not be responsible for evaluating portions of responses that are improperly aligned with the SOW subsections. See also Subsection 1.1, Instructions for Response Blocks, of the SOW regarding SOW Reply instructions.

Provide responses to the SOW in a font color for narrative that is different than the SOW font color.

**5. Respondent's Experience Reply**

Respondent will provide an Experience Reply that provides all the information required by this section.

The Respondent will supply a brief narrative of Respondent's prior relevant experience and ability to provide the proposed Wireless Voice Services (WVS) and Wireless Data Services (WDS) described in Attachment A – Statement of Work, including, at a minimum, a description of:

- a. Respondent's market penetration for WVS and WDS services.
- b. Respondent's experience providing services of similar scope to other public sector clients comparable to the State of Florida.
- c. Respondent's experience supporting devices and software systems of different manufacturers. List similar or like systems the Respondent has supported in the last three (3) years.
- d. Respondent's experience providing Highly-available, Highly-reliable telecommunications infrastructures and services.

- e. Respondent's experience providing sufficient staffing levels, local staffing, and a quality staff driven to proactively address issues.
- f. Proposed Key Staff – given the requirements in Sections 2.2 through 2.7 of Attachment A, Statement of Work:
  - i. Describe in detail the proposed offering for key staff positions, addressing the minimum requirements listed in the Statement of Work.
  - ii. Provide resumes for all persons being proposed for the key staff positions.
  - iii. Provide a proposed Staffing Organizational Chart, including all staff (both key staff and non-key staff) that are anticipated to be assigned to the Contract, including names and titles (full-time and part-time).
  - iv. Describe the proposed Customer Support Team model, including staffing levels, minimum qualifications, and average years of experience of the proposed team.

#### **6. Letter of Bondability**

A letter signed on or after October 1, 2020, from a surety company or bonding agent authorized to do business in the State and written on company letterhead indicating the Respondent's ability to obtain a performance bond in the amount of at least five hundred thousand dollars (\$500,000). For additional information see Section 16, Performance Bond, of Attachment B – Draft Contract.

#### **7. Pricing and Devices**

Submit the following items in one (1) separate electronic file folder:

- Vendor's Services and Discounts Pricing
- Vendor's Services and Discounts Pricing, Public Safety, if the Respondent is proposing to provide services in accordance with SOW Section 4, Public Safety Service Plans and Devices
- Vendor's Device List

**Note: The items submitted in this Pricing and Devices portion will not be evaluated or scored by the Department during the evaluation phase of the ITN, nor will these items be used to determine vendor responsiveness. The Department intends for these items to be utilized by the negotiation team to establish a baseline for service and pricing discussions with Respondents during the negotiation phase of the ITN.**

#### **3.8 Public Records, Respondent's Confidential Information, and Redacted Replies**

The following subsections supplement Section 19, Public Records, of the PUR 1001 Form, General Instructions to Respondents. By submitting a Reply, the Respondent agrees to protect, defend, and indemnify the Department for any and all claims arising from or relating to the Respondent's determination that the redacted portions of its Reply are confidential, proprietary, trade secret, or otherwise not subject to disclosure. **If the Respondent fails to mark material exempt, or fails to submit a redacted copy of information it claims is confidential, the Department is authorized to produce, in their entirety, all documents, data, or records submitted to the Department in answer to a public records request for these records.** However, no portion of a Reply will be produced in response to a public records request until such time as the Department provides notice of an intended decision with regard to this ITN or until thirty (30) days after opening the final Replies, whichever is earlier (see Section 3.8.3, Public Inspection, below, for additional information).

### **3.8.1 Electronic and Written Communications**

Unless exempted by law, all electronic and written communications pertaining to this ITN, whether sent from or received by the Department, are subject to Florida's broad Public Records Law, found in Chapter 119, Florida Statutes.

### **3.8.2 Replies**

Unless exempted by law, all materials submitted as part of a Reply to this ITN will become a public record subject to the provisions of Chapter 119, Florida Statutes. Selection or rejection of a Reply does not affect the public record status of the materials.

### **3.8.3 Public Inspection**

Unless exempted by law, all public records are subject to public inspection and copying under Chapter 119, Florida Statutes. As noted above, a time-limited exemption from public inspection is provided for the contents of Replies pursuant to section 119.071(1)(b), Florida Statutes. Once that exemption expires, all contents of Replies become subject to public inspection, unless another exemption applies. Any claim of trade secret exemption for any information contained in Respondent's Reply will be waived upon submission of the Reply to the Department, unless the claimed trade secret information is submitted in accordance with Subsection 3.8.4, How to Claim Trade Secret or Other Exemptions, below. This waiver includes any information included in the Respondent's Reply outside of the separately bound document described below.

### **3.8.4 How to Claim Trade Secret or Other Exemptions**

If a Respondent considers any portion of materials made or submitted in the course of replying to this ITN to be trade secret under section 812.081, Florida Statutes, or other applicable law, or otherwise confidential under Florida or federal law, in order to preserve the confidentiality of the material, the Respondent must clearly designate, in writing, that portion of the materials as "confidential" when submitted to the Department. The Respondent must submit all such information as a separately bound, *unredacted* document clearly labeled "Confidential, Unredacted Reply" together with a brief written description of the grounds for claiming exemption from the Public Records Law, including the specific statutory citation for such exemption.

The Respondent is to also simultaneously provide the Department with a separate, electronic *redacted* copy of its Reply. The file name of the electronic redacted copy is to contain the name of the Respondent, the ITN number, and redacted copy (e.g., Respondent Name DMS ITN \_redacted copy.pdf). Prominently display the phrase "Redacted Copy" on the first page of the electronic redacted copy and each page on which information is redacted.

The redacted copy is to be submitted no later than the Reply submittal deadline. Where such information is part of material already required to be submitted as a separately bound or enclosed portion of the Reply, further segregate it and separately bind or enclose and clearly label it as set forth above in addition to any other labeling required for the material.

Negotiation Meetings. If the Respondent is invited to negotiations, it will be incumbent upon the Respondent to identify, in real-time, portions of the Respondent's negotiation sessions that include references to materials and/or information the Respondent claims are confidential, proprietary, trade secret, or otherwise not subject to disclosure. If the Respondent fails to inform the Department that any portion of the negotiation meetings should be considered confidential, proprietary, trade secret or otherwise not subject to

disclosure, the Department is authorized to produce the audio recording in answer to a public records request for these records. The Respondent is responsible for defending its determination that the portions of the negotiation sessions are exempt and not subject to disclosure.

### **3.8.5 Public Records Request**

If a Respondent fails to mark any materials submitted to the Department as confidential, or fails to submit a redacted copy as provided in this section, or fails to claim, in real-time, portions of the negotiations sessions as exempt, the Respondent **waives** the exemption, and the Department may produce all of the Respondent's documents, data, or records or the Department's recordings of negotiation sessions to any person requesting a copy under Chapter 119, Florida Statutes. The Respondent exclusively bears the burden of complying with Subsection 3.8, Public Records, Respondent's Confidential Information, and Redacted Replies, to ensure its exempt information is appropriately marked and protected. If a requestor asserts a right to the confidential information, the Department will notify the Respondent that such an assertion has been made. It is the Respondent's responsibility to assert that the information in question is exempt from disclosure under Chapter 119, Florida Statutes, or other applicable law. If the Department becomes subject to a demand for discovery or disclosure of the confidential information of the Respondent in a legal proceeding, the Department will give the Respondent prompt notice of the demand prior to releasing the information (unless otherwise prohibited by applicable law). The Respondent is responsible for defending its determination that the redacted portions of its Reply are confidential, proprietary, trade secret or otherwise not subject to disclosure.

### **3.8.6 Department Not Obligated to Defend Respondent's Claims**

The Department is not obligated to agree with a Respondent's claim of exemption and, by submitting a Reply, the Respondent agrees to defend its claim that each and every portion of the redacted material is exempt from inspection and copying under the Public Records Law. Further, by submitting a Reply, the Respondent agrees to protect, defend, indemnify and hold harmless the Department for any and all claims and litigation (including litigation initiated by the Department), including attorney's fees and costs, arising from or in any way relating to Respondent's assertion that the redacted portions of its Reply or portions of the negotiation sessions are trade secrets or otherwise exempt from public disclosure under Chapter 119, Florida Statutes. The Department may use counsel of its choosing to defend any such claims, and the Respondent shall promptly pay the Department's invoices for legal services on a monthly basis for all costs and expenses, including legal fees, incurred in defending such claims.

### **3.9 Additional Information**

By submitting a Reply, the Respondent certifies that it agrees to all criteria specified in this solicitation. The Department may request, and the Respondent shall provide, clarifying information or documentation. Failure to supply the information or documentation as requested may result in the Reply being deemed non-responsive.

### **3.10 Respondent's Pricing**

Respondents are to submit pricing at the time of their Reply. Pricing should be submitted as if the terms and conditions of Attachment B – Draft Contract are final. There is no guaranteed minimum spend from the Department or the Customers. Respondents are instructed to only submit pricing for services that are within the contemplated scope of this procurement, including additional options or features proposed by the Respondent that are in accordance with the SOW.

If the proposed pricing includes services outside of the scope of the Contract, those services will not become part of the Contract and will neither be included in CSAB nor be offered to Customers.

Pricing must be uniform with no variation for geographic location of service delivery.

Respondents are encouraged to provide the best possible pricing at all times. Pricing submitted will be considered pricing for the initial and any renewal periods.

Respondents' proposed pricing is inclusive of all government sanctioned surcharges and fees (as provided in the SOW, Subsection 5.6, Taxes and Government Sanctioned Fees) necessary to deliver the proposed services, unless otherwise separately identified in the Reply. The only additional costs permitted will be reasonable costs for expedited orders.

### **3.10.1 Vendor's Device List**

The Respondent should submit a Vendor's Device List of the Respondent's proposed devices and pricing, which will become part of the final Contract, as modified during negotiations. The Vendor's Device List should include all proposed devices, including, at a minimum, cellular phones, smartphones, tablets, broadband access devices (data-only), cellular mobile broadband devices (support for internet access), devices supporting secure access to MFN, and accessories. Devices may be shown with a variety of packages, with detailed pricing, and descriptions of associated services, devices and/or features. Any services, devices and/or features provided at no cost should be identified as \$0.00. If the Respondent is proposing Public Safety services and devices, the Vendor's Device List may also include Public Safety wearables and other Public Safety wireless enabled devices.

For all items listed below, the Vendor's Device List should include: manufacturer and model, vendor's identification number (SKU), vendor's commercially advertised retail price as of the date the Reply is submitted to the Department, State purchase price, and any promotional pricing, as well as the following device-specific information:

- 1) Smartphones
  - a. Operating system, camera, removable memory, hearing aid compatibility, mode, and other features.
  - b. At least one unlocked iPhone and one unlocked Android smartphone.
- 2) Air Cards and hotspots
  - a. Mode, compatibility with 4G LTE, compatibility with 5G, compatibility with Apple Operating Systems (iOS, Mac OS), compatibility with Microsoft Operating systems (Windows), external antenna, and other features.
- 3) Tablets
  - a. Operating system, camera, removable memory, and other features.
- 4) Basic Phones
  - a. At least one basic phone that is available to Customers at no charge, other than the cost of the purchased service plan.
- 5) Accessories
  - a. May include phone cases, tablet cases, headphones and ear buds, chargers, screen protectors, foldable keyboards, belt clips, and hands-free kits.
- 6) Public Safety Wearables

### 3.10.2 Vendor's Services and Discount Pricing

The Respondent should submit services and discount pricing, which will become part of the final Contract, as modified during negotiations. If bidding on the public safety portion of this procurement, the Respondent should also submit public safety-specific pricing. Respondents may mirror the formats of existing End User Price Lists (EUPLs), also referred to as User Rates, or create their own. The current EUPLs can be found on this DMS website: [https://www.dms.myflorida.com/business\\_operations/telecommunications/suncom2/voice\\_services/mobile\\_communication\\_services](https://www.dms.myflorida.com/business_operations/telecommunications/suncom2/voice_services/mobile_communication_services). Respondent's should state prices as monthly recurring charges (MRC) or non-recurring charges (NRC).

The Services and Discounts Pricing should include the following, at a minimum:

#### 1) Non-pooled Plans

- a. Pricing and details of all non-pooled plans, which may include:
  - i. Voice per minute rate plans: usage based, limited
  - ii. Unlimited plans: voice; voice and text; voice, text, and data; voice, data, messaging, and hotspot
  - iii. Messaging plans: limited and unlimited
  - iv. Data only device plans: per megabyte data plan, data plan with tethering, data plan without tethering, and unlimited data
- b. Relevant unit pricing, including price per minute, variation of price per minute for nights and weekends, monthly rollover of minutes or data.
- c. Description of services included in the monthly recurring costs, including the number of messages (SMS/MMS), minutes (anytime, nights, or weekends), data limits, and included features, such as call waiting.
  - i. Detail how airtime and other measured usage are billed; for example, in full-minute increments, rounded up to the next full increment at the end of each call for billing purposes, unanswered outgoing calls incurring airtime.
  - ii. Description of billing for calls directly dialing or receiving from the same carrier.
  - iii. If the pricing changes for nights and weekends, describe the times the carrier deems are nights and weekends and any changes to charges during this time.
  - iv. Detail any prohibited activities, such as those prohibited for compliance with the law or to prevent interference with the network.

#### 2) Pooled Plans

- a. Pricing and details of all pooled plans, which may include:
  - i. Description of tiers, including the number of minutes included in the plans.
- b. Relevant unit pricing, including price per minute, variation of price per minute for nights and weekends, monthly rollover of minutes or data.
- c. Describe:
  - i. how the minutes are aggregated and credits are applied;
  - ii. how a Customer can have more than one pool;
  - iii. rollover minutes;
  - iv. pool limitations, e.g., limits to the number of users; and
  - v. included features, such as call waiting.

#### 3) Push-to-Talk

- a. Pricing and details of all push-to-talk plans, which may include:
  - i. Standalone push-to-talk and add-on push-to-talk plans.
  - ii. Relevant unit pricing including price per minute, variation of price per minute for nights and weekends, monthly rollover of minutes or data.

- iii. Description of services included in the monthly recurring costs and included features
  - 1. Detail how measured usage is billed, for example, in full-minute increments, rounded up to the next full increment at the end of each call for billing purposes, or unanswered outgoing calls incurring airtime.
  - 2. If the pricing changes for nights and weekends, describe the times the carrier deems are nights and weekends and any changes to charges during this time.
  - 3. Detail any prohibited activities, such as those prohibited for compliance with the law or to prevent interference with the network.

**4) Machine-to-Machine**

- a. Pricing and details of all machine-to-machine and internet of things service plans which may include:
  - i. Description of tiers, including the usage caps of each tier. One (1) MB to twenty (20) GB requested, at minimum.
- b. Relevant unit pricing, including price per minute, variation of price per MB for nights and weekends, and monthly rollover of minutes or data.
- c. Description of services included in the monthly recurring costs and included features.
  - i. Detail how measured usage is billed.
  - ii. Detail any prohibited activities, such as those prohibited for compliance with the law or to prevent interference with the network.

**5) Discounts**

- a. All proposed discounts off accessories and devices.
- b. State what published price the discount percentage applies to (MSRP, vendor published catalog, etc.).
  - i. Describe any additional proposed discounts, such as 100% discount off activation fees.
  - ii. Specific pricing for devices should be listed in the Vendor's Device List.

**6) Additional Features, Fees, and Other Items**

- a. Respondents may describe and detail any additional offerings that are contemplated within the SOW.
  - i. These shall include surcharges and fees (see SOW Section 5.6, Taxes and Government Sanctioned Fees).
  - ii. These may include chargeable features, such as robo-call blocking, mobile device management, etc.
  - iii. Respondents may also suggest tiered pricing.
  - iv. Where applicable, Respondents should detail the plan name and type, monthly recurring cost, etc.
- b. There will be no activation fees for services and devices purchased off the Contract. Current MCS contracts do not allow activation fees for services and devices.

**SECTION 4. SELECTION METHODOLOGY**

**4.1 Responsiveness and Responsibility**

The Department will determine which Respondents are responsive and responsible, and which have submitted a Responsive Reply that meets the requirements of this solicitation (see section

287.012, Florida Statutes). The Department will perform the initial responsiveness check. Replies found to be nonresponsive will not be evaluated.

The Department reserves the right to act upon information discovered after the initial responsiveness check impacting the responsibility or responsiveness of the Respondent.

#### 4.2 Evaluation Process – General Overview

The Department will appoint an evaluation team for the evaluation and scoring of the Responsive Replies for the evaluation phase. Each evaluator will be provided a copy of each Respondent's Reply that is deemed Responsive.

The evaluators will score Replies against the evaluation criteria set forth in subsection 4.3, Evaluation of the Reply, in order to establish a competitive range of Replies reasonably susceptible of award. The Evaluation Summary Score Sheet Table, to be used by the Department to calculate evaluation scores, provides for the SOW sections that will be scored and the relative weights given to the scored sections.

See subsection 4.4, Negotiations, for information on the negotiation phase of the ITN. All Replies that meet the Mandatory Responsiveness Requirements will be evaluated as described in section 4, Selection Methodology.

#### 4.3 Evaluation of the Reply

The evaluators will independently review and evaluate the Responsive Replies. Using the assessment scale below, the evaluators will assign scores zero (0) to four (4) based on the quality of each section of the Reply to the SOW. In determining the quality of a Reply, the evaluators will use the following guiding questions:

- How well does the Reply demonstrate an understanding of the services requested?
- How well does the Reply demonstrate the Respondent's ability to provide the services requested?
- How well does the Reply address the requested services?

<b>Assessment</b>	<b>Evaluator Score</b>
Unacceptable	0
Poor	1
Adequate	2
Good	3
Exceptional	4

##### 4.3.1 Scoring

Scoring, for purposes of determining the competitive range, will be a total of the evaluator's weighted scores for each Respondent for all scored sections of the SOW.

The table below demonstrates the calculations the Department will use to determine the Respondent's Final Weighted Score, based on the raw scores given by the Evaluation Team members while evaluating the Respondent's Reply.

The Raw Points scored for each section, by each evaluator, will be averaged together and then multiplied by the Weight Factor in the table below for each section. This calculation will render the Respondent's Weighted Scores for each section. The Respondent's Weighted Scores for each section will be added together to determine the Respondent's Final Weighted Score.

<b>EVALUATION SUMMARY SCORE SHEET</b>					
<b>Section</b>	<b>Maximum Possible Raw Score</b>		<b>Weight Factor</b>		<b>Maximum Possible Weighted Score</b>
<b>1.6</b> Evolving Technology	4	X	50	=	200
<b>2.1</b> Staffing Responsibilities	4	X	100	=	400
<b>3.6</b> Wireless Data Services	4	X	75	=	300
<b>3.10</b> State of Florida Coverage	4	X	50	=	200
<b>3.12</b> Security	4	X	50	=	200
<b>3.16</b> Highly Available and Highly Reliable Design Characteristics	4	X	25	=	100
<b>3.17</b> Reports, Updates, and Notification Requirements	4	X	50	=	200
<b>3.19</b> Customer Support	4	X	50	=	200
<b>3.20</b> Contractor's MCS Portal	4	X	25	=	100
<b>3.21</b> Devices	4	X	50	=	200
<b>3.22</b> Cooperation with Other Contractors	4	X	25	=	100
<b>3.23</b> Customer Migration	4	X	75	=	300
<b>3.26</b> Project Management	4	X	25	=	100
Respondent's Experience Reply	4	X	300	=	1,200
<b>Maximum Possible Final Weighted Score:</b>					<b>3,800</b>

For additional instructions for replying to the SOW, see SOW subsection 1.1. For selection methodology, scoring, and weighting, see this ITN section 4, Selection Methodology.

#### **4.3.2 Other Department Rights for Evaluation**

The Department reserves the right at any time during the Evaluation Process to:

1. Conceal pricing information from evaluators or provide an instruction to evaluators to disregard pricing information in their evaluation of a Responsive Reply.
2. Redact, omit, or provide instruction to evaluators to disregard any portions of a proposed offering which the Department determines are outside of the scope of this procurement.

## **4.4 Negotiations**

### **4.4.1 Negotiations Process – General Overview**

After the evaluation of Replies based on the criteria identified above, the Department will establish a competitive range of Replies reasonably susceptible of award and will select one (1) or more Respondents within the competitive range to commence negotiations.

The Department will establish a negotiation team to conduct the negotiations. The negotiation team will make a recommendation of (an) award(s) to the Respondent(s) that will provide best value based on the selection criteria in the ITN. The negotiation team will not be bound by evaluator scoring but may use the evaluator scoring as a reference tool during the negotiation process.

The Department will require the Respondent(s) to provide the Vendor's Services and Discounts Pricing; Vendor's Services and Discounts Pricing, Public Safety (if proposing public safety services); and Vendors Device List if they were not originally included in the Respondent's Reply.

All pricing submitted may be reduced during negotiations but cannot be raised unless the increase is reflected in the BAFO and is directly related to changes in offered services in the BAFO and as negotiated in accordance with this ITN. During the negotiation process, the Department also reserves the right to negotiate a la carte services, categories, and components of services.

The format and content of any pricing submissions, including but not limited to BAFOs, may be amended during negotiations at the discretion of the negotiation team.

The Department reserves the right to negotiate different terms, additional terms, and related price adjustments if the Department determines that such changes would provide the best value to the State. Additional operational requirements may be defined and clarifications required.

The Department may require additional technical detail, diagrams, demonstrations, and documentation. The negotiation team may request proposed alternative terms or deliverables during negotiations, but it is under no obligation to accept proposed alternative terms or deliverables.

The Department reserves the right to negotiate concurrently or sequentially with competing Respondent(s). Negotiations will not be open to the public but will be recorded. Recordings of negotiations and negotiation team strategy meetings will be subject to the provisions of section 286.0113, Florida Statutes.

Negotiation meetings will be conducted in Tallahassee, Florida, if conducted in-person, or using technology-based solutions, if conducted remotely. The Department reserves the right to schedule in-person negotiations at a different location in the State. The Department may distribute an agenda in advance of any negotiation session. Representatives for each Respondent should plan to be available, at least by telephone, without interruptions, for the entirety of the Respondent's scheduled negotiation meeting(s).

Negotiations will continue as determined by the negotiation team, until acceptable terms and conditions are agreed upon through a BAFO, if applicable, or it is determined that an acceptable agreement cannot be reached. The Department reserves the right to conclude negotiations at any time and proceed to Contract award.

#### **4.4.2 Respondent Attendance at Negotiations**

The Department reserves the right to limit the number of representatives permitted to attend the negotiation sessions.

#### **4.4.3 Revised Replies and Best and Final Offers**

During the negotiation phase, the Department may request clarification and revisions to Replies (including BAFOs) and identify information to be submitted to the Department until it is satisfied

that it has achieved the best value for the State. Failure to provide information requested by the Department during the negotiation phase may result in termination of negotiations with the Respondent.

It is anticipated that the Department will use language in the Request for BAFO expressing contractual requirements within the procurement documents where the language was previously permissive. For example, the word 'should' may be replaced by the word 'must' in the final SOW attached to the Request for BAFO.

#### **4.4.4 Other Department Rights During Negotiations**

The Department has sole discretion in deciding whether and when to take any of the following actions and to decide the scope and manner of such actions.

The Department reserves the right at any time during the negotiation process to:

- a) Schedule additional negotiation sessions with any or all Respondents.
- b) Require any or all Respondents to provide additional, revised, or final written Replies addressing specific topics, including, but not limited to, modifications to the solicitation specifications, terms and conditions, or business references.
- c) Require any or all Respondents to provide revised Replies and written BAFO(s).
- d) Require any or all Respondents to address services, prices, or conditions offered by any other Respondent.
- e) Pursue a Contract with one (1) or more Respondents for the services encompassed by this solicitation, including any addendums thereto and any request for additional, revised, or final written Replies or request for BAFOs.
- f) Pursue the division of Contracts between Respondents by type of service or geographic area, or both.
- g) Finalize Contract terms and conditions with any Respondent at any time.
- h) End negotiations with any or all Respondents at any time, regardless of the status of or schedule of negotiations, and to continue with other Respondents, or not continue with any Respondents.
- i) Conclude negotiations at any time and proceed to Contract award.
- j) Re-open negotiations with any responsive Respondent.
- k) Take any additional, administrative steps deemed necessary in determining the final award, including conducting demonstrations, additional fact-finding, evaluation, or negotiation where necessary and consistent with the terms of this solicitation.
- l) Request the assistance of and use subject matter experts for any portion of the procurement or throughout the procurement.
- m) Review and rely on relevant information contained in the Replies.
- n) Request pricing options different from the initial pricing provided by the Respondent. This information may be used in negotiations.
- o) Request business references and materials related to a reference check.
- p) Contact Respondent's Customers, if any, or other entities with information relevant to the Respondent's responsibility, experience, and/or ability.

#### **4.4.5 Negotiation Meetings Not Open to Public**

In accordance with section 286.0113, Florida Statutes, negotiations between the Department and Respondents are exempt from Chapter 286, Florida Statutes, and s. 24(b), Art. I of the State

Constitution. Also, any portion of a team meeting at which negotiation strategies are discussed are exempt from section 286.011, Florida Statutes.

The Department will record all meetings of the negotiation team and all negotiation meetings between the Department and Respondents, as required by law, and such recordings will eventually become public record pursuant to Chapter 286, Florida Statutes. During negotiations, Respondents must inform the Department if any portion of the meetings should be considered confidential, proprietary, trade secret, or otherwise not subject to disclosure pursuant to Chapter 119, Florida Statutes, the Florida Constitution, or other authority, so that the Department can make appropriate arrangements for the segregation of the recording.

## **4.5 Final Selection and Notice of Intent to Award Contract**

### **4.5.1 Award Selection**

Contract(s) will be awarded, if any award is made, to the responsive and responsible vendor(s) whose BAFO is assessed as providing the best value to the State in accordance with the selection criteria of this ITN.

### **4.5.2 Selection Criteria**

The following award selection criteria will apply for this ITN:

- a) The Respondent's demonstration of its prior relevant experience, including track record, and the overall professional experience of the Respondent at providing the proposed services;
- b) The Respondent's ability and approach to meeting the goals of the ITN, as stated in subsection 1.5, Goals of the ITN, and SOW subsection 1.3, MCS Objectives;
- c) The Respondent's ability and approach to providing the services and associated devices sought in the SOW;
- d) The Respondent's pricing.

### **4.5.3 Department's Negotiation Team Recommendation**

The Department's negotiation team will make a recommendation as to the Contract award(s) that will provide the best value to the State based on the selection criteria.

## **SECTION 5. AWARD**

### **5.1 Rights for Award**

The Department reserves the right to:

- Award a contract to one (1) or more Respondents for the services encompassed by this solicitation.
- Award a contract to one (1) or more Respondents, or no Respondents at all, for all or part of the work contemplated by this solicitation.
- Select one (1) or more Respondents by type of service, geographic area, and/or both.
- Award contracts for less than the entire geographic area.
- Award and contract with other Responsive Respondents in the event that the Department is unable to contract with the initially awarded Respondent(s).
- Reject all Replies and determine whether to reissue a competitive solicitation.
- Withdraw or cancel the solicitation and make no award.

**5.2 Agency Decision**

The Department will post a Notice of Intent to Award to enter into one (1) or more contracts with the Respondent(s) identified therein, on the VBS website: [http://vbs.dms.state.fl.us/vbs/main\\_menu](http://vbs.dms.state.fl.us/vbs/main_menu).

If the Department decides to reject all Replies, it will post its notice on the VBS website: [http://vbs.dms.state.fl.us/vbs/main\\_menu](http://vbs.dms.state.fl.us/vbs/main_menu).

**5.3 Other Reserved Rights**

- The Department has the right to use any or all ideas or adaptations of the ideas presented in any Reply. Selection or rejection of a Reply will not affect this right.
- The Department reserves the right, after posting a Notice of Intent to Award, to withdraw or cancel the procurement, or amend its Notice of Intent to Award and re-open negotiations with any Respondent at any time prior to execution of a Contract.

**5.4 No Contract until Execution**

A Notice of Intent to Award under this ITN shall not constitute or form any contract between the Department and a Respondent. No contract shall be formed until such time as a Respondent and the Department formally execute a contract with requisite written signatures.

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK**

### FORM 1 – CONTACT INFORMATION

For solicitation purposes, the Respondent's contact person will be:

Should the Respondent be awarded the Contract, the Account Manager's contact information will be:

Name	_____	_____
Title	_____	_____
Company Name	_____	_____
Address	_____	_____
Telephone	_____	_____
Fax	_____	_____
E-mail	_____	_____
FEID #	_____	_____

\_\_\_\_\_  
Name of Respondent's Organization

\_\_\_\_\_  
Signature of Authorized Representative and Date

\_\_\_\_\_  
Print Name

**FORM 2 - NOTICE OF CONFLICT OF INTEREST**

**Company Name** \_\_\_\_\_

For the purpose of participating in the solicitation process and complying with the provisions of Chapter 112, Florida Statutes, the company states the following conflict(s) of interest exists as noted below (if none, write N/A in the applicable section(s) below):

The persons listed below are corporate officers, directors, or agents and are currently employees of the State of Florida or one of its agencies:

_____	_____
_____	_____
_____	_____

The persons listed below are current State of Florida employees who own an interest of five percent (5%) or more in the company named above:

_____	_____
_____	_____
_____	_____

\_\_\_\_\_  
Name of Respondent's Organization

\_\_\_\_\_  
Signature of Authorized Representative and Date

\_\_\_\_\_  
Print Name

**FORM 3 - NON-COLLUSION STATEMENT**

I state that I \_\_\_\_\_ of \_\_\_\_\_,  
(Name and Title) (Name of Respondent)

am authorized to make this statement on behalf of my firm and its owner, directors, and officers. I am the person responsible in my firm for the price(s) and amount(s) submitted in response to this ITN and the preparation of the Reply. I state that:

1. The price(s) and amount(s) submitted in response to this ITN, either in the initial Reply or during negotiations, will be arrived at independently and without consultation, communication, or agreement with any other Respondent or potential Respondent.
2. Neither the price(s) nor the amount(s) submitted in response to this ITN, and neither the approximate price(s) nor approximate amount(s) submitted in response to this ITN, either in the initial Reply or during negotiations, have been or will be disclosed to any other firm, vendor, Respondent, or potential Respondent, and they will not be disclosed before Reply opening.
3. No attempt has been made or will be made to induce any firm or persons to refrain from submitting a Reply to this ITN, or to submit prices higher than the prices submitted in this Reply, or to submit any intentionally high or noncompetitive price(s) or other form of complementary Reply.
4. The Reply of my firm is made in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive Reply.
5. \_\_\_\_\_, its affiliates, subsidiaries, officers, director, and employees  
(Name of Respondent)

are not currently under investigation by any governmental agency and have not in the last ten (10) years been convicted or found liable for any act prohibited by state or federal law in any jurisdiction involving conspiracy or collusion with respect to a bid on any public contract, except as follows:

I state that I and the named firm understand and acknowledge that the above representations are material and important and will be relied on by the State of Florida for which this Reply is submitted. I understand, and my firm understands, that any misstatement in this statement is, and will be treated as, fraudulent concealment from the State of Florida of the true facts relating to the submission of Replies for this contract.

Dated this \_\_\_\_\_ day of \_\_\_\_\_

Name of Respondent: \_\_\_\_\_

Signed by: \_\_\_\_\_

Print Name \_\_\_\_\_

**FORM 4 - STATEMENT OF NO PRIOR DISQUALIFYING INVOLVEMENT**

I, as an authorized representative of the Respondent, certify that nothing in section 287.057(17)(c), Florida Statutes (see below), prohibits the Respondent's entry into any Contract resulting from this solicitation.

**Section 287.057(17)(c), Florida Statutes:** A person who receives a contract that has not been procured pursuant to subsections (1)-(3) [of s. 287.057, F.S.] to perform a feasibility study of the potential implementation of a subsequent contract, who participates in the drafting of a solicitation or who develops a program for future implementation, is not eligible to contract with the agency for any other contracts dealing with that specific subject matter, and any firm in which such person has any interest is not eligible to receive such contract. However, this prohibition does not prevent a Respondent who responds to a request for information from being eligible to contract with an agency.

\_\_\_\_\_  
Name of Respondent's Organization

\_\_\_\_\_  
Signature of Authorized Representative and Date

\_\_\_\_\_  
Print Name

### FORM 5 – MANDATORY RESPONSIVENESS REQUIREMENTS

The Respondent certifies that it is in compliance with Subsection 3.1, General Instructions to Vendors (PUR 1001 Form).
The Respondent certifies that neither it, nor its affiliates, is a convicted vendor or a discriminatory vendor as described in sections 287.133 and 287.134, Florida Statutes, respectively.
The Respondent certifies that it is not on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List, and is not participating in a boycott of Israel.
The Respondent certifies that it is currently authorized to do business with the State, or will obtain authorization through the Department of State, Division of Corporations, should the Respondent be awarded the Contract, prior to Contract execution. Website: <a href="http://www.sunbiz.org">www.sunbiz.org</a>
The Respondent must be, at the time of Reply submittal, a facilities-based mobile wireless service provider with a network that covers at least 90% of the nation’s non-rural population. A Respondent which has been determined by the Federal Communications Commission (FCC) to be a “nationwide service provider” in the Consolidated Communications Marketplace Report – 2018, paragraph 6, page 4, and paragraph 44, page 37, is presumed to meet this coverage requirement. A Respondent not listed in the above-mentioned FCC report as a nationwide service provider must submit documentation showing that it has been independently verified by a government entity as meeting these coverage requirements. The report is located here: <a href="https://docs.fcc.gov/public/attachments/FCC-18-181A1.pdf">https://docs.fcc.gov/public/attachments/FCC-18-181A1.pdf</a>

Signature below certifies that the signatory has the authority to respond to this solicitation on the Respondent’s behalf and certifies conformance with all Mandatory Responsiveness Requirements listed above.

\_\_\_\_\_  
Name of Respondent’s Organization

\_\_\_\_\_  
Printed Name of Organization’s Authorized Representative

\_\_\_\_\_  
Signature of Organization’s Authorized Representative

\_\_\_\_\_  
Date

**FORM 6 - BUSINESS EXPERIENCE**

Provide the information requested below. Print and complete this form as many times as needed to demonstrate experience in providing the same or similar services sought in this procurement.

The experience cannot be from:

- a. Current employees of DMS.
- b. Former employees of DMS within the past three (3) years.
- c. Persons currently or formerly employed by the Respondent's organization.
- d. Board members of the Respondent's organization.
- e. Relatives.
- f. Corporations based solely in a foreign country.
- g. Any person involved in the drafting of this ITN or the procurement process.

The same entity may not be listed more than once.

In the event the Respondent has had a name change since the time work was performed for a listed reference, the name under which the Respondent operated at that time should be provided in the space provided for "Brief Summary of Services."

The Department reserves the right to contact entities stated below, and also other than those identified by the Respondent, to obtain additional information regarding past performance. The Department may also solely rely on the information stated below without contacting the entities state below.

<b>Information</b>	<b>Experience #1</b>
Company Name	
Company Person	
Title	
Address	
City	
State	
Telephone Number	
Email Address	
Contract Period (contract start date to contract end date)	
Brief summary of services	

<b>Information</b>	<b>Experience #2</b>
Company Name	
Company Person	
Title	
Address	
City	
State	
Telephone Number	
Email Address	

Contract Period (contract start date to contract end date)	
Brief summary of services	

<b>Information</b>	<b>Experience #3</b>
Company Name	
Company Person	
Title	
Address	
City	
State	
Telephone Number	
Email Address	
Contract Period (contract start date to contract end date)	
Brief summary of services	



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](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](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

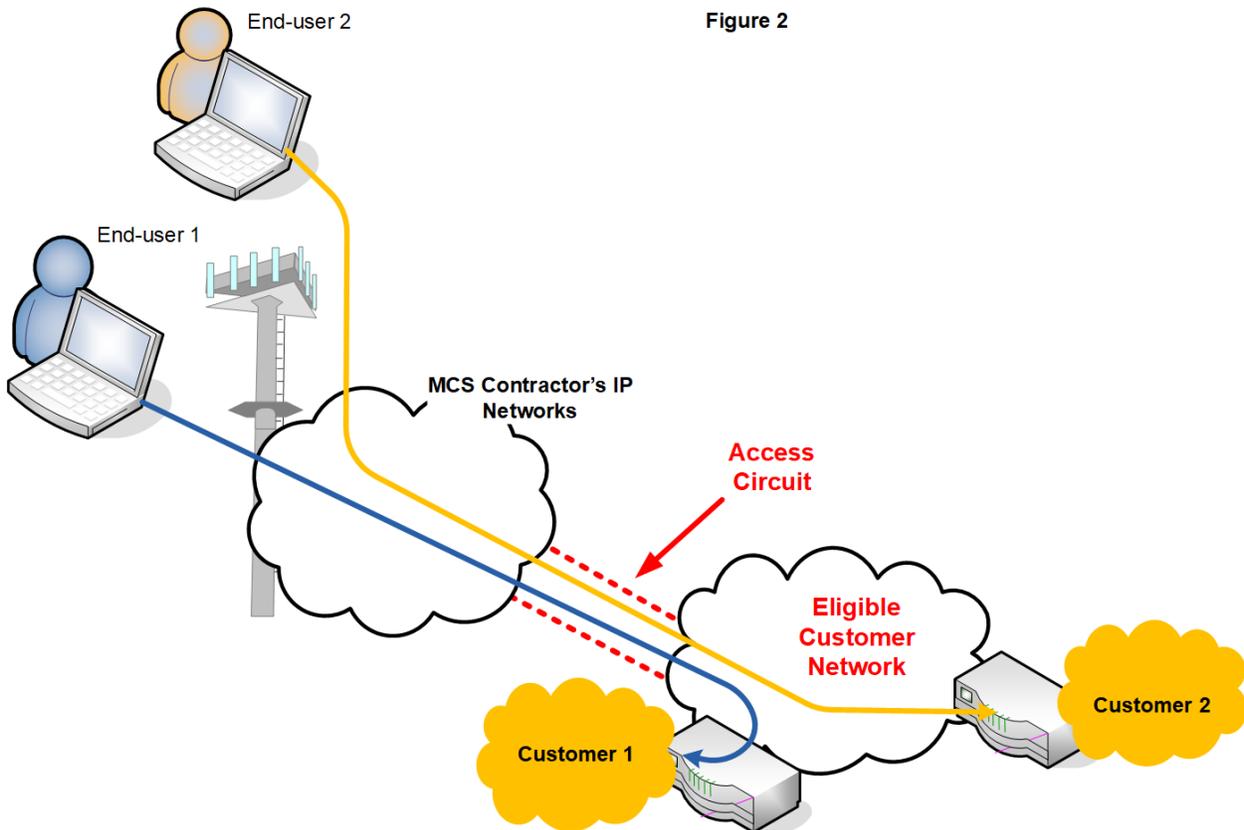
This subsection is applicable only to Wireless Data Services.

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.

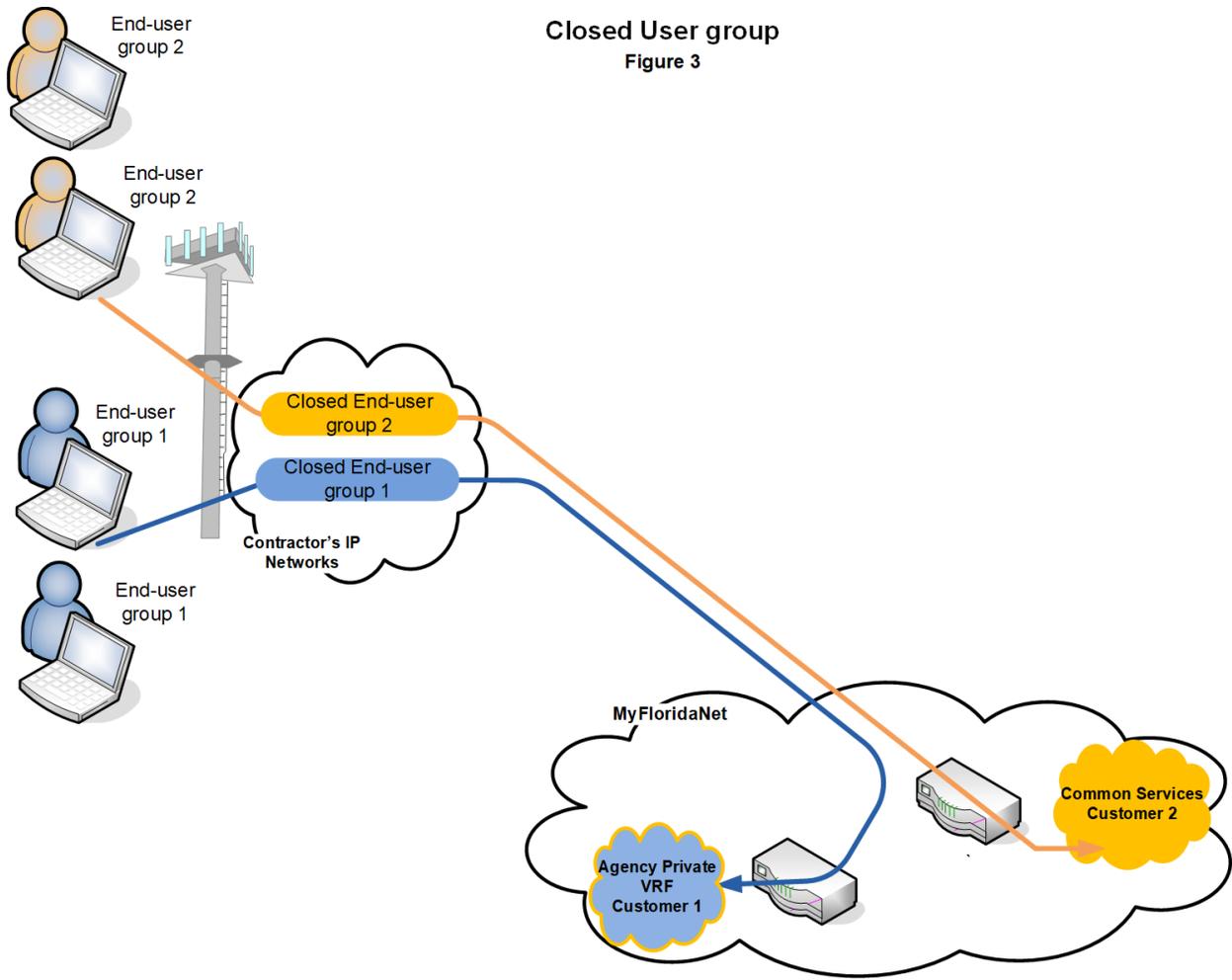
### 3.5 Wireless Data Service - Closed User Groups

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.

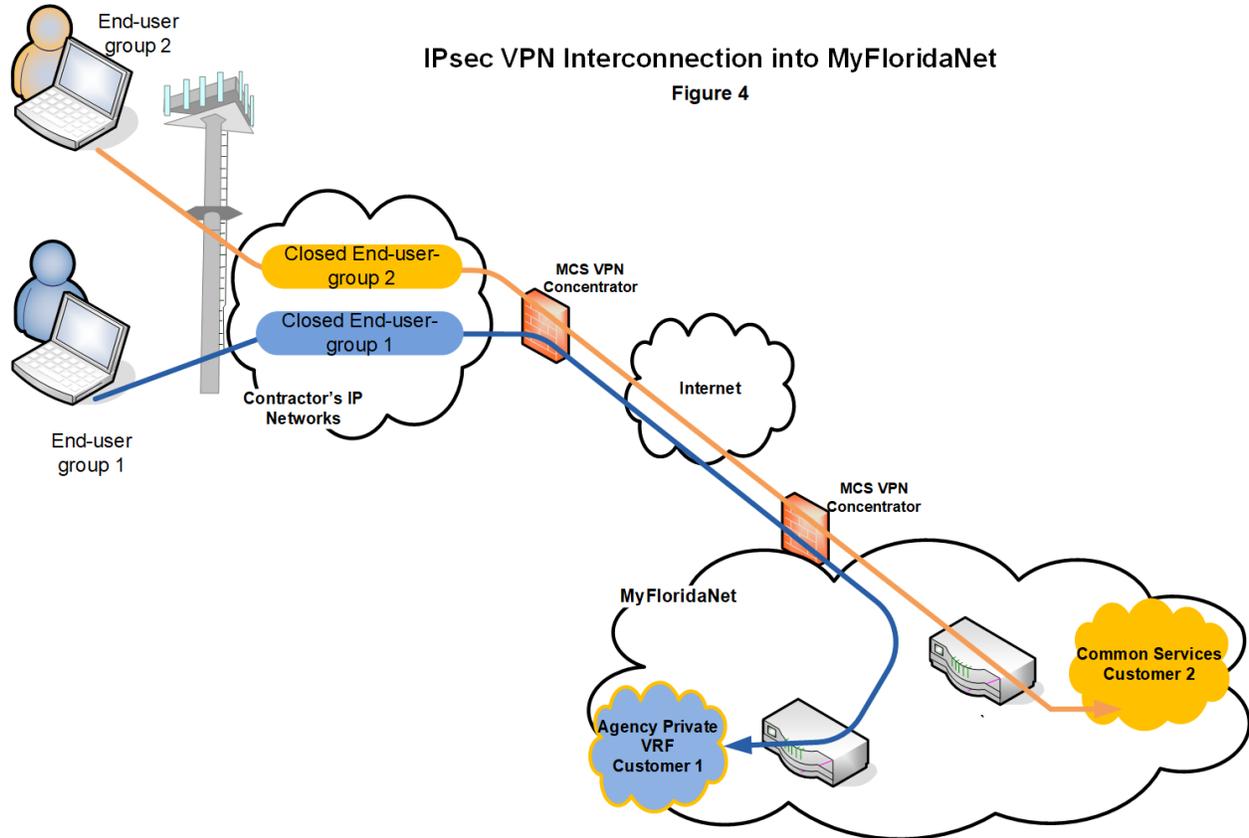
### 3.6 Wireless Data Service – Network-to-Network Interface Design

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

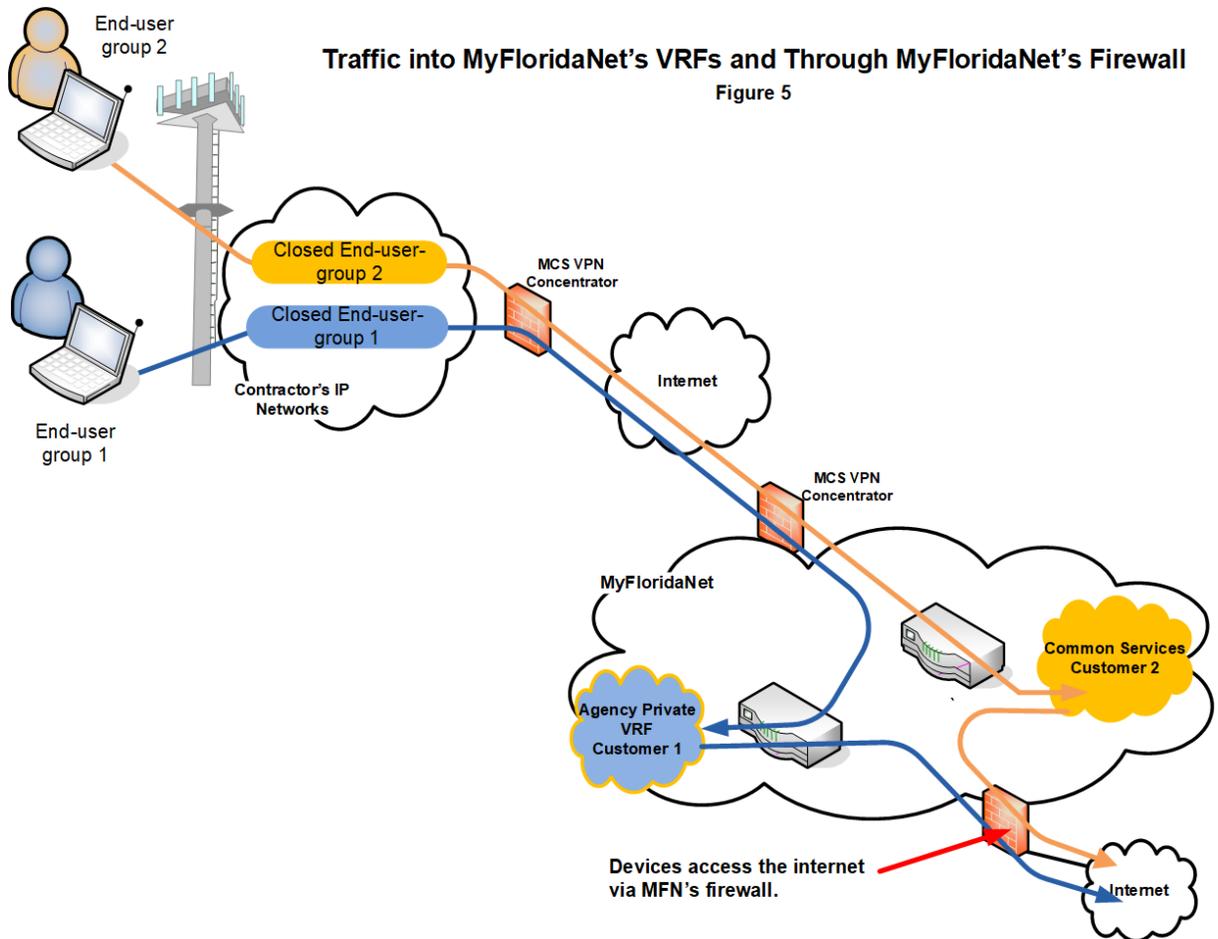
This subsection is applicable to only Wireless Data Services.

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

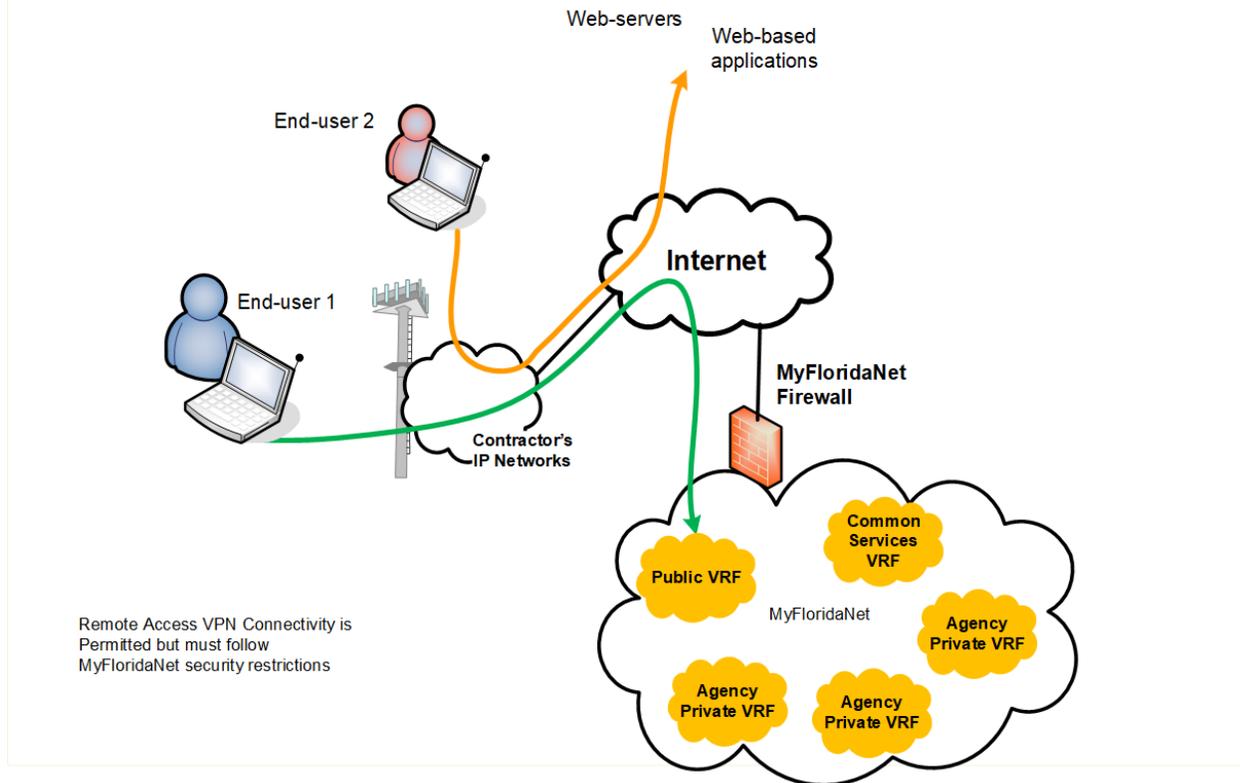
This subsection is applicable to only Wireless Data Services.

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

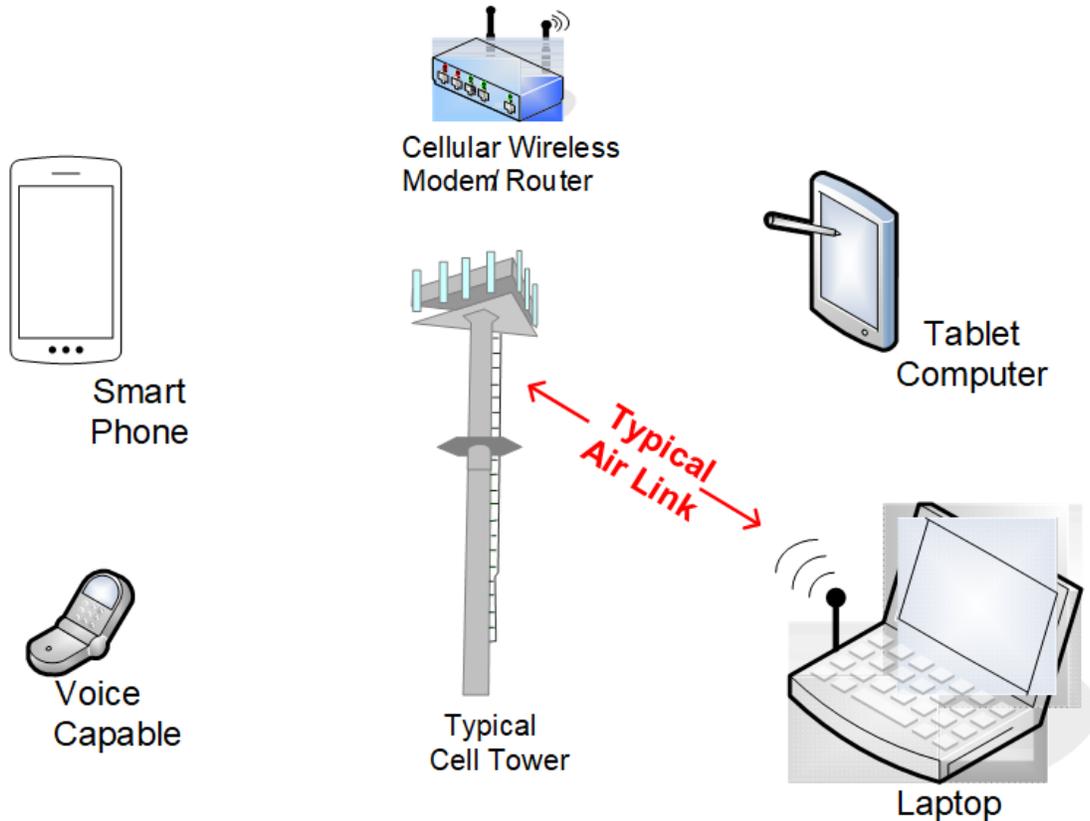
This subsection is applicable to both WVS and WDS.

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.

<b>Infrastructure Checklist</b>	
<b>Section Reference</b>	<b>Requirement</b>
<b>SOW Section 2</b>	
<b>2.1 - 2.6</b>	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.
<b>2.7</b>	The Contractor has demonstrated that its Customer Support Team is staffed and trained.
<b>SOW Section 3</b>	
<b>3.5</b>	Contractor's closed user group isolation method is developed and approved by DMS.
<b>3.6</b>	The Network-to-Network Interface is operational.
<b>3.7</b>	Closed user group traffic successfully mapped into MFN and as permitted is able to access the internet via the MFN firewall.
<b>3.8</b>	MCS traffic is routed directly to the internet.
<b>3.9</b>	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.
<b>3.12</b>	Security and fraud services are ready for production.
<b>3.13</b>	Processes related to test and demonstration accounts for WVS and WDS are final.
<b>3.14</b>	Emergency services programs are ready for production.
<b>3.16</b>	Design characteristics have been reviewed and are ready for production.
<b>3.17</b>	Reports and reporting options are ready for production.
<b>3.18</b>	SLA processes are ready for production.
<b>2.7 and 3.19</b>	The Customer Support Team is staffed and trained.

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

<b>SOW Section 6</b>	
----------------------	--

<b>6</b>	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.

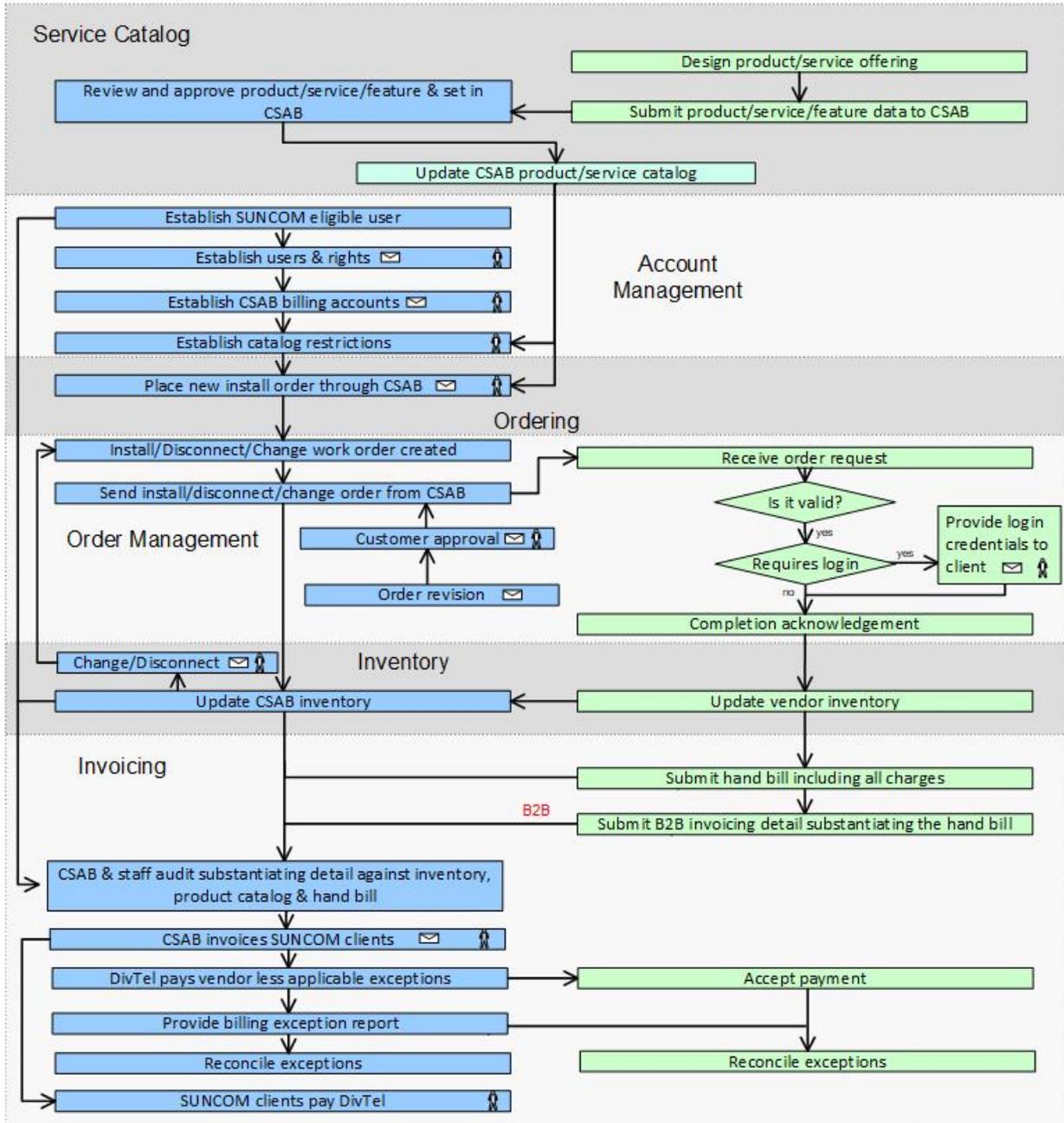
### 5.2 Communications Service Authorization and Billing Transaction Flowchart

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

**DST** **Vendor**



**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 10<sup>th</sup> 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 1<sup>st</sup> 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.**



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

**Ron DeSantis, Governor**  
Jonathan R. Satter, Secretary

---

**ATTACHMENT B**

**DRAFT CONTRACT**

**FOR**

**MOBILE COMMUNICATION SERVICES**

**CONTRACT NO: DMS-19/20-006**

**BETWEEN**

**THE STATE OF FLORIDA**

**DEPARTMENT OF MANAGEMENT SERVICES**

**AND**

**<<PARTY NAME>>**

# DRAFT CONTRACT

## Table of Contents:

SECTION 1. CONTRACT TERM AND TERMINATION .....	3
SECTION 2. CONTRACT DOCUMENTS AND HIERACHY .....	4
SECTION 3. PAYMENT AND FEES.....	4
SECTION 4. CONTRACT ADMINISTRATION.....	6
SECTION 5. CONTRACT MANAGEMENT.....	8
SECTION 6. COMPLIANCE WITH LAWS.....	9
SECTION 7. WORKERS' COMPENSATION AND GENERAL LIABILITY INSURANCE, AND INDEMNIFICATION.....	11
SECTION 8. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY.....	12
SECTION 9. DATA SECURITY.....	14
SECTION 10. GRATUITIES AND LOBBYING.....	17
SECTION 11. CONTRACT MONITORING.....	17
SECTION 12. CONTRACT AUDITS.....	19
SECTION 13. BACKGROUND SCREENING AND SECURITY.....	19
SECTION 14. COMMUNICATIONS AND CONFIDENTIALITY.....	21
SECTION 15. LICENSING .....	22
SECTION 16. PERFORMANCE BOND.....	23
SECTION 17. CUSTOMER OF RECORD.....	23
SECTION 18. SPECIFIC APPROPRIATION.....	24
SECTION 19. MISCELLANEOUS.....	24

## Exhibits:

Exhibit A – Definitions and Acronyms

Exhibit B – Final Statement of Work, including:

Exhibit 1 to Exhibit B – Final Service Level Agreements;

Exhibit C – Contractor's Pricing, including:

Exhibit 1 to Exhibit C – Vendor's Services and Discounts Pricing

Exhibit 2 to Exhibit C – Vendor's Device List

Exhibit 3 to Exhibit C – Vendor's Services and Discounts Pricing, Public Safety <if applicable>

Exhibit D – Instructional Document for Request for Best and Final Offer to ITN DMS-19/20-006

Exhibit E – Relevant Portions of the Contractor's Best and Final Offer to ITN DMS-19/20-006

Exhibit F – ITN DMS-19/20-006

## CONTRACT

This Contract is between the STATE OF FLORIDA, DEPARTMENT OF MANAGEMENT SERVICES (Department), an agency of the State of Florida with offices at 4050 Esplanade Way, Tallahassee, Florida 32399-0950, and <INSERT VENDOR NAME> (Contractor) with offices at <insert address>, each a "Party" and collectively referred to herein as the "Parties."

The Parties enter into this Contract (Contract) in accordance with Chapters 282 and 287, Florida Statutes (F.S.), and with the negotiated terms and conditions of Invitation to Negotiate, DMS-19/20-006, Mobile Communication Services.

### SECTION 1. CONTRACT TERM AND TERMINATION

#### 1.1 Initial Term

The initial term of the Contract will be five (5) years and will begin on the date the Contract is signed by all Parties.

#### 1.2 Renewal

Upon written agreement, the Department and the Contractor may renew the Contract, in whole or in part, for up to five (5) renewal years in accordance with section 287.057(13), F.S., and Rule 60A-1.048, Florida Administrative Code (F.A.C.).

#### 1.3 Suspension of Work and Termination

##### 1.3.1 Suspension of Work

The Department may, at its sole discretion, suspend any or all activities under the Contract, at any time, when it is in the best interest of the State of Florida to do so. The Department may, at its sole discretion, suspend the Contract at any time, when in the best interest of the Department or Customer to do so. The Department or the Customer will provide the Contractor written notice outlining the particulars of suspension and the effective date of the suspension. After receiving a suspension notice, the Contractor must comply with the notice and will cease the specified activities associated with the Contract. Within ninety (90) days, or any longer period agreed to by the Contractor, the Department will either (1) issue a notice authorizing resumption of work, at which time activity will resume, or (2) terminate the Contract. Suspension of work will not entitle the Contractor to any additional compensation.

##### 1.3.2 Termination for Convenience

The Contract may be terminated by the Department in whole or in part at any time, when, at the sole discretion of the Department, it is deemed to be in the best interest of the State of Florida to do so. If the Contract is terminated before performance is completed, the Contractor will be paid only for that work satisfactorily performed, prior to the termination, for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Contract price as the amount of work satisfactorily performed. All work in progress will become the property of the Customer and will be turned over promptly by the Contractor.

##### 1.3.3 Termination for Cause

If the performance of the Contractor is not in compliance with the Contract requirements the Department may, at its sole discretion, (a) immediately terminate the Contract, (b) notify the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Contract will terminate at the end of such time, or (c) take other action deemed appropriate by the Department.

#### **1.3.4 Termination Assistance**

In case of termination, whether for cause or for convenience, the Contractor will provide prompt and thorough transition assistance and cooperation, including as specified in Subsection 3.24, Transition for Future Iterations of this Service, of the Statement of Work (SOW).

## **SECTION 2. CONTRACT DOCUMENTS AND HIERACHY**

The Contract including any exhibits referred to herein, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral, with respect to such subject matter. The Contract consists of the documents listed below, and in the event any of these documents conflict, the conflict will be resolved in the following order of priority (highest to lowest):

1. This Final Contract document;
2. Attachment A – Definitions and Acronyms;
3. Attachment B – Final Statement of Work, including:
  - a. Exhibit 1 – Final Service Level Agreements;
4. Attachment C – Contractor's Pricing, including:
  - a. Exhibit 1 – Vendor's Services and Discounts Pricing
  - b. Exhibit 2 – Vendor's Device List
  - c. Exhibit 3 – Vendor's Services and Discounts Pricing, Public Safety <if applicable>
5. Attachment D – Instructional Document for Request for Best and Final Offer to ITN DMS-19/20-006;
6. Attachment E – Relevant Portions of the Contractor's Best and Final Offer to ITN DMS-19/20-006; and
7. Attachment F – ITN DMS-19/20-006.

In accordance with Rule 60A-1.002(7), F.A.C., Form PUR 1000, is included herein by reference but is superseded in its entirety by the Contract.

## **SECTION 3. PAYMENT AND FEES**

### **3.1 Price Adjustments**

Pricing may be updated in accordance with SOW Section 1.5, Update Process to End User Price Lists and Vendor's Equipment List.

### **3.2 Price Decreases**

During the term of the Contract (including renewal years), the Department encourages the Contractor to offer price decreases that are in line with increased efficiencies and added infrastructure enhancements. The Department reserves the right to further negotiate reduction in pricing for the renewal years. The following additional price decrease terms apply:

**3.2.1 Volume Discounts**

Contractor may offer additional discounts for one-time delivery of large single orders.

**3.2.2 Preferred Pricing**

The pricing included in the Contract is guaranteed, by the Contractor, to be a maximum price. Additionally, Contractor's pricing will not exceed the pricing offered under comparable contracts. Comparable contracts are those that are similar in size, scope and terms. In compliance with section 216.0113, F.S., Contractor must annually submit an affidavit from the Contractor's authorized representative attesting that the Contract complies with this clause.

**3.2.3 Sales Promotions**

In addition to decreasing prices for the balance of the Contract term due to a change in market conditions, Contractor may conduct sales promotions involving price reductions for a specified lesser period. Contractor must submit documentation identifying the proposed (1) starting and ending dates of the promotion, (2) commodities or contractual services involved, and (3) promotional prices compared to then-authorized prices.

**3.3 Purchase Orders and Communication Service Authorizations**

A Customer may use Purchase Orders (POs) issued through MyFloridaMarketPlace (MFMP) or Purchase Orders issued through the Communications Services Authorization and Billing (CSAB) system (known as Communication Service Authorizations (CSAs) to buy commodities or services. The Department may also issue POs or CSAs on behalf of Customers. The Contractor must provide commodities or services pursuant to POs or CSAs. The PO or CSA period of performance survives the expiration of the Contract. All terms and conditions of the Contract will be incorporated into the PO or CSA and will survive the termination of the Contract. The duration of POs or CSAs must not exceed the expiration of the Contract by more than twelve (12) months, unless they have been entered into pursuant to an Extended Pricing Plan, in which case they may not exceed the expiration of the Contract by more than thirty-six (36) months. Extended Pricing Plans are discounted prices offered in exchange for a Customer's commitment to lease commodities or purchase contractual services for an extended time.

**3.4 Payment Invoicing**

Payment will be made in accordance with section 215.422, F.S. The Contractor will be paid upon submittal of an invoice to the Department, or Customer if direct billed, after delivery and acceptance of commodities or contractual services is confirmed and the invoice is accepted by the Customer. The Contractor shall submit invoices for fees or other compensation for services or expenses in sufficient detail for a proper pre-audit and post-audit, and invoices must include the Contract number and the Contractor's Federal Employer Identification Number. The Department reserves the right to request additional documentation as needed, and Contractor will follow all invoice directives in the SOW and this Contract document.

The Contractor shall have a "No Shut Off" policy for all State agency Customer accounts. Contractor shall identify/flag all State agency Customer accounts as "Government Accounts" for which service will not be interrupted due to an outstanding balance, disputed amount owed, or late payments due.

**3.5 Travel**

Travel expenses are not reimbursable unless specifically authorized by the Customer in writing and, if authorized, may be reimbursed only in accordance with section 112.061, F.S.

**3.6 Annual Appropriation**

Pursuant to section 287.0582, F.S., the Department's performance and obligation to pay under the Contract is contingent upon an annual appropriation by the Legislature.

**3.7 MyFloridaMarketPlace Transaction Fee**

The State of Florida, through the Department, has instituted MFMP, a statewide eProcurement system. Pursuant to section 287.057(22), F.S., all payments issued by Customers to the Contractor for purchases of commodities or contractual services will be assessed a Transaction Fee as prescribed by Rule 60A-1.031, F.A.C., or as may otherwise be established by law, which the Contractor shall pay to the State.

For payments within the State of Florida accounting system (FLAIR or its successor), the Transaction Fee shall, when possible, be automatically deducted from payments to the Contractor. If automatic deduction is not possible, the Contractor shall pay the Transaction Fee pursuant to subsection (2) of Rule 60A-1.031, F.A.C. By submission of these reports and corresponding payments, the Contractor certifies their correctness. All such reports and payments shall be subject to audit by the State of Florida or its designee.

The Contractor shall receive a credit for any Transaction Fee paid by the Contractor for the purchase of any item(s) if such item(s) are returned to the Contractor through no fault, act, or omission of the Contractor. Notwithstanding the foregoing, a Transaction Fee is non-refundable when an item is rejected or returned, or declined, due to the Contractor's failure to perform or comply with specifications or requirements of the agreement.

Failure to comply with these requirements shall constitute grounds for declaring the Contractor in breach. VENDORS DELINQUENT IN PAYING TRANSACTION FEES SHALL BE EXCLUDED FROM CONDUCTING FUTURE BUSINESS WITH THE STATE.

**3.8 Taxes**

Taxes, customs, and tariffs on commodities or contractual services purchased under the Contract will not be assessed against the Customer unless authorized by Florida law.

**3.9 Return of Funds**

Contractor will return any overpayments due to unearned funds or funds disallowed pursuant to the terms of the Contract that were disbursed to the Contractor by the Department or Customer. The Contractor must return any overpayment within forty (40) calendar days after either discovery by the Contractor, its independent auditor, or notification by the Department or Customer of the overpayment.

**SECTION 4. CONTRACT ADMINISTRATION**

**4.1 Department's Contract Administrator**

The Department's Contract Administrator, whose primary responsibility will be to maintain the Contract file, is as follows:

Jane Doe  
<Insert division>  
<Insert agency>  
<Insert physical address>  
Telephone: (XXX) XXX-XXXX  
Email: jane.doe@xxxxx.com

In the event that the Department changes the Department's Contract Administrator, the Department will notify the Contractor's Contract Manager in writing via email and document such in the Contract file. Such changes do not require a formal written amendment to the Contract.

#### **4.2 Department's Contract Manager**

The Department's Contract Manager, who is primarily responsible for enforcing the performance of the Contract terms and conditions and will serve as a liaison with the Contractor, will be as follows:

Jane Doe  
<Insert division>  
<Insert agency>  
<Insert physical address>  
Telephone: (XXX) XXX-XXXX  
Email: jane.doe@xxxxx.com

In the event that the Department changes the Department's Contract Manager, the Department will notify the Contractor in writing via email. Such changes do not require a formal written amendment to the Contract.

#### **4.3 Department's Product Manager**

The Department's Product Manager, who is primarily responsible for monitoring the performance of the Contract terms and conditions and will serve as a liaison with the Contractor, will be as follows:

Jane Doe  
<Insert division>  
<Insert agency>  
<Insert physical address>  
Telephone: (XXX) XXX-XXXX  
Email: jane.doe@xxxxx.com

In the event that the Department changes the Department's Product Manager, the Department will notify the Contractor in writing via email. Such changes do not require a formal written amendment to the Contract.

#### **4.4 Contractor's Contract Manager**

The Contractor's Contract Manager, who is primarily responsible for the Contractor's oversight of the Contract performance, will be as follows:

Jane Doe  
<Insert Contractor name>  
<Insert Contractor's physical address>

Telephone: (XXX) XXX-XXXX  
Email: jane.doe@xxxxx.com

In the event that the Contractor changes its Contract Manager, the Contractor will notify the Department's Contract Manager in writing via email. Such a change does not require a formal written amendment to the Contract.

#### 4.5 Contractor's Account Manager

The Contractor's Account Manager, who will serve as a liaison with the Department's Contract Administrator, will be as follows:

Jane Doe  
<Insert Contractor name>  
<Insert Contractor physical address>  
Telephone: (XXX) XXX-XXXX  
Email: jane.doe@xxxxxx.com

In the event that the Contractor changes its Account Manager, the Contractor will notify the Department's Contract Manager in writing via email. Such changes do not require a formal written amendment to the Contract.

### SECTION 5. CONTRACT MANAGEMENT

#### 5.1 Notices

All notices required under the Contract must be delivered to the designated Contract Manager by certified mail, return receipt requested, reputable air courier service, email, or personal delivery, or as otherwise identified herein or by the Department.

#### 5.2 Change Request

The Department's Contract Manager may authorize operational changes to services and infrastructure that do not have a pricing impact (non-billable changes) via a change request. Such authorized operational changes do not require a Contract amendment but will be memorialized in writing and placed in the Contract Managers' files. The Department reserves the right to make the final determination if a change request or Contract amendment is required. Any change that would allow the Contractor to offer less of any deliverable, including commodities, services, technology, or software, requires a Contract amendment. Vendor's Equipment List and End User Price List updates must be made in accordance with SOW Section 1.5, End User Price Lists (EUPLs) and Vendor's Device List, and may not require an amendment or change request.

#### 5.3 Diversity Reporting

The State of Florida supports its diverse business community by creating opportunities for woman-, veteran-, and minority-owned small business enterprises to participate in procurements and contracts. The Department encourages supplier diversity through certification of woman-, veteran-, and minority-owned small business enterprises and provides advocacy, outreach, and networking through regional business events. For additional information, please contact the Office of Supplier Diversity (OSD) at [osdinfo@dms.myflorida.com](mailto:osdinfo@dms.myflorida.com).

Upon request, the Contractor will report to the Department its spend with business enterprises certified by the OSD. These reports must include the time period covered, the

name and Federal Employer Identification Number of each business enterprise utilized during the period, commodities and contractual services provided by the business enterprise, and the amount paid to the business enterprise on behalf of each Customer purchasing under the Contract.

**5.4 Designated Centralized Nonprofit Agency**

Subject to the agency determination provided for in section 413.036, F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INSOFAR AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated centralized nonprofit agency and the commodities or contractual services it offers is available at [https://www.dms.myflorida.com/business\\_operations/state\\_purchasing/state\\_contracts\\_and\\_agreements/\(contractType\)/4577](https://www.dms.myflorida.com/business_operations/state_purchasing/state_contracts_and_agreements/(contractType)/4577).

**5.5 PRIDE**

Subject to the agency determination provided for in sections 946.515 and 287.042(1), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INSOFAR AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the commodities or contractual services it offers is available at <http://www.pride-enterprises.org>.

**SECTION 6. COMPLIANCE WITH LAWS**

**6.1 Conduct of Business**

The Contractor must comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, State, and local agencies having jurisdiction and authority. These may include, but are not limited to, Chapters 282 and 287, F.S., Subtitle 60FF, F.A.C., the Communications Assistance for Law Enforcement Act, the Payment Card Industry DSS, IRS Publication

1045, Section 274A of the Immigration and Nationality Act, the Americans with Disabilities Act, Health Insurance Portability and Accountability Act (HIPAA) (including executing any Business Associate Agreements as requested by Customers), and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status. The Contractor must comply with and must assist the Department and Customers with compliance with Subtitle 60FF, F.A.C., (and Subtitle 60GG, F.A.C., if applicable).

## **6.2 Dispute Resolution, Governing Law, and Venue**

Any dispute concerning performance of the Contract shall be decided by the Department's Contract Manager, who will reduce the decision to writing and serve a copy on the Contractor. The decision of the Department's Contract Manager shall be final and conclusive. Exhaustion of this administrative remedy is an absolute condition precedent to the Contractor's ability to pursue legal action related to the Contract or any other form of dispute resolution. The laws of the State of Florida govern the Contract. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Contract. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county chosen by the Department.

## **6.3 Department of State, Registration**

Consistent with Chapters 605 through 623, F.S., the Contractor must provide the Department with conclusive evidence of a certificate of status, not subject to qualification, if a Florida business entity, or of a certificate of authorization if a foreign business entity.

## **6.4 Suspended, Convicted, and Discriminatory Vendor Lists**

In accordance with sections 287.042, 287.133, and 287.134, F.S., an entity or affiliate who is on the Suspended Vendor List, Convicted Vendor List, or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Contract. The Contractor must notify the Department if it or any of its suppliers, subcontractors, or consultants have been placed on the Suspended Vendor List, Convicted Vendor List, or the Discriminatory Vendor List during the term of the Contract.

## **6.5 Scrutinized Companies—Termination by the Department**

The Department may, at its option, terminate the Contract if the Contractor is found to have submitted a false certification as provided under section 287.135(5), F.S., or been placed on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or been engaged in business operations in Cuba or Syria, or to have been placed on the Scrutinized Companies that Boycott Israel List or is engaged in a boycott of Israel. Notwithstanding the foregoing, the Parties are aware of the Eleventh Circuit Court's decision in *Odbrecht Constr. v. Sec'y*, Fla. DOT, 715 F.3d 1268 (11<sup>th</sup> Cir. Fla. 2013), and agree that the provisions of sections 287.135(1)-(5), F.S., pertaining to a company engaged in business operations in Cuba or Syria shall not apply to this Contract unless and until the Eleventh Circuit Court's decision in *Odbrecht Constr. v. Sec'y*, Fla. DOT, 715 F.3d 1268 (11<sup>th</sup> Cir. Fla. 2013) is overturned.

## **6.6 Cooperation with Inspector General**

Pursuant to section 20.055(5), F.S., Contractor, and its subcontractors, if any, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor must provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but will not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Contract. The Contractor agrees to reimburse the State of Florida for the reasonable costs of investigation incurred by the Inspector General or other authorized State of Florida official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State of Florida which results in the suspension or debarment of the Contractor. Such costs include, but will not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

## **6.7 E-Verify**

The Contractor (and its subcontractors) have an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees. By executing this Contract, the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees. The Contractor must obtain an affidavit from its subcontractors in accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of the Contract. In order to implement this provision, the Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the Contract Manager within five (5) days of Contract execution.

This section serves as notice to the Contractor regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and the Department's obligation to terminate the Contract if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. If terminated for such reason, the Contractor will not be eligible for award of a public contract for at least one (1) year after the date of such termination. The Department reserves the right to order the immediate termination of any contract between the Contractor and a subcontractor performing work on its behalf should the Department develop a good faith belief that the subcontractor has knowingly violated section 448.095(1), F.S.

## **SECTION 7. WORKERS' COMPENSATION AND GENERAL LIABILITY INSURANCE, AND INDEMNIFICATION**

### **7.1 Workers' Compensation Insurance**

The Contractor shall maintain Workers' Compensation insurance as required under the Florida Workers' Compensation Law or the workers' compensation law of another jurisdiction, where applicable. The Contractor must require all subcontractors to similarly provide Workers' Compensation Insurance for all of the latter's employees. In the event work is being performed by the Contractor under the Contract and any class of employees performing the work is not protected under Worker's Compensation statutes, the Contractor must provide, and cause each subcontractor to provide, adequate insurance, satisfactory to the Department, for the protection of employees not otherwise protected.

## **7.2 General Liability Insurance**

The Contractor shall maintain insurance sufficient to adequately protect the Department and Customers from all claims or liability for personal injury or property damage arising out of, resulting from the performance of, or in connection with the operation of, the Contract. All insurance shall be with insurers authorized to transact the applicable line of insurance business in the State of Florida. The Contractor shall provide the Department with Certification(s) of Insurance evidencing that all appropriate coverage is in place and showing the Department to be an additional insured within thirty (30) days after Contract execution and on the Contract anniversary date each year of the Contract.

The Contractor must submit via email, to the Department's Contract Manager, notice of any cancellation or nonrenewal at least ten (10) calendar days prior to cancellation or nonrenewal. In the event of cancellation or nonrenewal, the Contractor will be responsible for securing a replacement insurance policy in accordance with this section within thirty (30) Business Days after the final date of the cancelled or nonrenewed policy.

## **7.3 Indemnification**

The Contractor agrees to indemnify, defend, and hold the Department, Customers, and the State of Florida, its officers, employees, and agents harmless from all fines, claims, assessments, suits, judgments, or damages, including consequential, special, indirect, and punitive damages, including court costs and attorney's fees, arising from or relating to violation or infringement of a trademark, copyright, patent, trade secret or intellectual property right or out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Contract, as well as for any determination arising out of or related to the Contract that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Department. The Contract does not constitute a waiver of sovereign immunity or consent by the Department or the State of Florida or its subdivisions to suit by third parties.

Without limiting this indemnification, the Department or Customer may provide the Contractor (1) written notice of any action or threatened action, (2) the opportunity to take over and settle or defend any such action at Contractor's sole expense, and (3) assistance in defending the action at Contractor's sole expense.

## **SECTION 8. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY**

### **8.1 Public Records**

Solely for the purpose of this section, the Department's Contract Manager is the agency custodian of public records. If, under this Contract, the Contractor is providing services and is acting on behalf of the Department, as provided in section 119.0701, F.S., the Contractor shall:

1. Keep and maintain public records required by the Department to perform the service.
2. Upon request from the Department's custodian of public records, provide the Department with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.

3. Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the Contract term and following the completion of the Contract if the Contractor does not transfer the records to the Department.
4. Upon completion of the Contract, transfer, at no cost, to the Department all public records in possession of the Contractor or keep and maintain public records required by the Department to perform the service. If the Contractor transfers all public records to the Department upon completion of the Contract, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the Contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department.

**IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT THE TELEPHONE NUMBER, EMAIL ADDRESS AND MAILING ADDRESS PROVIDED FOR THE CONTRACT MANAGER.**

#### **8.2 Protection of Trade Secrets or Confidential Information**

If the Contractor considers any portion of materials made or received in the course of performing the Contract ("contract-related materials") to be trade secret under section 688.002 or 812.081, F.S., or any other applicable law, or otherwise confidential under Florida or federal law, the Contractor must clearly designate that portion of the materials as trade secret or otherwise confidential when submitted to the Department. The Contractor will be responsible for responding to and resolving all claims for access to contract-related materials it has designated trade secret or otherwise confidential.

If the Department is served with a request for discovery of contract-related materials designated by the Contractor as trade secret or otherwise confidential, the Contractor will be responsible for filing the appropriate motion or objection in response to the request for discovery. The Department will provide materials designated trade secret or otherwise confidential if the Contractor fails to take appropriate and timely action to protect the materials designated as trade secret or otherwise confidential.

The Contractor will protect, defend, indemnify, and hold harmless the Department for claims, costs, fines, and attorney's fees arising from or relating to its designation of contract-related materials as trade secret or otherwise confidential.

#### **8.3 Document Management and Record Retention**

The Contractor must retain sufficient documentation to substantiate claims for payment under the Contract and all other records, electronic files, papers, and documents that were

made in relation to the Contract, including those required by Section 6.6, Cooperation with Inspector General. Contractor must retain all documents related to the Contract for five (5) years after expiration of the Contract, or, if longer, the period required by the General Records Schedules maintained by the Florida Department of State available at:<http://dos.myflorida.com/library-archives/records-management/general-records-schedules/>.

#### **8.4 Intellectual Property**

Unless specifically addressed in the Contract, intellectual property rights to all property created or otherwise developed by the Contractor for the Department or the Customer will be owned by the State of Florida at the completion of the Contract.

Any inventions or discoveries developed in the course of or as a result of services performed under the Contract which are patentable pursuant to 35 U.S.C. § 101 are the sole property of the State of Florida. Contractor must inform the Customer of any inventions or discoveries developed or made in connection with the Contract and will be referred to the Florida Department of State for a determination on whether patent protection will be sought for the invention or discovery. The State of Florida will be the sole owner of any and all patents resulting from any invention or discovery made in connection with the Contract.

Contractor must notify the Department or State of Florida of any publications, artwork, or other copyrightable works developed in connection with the Contract. All copyrights created or developed in connection with the Contract are the sole property of the State of Florida.

### **SECTION 9. DATA SECURITY REQUIREMENTS**

#### **9.1 Duty to Secure State Data**

The Contractor will maintain the security of State Data, including, but not limited to, keeping a secure area around any displayed or otherwise visible State Data and ensuring such data is stored and secured when not in use. The Contractor will be responsible for ensuring that all Persons it contracts with to maintain, store, or process State Data on its behalf will comply with all data security requirements of this section. The Contractor will also comply with any other State or federal rules and regulations regarding security of information. The State will remain the owner of all State Data and any other data made available by the State to the Contractor pursuant to this Contract.

Unless otherwise agreed in writing, the Contractor and its subcontractors will not perform any of the services under this Contract from outside of the United States. The Contractor will not allow, through its action or inaction, any State Data to be sent by any medium, transmitted, or to be Accessed outside of the United States.

The Contractor shall comply with section 501.171, F.S. Additionally, the Contractor shall reimburse the Department for any costs incurred providing the notifications required by subsections 501.171(3) and (4), F.S., if the Contractor is responsible for a breach. For purposes of this paragraph, "breach," is as defined in section 501.171(1)(a), F.S.

## 9.2 State Data Access

The Contractor shall retain a list of all Persons, as defined in Attachment E – Definitions and Acronyms, with Access to State Data, including a statement confirming that each Person has passed the background screening required herein. This statement shall not include the substance of the screening results, only that the Person has passed the screening.

The Contractor shall create a written policy for the protection of State Data, including a policy and procedure for Access to State Data. The Contractor shall retain the policy and information required in this subsection in accordance with Section 8.3, Document Management and Record Retention. The documents are subject to disclosure within thirty-six hours upon written or oral demand by the Department or its designated agents or auditors and are subject to audit and screening.

The Contractor shall document and record, with respect to each instance of Access to State Data:

1. The identity of all individual(s) who Accessed State Data in any way, whether those individuals are authorized Persons or not;
2. The duration of the individual(s)' Access, including the time and date at which the Access began and ended;
3. The identity, form, and extent of State Data Accessed, including, but not limited to, whether the individual Accessed partial or redacted versions of State Data, read-only versions of State Data, or editable versions of State Data; and
4. The nature of the Access, including whether the State Data was edited or shared with any other individual or entity during the duration of the Access, and, if so, the identity of the individual or entity.

The damages that would result from the Contractor's failure to compile, retain, and disclose the written policy and information required in this subsection are by their nature impossible to ascertain presently and will be difficult to ascertain in the future. The issues involved in determining such damages will be numerous, complex, and unreasonably burdensome to prove. The Contractor therefore agrees to credit the Department the sum of \$10,000 for each breach of this subsection. The parties acknowledge that these credits are liquidated damages, exclusive of any other right to damages, not intended to be a penalty, and solely intended to compensate for unknown and unascertainable damages.

## 9.3 Violations of Data Security Requirements

A "Security Breach" in this Section 9 means an unauthorized Access of State Data. Good faith Access of State Data by a Person, as defined in Attachment E – Definitions and Acronyms, does not constitute a security breach, provided that the information is not used for a purpose unrelated to the furtherance of the Contract or subject to further unauthorized Access. However, unauthorized Access includes incidents where Persons with authorized Access for certain purposes otherwise gain Access for unauthorized purposes.

The Contractor agrees that a Security Breach, including any violations of Section 9.1, Duty to Secure State Data, will entitle the State to a credit commensurate with the Department and Customer's internal staffing and administrative costs associated with managing the Security Breach or violation of Section 9.1, Duty to Secure State Data, as determined by the Department. Such credits will not preclude the State from recovering other damages

it may suffer as a result of the Security Breach or violation of Section 9.1, Duty to Secure State Data.

#### **9.4 Notification Requirements**

In the event of a Security Breach, including any violations of Section 9.1, Duty to Secure State Data, or a credible allegation or suspicion of a Security Breach or violation of Section 9.1, Duty to Secure State Data (as determined by the Contractor or the Department), the Contractor must notify the Department's Contract Manager and the affected Customer as expeditiously as practicable, but in all instances no later than one (1) calendar day of knowledge of the Security Breach or credible allegation or suspicion of such.

Notification is required regardless of the number of persons or type of State Data affected or potentially affected. The notification must be clear and conspicuous and include a description of the following:

1. The incident in general terms;
2. The type of information that was subject to the violations of Section 9.1, Duty to Secure State Data, or credible allegation or suspicion of Security Breach;
3. The type and number of entities and individuals who were, or potentially have been, affected by the incident; and
4. The actions taken by the Contractor to protect the State Data from further unauthorized Access. However, the description of those actions in the notice may be general so as not to further increase the risk or severity of the Security Breach.

The Contractor must also as expeditiously as practicable, but no later than thirty-six hours from the time of discovery, set up a conference call with the Department's Contract Manager. The conference call invitation must contain a brief description of the nature of the event. When possible, a thirty (30) minute notice will be given to allow Department personnel to be available for the call. If the designated time is not practical for the Department, an alternate time for the call will be scheduled. All available information about the Security Breach or suspected Security Breach must be shared on the call. The Contractor must answer all questions based on the information known at that time and answer additional questions as additional information becomes known. The Contractor must provide the Department with final documentation of the incident including all remedial actions of the Contractor.

#### **9.5 Other Indemnifications and Credit Monitoring**

The Contractor shall be fully liable for the actions of all Persons, as defined in Attachment E – Definitions and Acronyms, and shall fully defend, indemnify, and hold harmless the Department, Customers, the State of Florida, its officers, directors and employees from any claims, suits, actions, damages, proceedings, and costs of every name and description, including attorney's fees, to the extent arising or resulting from a violation by the Contractor or a Person, as defined in Attachment E – Definitions and Acronyms, of Section 9, Data Security, and Section 13, Background Screening and Security, resulting in the Security Breach of State Data. The Contractor shall provide credit monitoring services at its own cost for those individuals affected or potentially affected by a Security Breach of these sections by the Contractor or a Person, as defined in Attachment E – Definitions and Acronyms, for a twelve-month period of time following the Security Breach.

## **SECTION 10. GRATUITIES AND LOBBYING**

### **10.1 Gratuities**

The Contractor will not, in connection with the Contract, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State of Florida officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State of Florida officer or employee.

### **10.2 Lobbying**

Funds provided under this Contract shall not be used to violate the provisions of sections 11.062 and 216.347, F.S. Pursuant to section 287.058(6), F.S., the Contract does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Contract after Contract execution and during the Contract's term.

## **SECTION 11. CONTRACT MONITORING**

### **11.1 Performance Standards**

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Contract. The Department and the Customer will be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof. Coordination must be maintained by the Contractor with representatives of the Customer, the Department, or of other agencies involved in the Contract on behalf of the Department.

### **11.2 Performance Deficiencies and Service Level Agreements**

Service Level Agreements (SLAs) dictate the levels of service delivery for individual services. The parties acknowledge that these SLAs contain financial consequences, as required by section 287.058, F.S., are exclusive of any other right to damages, and are not intended to be a penalty. The Contractor therefore agrees to credit the Department consistently with the Contract, including as set forth in Attachment C - Service Level Agreements. Financial consequences that are due to a Customer after the completion of service, or exceed any payment due to the Contractor, shall be submitted by check rather than as a credit.

One, multiple, or recurring violations of a SLA may be considered a breach of the Contract and may result in a suspension or cancellation of PO(s) or CSA(s). The Department reserves the right to determine when violation(s) of SLAs constitute a breach of the Contract or will result in a suspension or cancellation of PO(s) or CSA(s). The Department's determination of a breach of the Contract or suspension or cancellation of PO(s) or CSA(s) will depend on the number and severity of the SLA violation(s), disruption to service, Contractor's response, and other factors.

In addition to the processes set forth in the Contract (e.g., SLAs), if the Department determines that there is a performance deficiency that requires correction by the Contractor, then the Department will notify the Contractor. The correction must be made within a timeframe specified by the Department. The Contractor must provide the Department with a corrective action plan describing how the Contractor will address all performance deficiencies identified by the Department.

If the corrective action plan is unacceptable to the Department, or implementation of the plan fails to remedy the performance deficiencies, the Department will retain ten percent (10%) of the total invoice amount and may suspend or cancel PO(s) or CSA(s) or may suspend work or terminate the Contract as set forth in Section 1.3, Suspension of Work and Termination. The retainage will be withheld until the Contractor resolves the performance deficiencies. If the performance deficiencies are resolved, the Contractor may invoice the Department for the retained amount. If the Contractor fails to resolve the performance deficiencies, the retained amount will be forfeited in order to compensate the Department for the performance deficiencies and the Department may suspend or cancel PO(s) or CSA(s) or may terminate the Contract as set forth in Section 1.3, Suspension of Work and Termination.

### **11.3 Timely Performance**

The Contractor will promptly notify the Department or Customer upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion (or delivery) of any commodity or contractual service. The Contractor will use commercially reasonable efforts to avoid or minimize any delays in performance and will inform the Department or Customer of the steps the Contractor is taking or will take to do so and the projected actual completion (or delivery) time. If the Contractor believes a delay in performance by the Department or Customer has caused or will cause the Contractor to be unable to perform its obligations on time, the Contractor will promptly so notify the Department or Customer and use commercially reasonable efforts to perform its obligations on time notwithstanding the Department or Customer's delay.

### **11.4 Force Majeure, Notice of Delay, and No Damages for Delay**

The Contractor will not be responsible for delay resulting from its failure to perform if neither the fault nor the negligence of the Contractor or its employees or agents contributed to the delay and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the Contractor's control, or for any of the foregoing that affect subcontractors or suppliers if no alternate source of supply is available to the Contractor. In case of any delay the Contractor believes is excusable, the Contractor will notify the Department or Customer in writing of the delay or potential delay and describe the cause of the delay either (1) within ten (10) days after the cause that creates or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result, or (2) if delay is not reasonably foreseeable, within five (5) days after the date the Contractor first had reason to believe that a delay could result. The foregoing will constitute the Contractor's sole remedy or excuse with respect to delay. Providing notice in strict accordance with this paragraph is a condition precedent to such remedy. No claim for damages will be asserted by the Contractor. The Contractor will not be entitled to an increase in the Contract price or payment of any kind from the Department or Customer for direct, indirect, consequential, impact or other costs, expenses or damages, including but not limited to costs of acceleration or inefficiency, arising because of delay, disruption, interference, or hindrance from any cause whatsoever. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this paragraph, after the causes have ceased to exist the Contractor will perform at no increased cost, unless the Department or Customer determines, in its sole discretion, that the delay will significantly impair the value of the Contract to the State of Florida or to Customers, in which case the Department or Customer may (1) accept allocated performance or deliveries from the Contractor, provided that the Contractor grants preferential treatment to Customers with respect to

commodities or contractual services subjected to allocation, or (2) purchase from other sources (without recourse to and by the Contractor for the related costs and expenses) to replace all or part of the commodity or contractual services that are the subject of the delay, which purchases may be deducted from the Contract quantity, or (3) terminate the Contract in whole or in part.

## **SECTION 12. CONTRACT AUDITS**

### **12.1 Performance or Compliance Audits**

The Department may conduct, or cause to have conducted, either or both performance and compliance audits of the Contractor and subcontractors as determined by the Department. The Department may conduct an audit and review all the Contractor's and subcontractor's data and records that directly relate to the Contract. To the extent necessary to verify the Contractor's claims for payment under the Contract, the Contractor's agreements or contracts with subcontractors, partners or agents of the Contractor, pertaining to the Contract, may be inspected by the Department upon fifteen (15) days' notice, during normal working hours and in accordance with the Contractor's facility access procedures where facility access is required. Release statements from its subcontractors, partners or agents are not required for the Department or its designee to conduct compliance and performance audits on any of the Contractor's contracts relating to the Contract. The State of Florida's Chief Financial Officer and the Office of the Auditor General also have authority to perform audits and inspections.

### **12.2 Payment Audit**

Records of costs incurred under terms of the Contract will be maintained in accordance with Subsection 8.3, Document Management and Record Retention. Records of costs incurred will include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Department, State of Florida's Chief Financial Officer, or the Office of the Auditor General.

## **SECTION 13. BACKGROUND SCREENING AND SECURITY**

All Contractor employees, subcontractors and agents performing work under the Contract must comply with all security and other requirements of the Department or the Customer.

### **13.1 Background Screening**

In addition to any background screening required by the Contractor as a condition of employment, the Contractor warrants that it will conduct a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other person, hereinafter referred to as "Person" or "Persons," operating under its direction with Access to State Data or who enter either the premises or facilities where State Data is stored or accessible. Contractor is not required to conduct the aforementioned background screening of a Person if that Person does not have Access to State Data and if that Person, whenever on Customer premises or facilities, is escorted by Customer authorized personnel.

The Contractor warrants that all Persons will have passed the background screening described herein before they have Access to State Data or begin performing services

under the Contract. The look-back period for such background screenings shall be for a minimum of six (6) years where six (6) years of historical information is available.

The minimum background check process will include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard:

1. Social Security Number Trace; and
2. Criminal Records (Federal, State, and County criminal felony and misdemeanor, national criminal database for all states which make such information available).

The Contractor agrees that each Person will be screened as a condition prior to performing services or having Access to State Data. The Contractor is responsible for any and all costs and expenses in obtaining and maintaining the criminal background screening information for each Person described above. The Contractor will maintain documentation of the screening in the Person's employment file. The Contractor will abide by all applicable laws, rules, and regulations including, but not limited to, the Fair Credit Reporting Act and/ any equal opportunity laws, rules, regulations, or ordinances.

### **13.2 Disqualifying Offenses**

If at any time it is determined that a Person has a criminal misdemeanor or felony record, regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict), within the last six (6) years from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that Person from any position with Access to State Data or directly performing services under the Contract. The disqualifying offenses are as follows:

1. Computer related crimes
2. Information technology crimes;
3. Fraudulent practices;
4. False pretenses;
5. Fraud;
6. Credit card crimes;
7. Forgery;
8. Counterfeiting;
9. Violations involving checks or drafts;
10. Misuse of medical or personnel records; and
11. Felony theft.

If the Contractor finds a Disqualifying Offense for a Person within the last six (6) years from the date of the court's disposition, it may obtain information regarding the incident and determine whether that Person should continue providing services under the Contract or have Access to State Data. The Contractor will consider the following factors only in making the determination: i) nature and gravity of the offense, ii) the amount of time that lapsed since the offense, iii) the rehabilitation efforts of the Person, and iv) relevancy of the offense to the job duties of the Person. If the Contractor determines that the Person should be allowed Access to State Data, then Contractor shall maintain all criminal background screening information and the rationale for such Access in the Person's employment file. The Contractor will promptly notify the Department of any determinations

made pursuant to this subsection. The Department reserves the right to require removal of any Persons from performing work on the Contract for any reason.

#### **13.2.1 Refresh Screening**

The Contractor will ensure that all background screening will be refreshed every five (5) years from the time initially performed for each Person during the term of the Contract.

#### **13.2.2 Self-Disclosure**

The Contractor shall ensure that all Persons have a responsibility to self-report within three (3) calendar days to the Contractor any updated court disposition regarding any disqualifying offense, regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict). The Contractor shall immediately reassess whether to disallow that Person Access to any State of Florida premises or from directly performing services under the Contract. Additionally, the Contractor shall require that the Person complete an annual certification that they have not received any additional criminal misdemeanor or felony record regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) for the Disqualifying Offenses and shall maintain that certification in the employment file.

In addition, the Contractor shall ensure that all Persons have a responsibility to self-report to the Contractor within three (3) calendar days, any arrest for any Disqualifying Offense. The Contractor shall notify the Department's Contract Manager within twenty-four (24) hours of all details concerning any reported arrest.

#### **13.3 Department's Ability to Audit Screening Compliance and Inspect Locations**

The Department reserves the right to audit the Contractor's background screening process upon two (2) days prior written notice to the Contractor during the term of the Contract. The Department will have the right to inspect the Contractor's working area, computer systems, and/or location upon two (2) Business Days prior written notice to the Contractor to ensure that Access to State Data is secure and in compliance with the Contract and all applicable state and federal rules and regulations.

### **SECTION 14. COMMUNICATIONS AND CONFIDENTIALITY**

#### **14.1 Public Statements**

The Contractor shall not, without first notifying the Department's Contract Manager and securing the Department's prior written consent, make public statements or publicly disseminate any information which concern the Contract or its subject matter, including, but not limited to:

1. disclose or permit disclosure of any data or information obtained or furnished in accordance with the Contract,
2. use any statement attributable to the Department or its employees,
3. mentioning the Contract in a press release or other promotional material, or
4. otherwise linking Contractor's name and either a description of the Contract or the name of the State, the Department or any Customer in any material published, either in print or electronically, to any entity that is not a party to Contract, except potential or actual authorized distributors, dealers, resellers, or service representative.

Public statements include press releases, publicity releases, promotions, marketing materials, corporate communications, or other similar communications. If provided, the Department's written consent shall not be construed to supersede or waive the Contract requirements imposed on the Contractor to maintain confidential information.

The Contractor will not use the State of Florida seal, name, or logo of the Department or State of Florida, or Contractor's relationship to the Department for any purpose without the prior written consent of the Department.

The Contractor may refer to the Contract as an experience citation with other customers without prior approval.

The Contractor shall have the following obligations with respect to the marketing of this Contract to any Customers:

1. To use its commercially reasonable best efforts to further the promotion, advertising, and marketing of services available under this Contract; and
2. To promote the utilization of this Contract to Other Eligible Users in favor of any other cooperative purchasing contract for similar services.

#### **14.2 Confidential Information**

The Contractor must maintain confidentiality of all confidential data, files, and records related to the services and commodities provided pursuant to the Contract and must comply with all state and federal laws, including, but not limited to Chapter 119, F.S., and sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures must be consistent with the most recent version of the Department security policies, protocols, and procedures. The Contractor must also comply with any applicable professional standards with respect to confidentiality of information.

### **SECTION 15. LICENSING**

All services shall include all required licenses for Customers to utilize the services at no additional cost to the Customer. All third-party license costs for Contractor-provided hardware and software shall be the responsibility of the Contractor. The Contract will take precedence over any and all End User License Agreement conflicting terms. Any provisions in an End User License Agreement that require the Department to indemnify the Contractor are inapplicable.

Additional terms affixed to products or services prior to delivery (e.g., attachment or inclusion of standard preprinted forms, product literature, service agreements, end user agreements, "clickwrap" agreements, "shrink wrap", "browserwrap", or terms accompanying or affixed to a product or service, whether written or electronic) incorporated onto the Contractor's or subcontractor's order or fiscal forms or other documents forwarded by the Contractor for payment will not be binding on the Department or Customer unless negotiated and agreed to in writing as specified in this section. A Customer may agree to additional terms and conditions specific to the Customer's order that are jointly negotiated and explicitly agreed upon by the Customer. A Customer's acceptance of a product or service or processing of documentation on forms furnished by the Contractor for approval or payment shall not constitute an acceptance of the Contractor's or subcontractor's proposed modification to terms and conditions or an agreement to modify or

add additional terms to this Contract. Should a court determine any provision of the Contract is invalid, the remaining provisions will not be affected, and the rights and obligations of the Parties will be construed and enforced as if the Contract did not contain the provision held invalid.

## **SECTION 16. PERFORMANCE BOND**

Within thirty (30) days of Contract execution, Contractor will deliver to the Department's Contract Manager a performance bond in the amount of \$500,000 (five hundred thousand). This shall also apply to any renewal years. The bond shall name the Department as the beneficiary and will be used to guarantee satisfactory performance by the Contractor throughout the term of the Contract.

1. The performance bond shall be maintained throughout the term of the Contract. The performance bond must be issued by an acceptable surety company, as determined by the Department, and which surety must be licensed to do business in the State of Florida. The insurer or bonding company shall pay losses suffered by the State of Florida directly to the Department.
2. The Contractor and insurer or bonding company shall provide the Department prior written notice or immediate notice upon knowledge of any attempt to cancel or to make any other material change in the status, coverage, or scope of the performance bond, or of the Contractor's failure to pay bond premiums.
3. The Department shall not be responsible for any premiums or assessments on or in relation to the performance bond.
4. The performance bond is to protect the Department and the State against any loss sustained through failure of the Contractor's performance in accordance with the Contract. No payments shall be made to the Contractor until the performance bond is in place and approved by the Department in writing.
5. Within thirty (30) days of Contract execution, and by Contract execution anniversary each year following, the Contractor shall provide the Department with a surety bond continuation certificate or other acceptable verification that the performance bond is valid and has been renewed for an additional year.
6. The performance bond provided under this section shall be used solely to the extent necessary to satisfy the damage claims made by the State of Florida pursuant to the terms of the Contract. In no event shall the performance bond be construed as a penalty bond.
7. No sooner than two (2) years after Contract execution, if it is in the best interest of the State of Florida, as determined by the Department, the Contractor's performance bond may be reduced for the remainder of the term. This reduction shall require an amendment to the Contract with the agreement of both parties.

## **SECTION 17. CUSTOMER OF RECORD**

The Department is considered the Customer of Record for all services for the purposes of the Federal Communications Commission and Customer Proprietary Network Information.

## **SECTION 18. SPECIFIC APPROPRIATION**

The following is the specific State fund from which the State will make payment under the first year of the Contract:

General Appropriations Act (Florida Law)  
2909 SPECIAL CATEGORIES  
CENTREX AND SUNCOM PAYMENTS FROM COMMUNICATIONS WORKING  
CAPITAL TRUST FUND

## **SECTION 19. MISCELLANEOUS**

### **19.1 Warranty of Contractor's Ability to Perform**

The Contractor warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Contract obligations. The Contractor warrants that neither it nor any affiliate is currently on the Suspended Vendor List, Convicted Vendor List, Discriminatory Vendor List, or on any similar list maintained by any other state or the federal government.

The Contractor shall notify the Department of any regulatory or legal actions filed by any federal, state, or local government entity and any other litigation that could impact the Contractor's ability to perform under this Contract within thirty (30) days of the action being filed. The Contractor must notify the Department of any legal actions filed against it for a breach of a contract of similar size and scope to this Contract within thirty (30) days of the action being filed. Failure to notify the Department of a legal action within thirty (30) days of the action will be grounds for termination for cause of the Contract.

The Contractor shall immediately notify the Department in writing if its ability to perform is compromised in any manner during the term of the Contract.

### **19.2 Subcontractors, Affiliates, Partners, Teammates, Third-Party Vendors**

The Contractor is fully responsible for satisfactory completion of all subcontracted work, including work by affiliates, partners, teammates, and all other third-party vendors, in accordance with the terms and conditions of the Contract.

### **19.3 Assignment**

The Contractor will not sell, assign, or transfer any of its rights, duties or obligations under the Contract without the prior written consent of the Department. However, the Contractor may waive its right to receive payment and assign the same upon notice to the Department. In the event of any assignment, the Contractor remains responsible for performance of the Contract, unless such responsibility is expressly waived by the Department. The Department may assign the Contract with prior written notice to the Contractor.

### **19.4 Independent Contractor**

The Contractor is an independent contractor. The Contractor and its employees, agents, representatives, and subcontractors, affiliates, partners, teammates, and all other third-party vendors are not employees or agents of the Department and are not entitled to the benefits of State of Florida employees. The Department will not be bound by any acts or

conduct of the Contractor or its employees, agents, representatives, or subcontractors, affiliates, partners, teammates, and all other third-party vendors.

**19.5 Risk of Loss**

Matters of inspection and approval are addressed in section 215.422, F.S. Until acceptance, risk of loss or damage will remain with the Contractor. The Contractor will be responsible for filing, processing, and collecting all damage claims. To assist the Contractor with damage claims, the Customer will: record any evidence of visible damage on all copies of the delivering carrier's Bill of Lading; report damages to the carrier and the Contractor; and provide the Contractor with a copy of the carrier's Bill of Lading and damage inspection report. When a Customer or the Department rejects a commodity, Contractor will remove the commodity from the premises within ten (10) days after notification of rejection, and the risk of loss will remain with the Contractor.

Commodities not removed by the Contractor within ten (10) days will be deemed abandoned by the Contractor and the Customer or the Department will have the right to dispose of it as its own property. Contractor will reimburse the Customer or the Department for costs and expenses incurred in storing or effecting removal or disposition of rejected commodities.

**19.6 Safety Standards**

Performance of the Contract for all commodities or contractual services must comply with requirements of the Occupational Safety and Health Act and other applicable State of Florida and federal requirements.

**19.7 Ombudsman**

A Vendor Ombudsman has been established within the Department of Financial Services. The duties of this office are found in section 215.422, F.S., which include disseminating information relative to prompt payment and assisting contractors in receiving their payments in a timely manner from a Customer. The Vendor Ombudsman may be contacted at (850) 413-5516.

**19.8 Time is of the Essence**

Time is of the essence regarding each and every obligation of the Contractor. Each obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

**19.9 Waiver**

The delay or failure by the Department or Customer to exercise or enforce any rights under the Contract will not constitute waiver of such rights.

**19.10 Modification and Severability**

With the exception of the process described in Section 5.2, Change Requests, this Contract may only be modified by a written agreement signed by the Department and the Contractor.

Should a court determine any provision of the Contract is invalid, the remaining provisions will not be affected, and the rights and obligations of the Parties will be construed and enforced as if the Contract did not contain the provision held invalid.



4050 Esplanade Way  
Tallahassee, FL 32399-0950

Ron DeSantis, Governor  
Jonathan R. Satter, Secretary

### Attachment C Service Level Agreements (SLAs)

Service Category	SLA Number	Deliverable Title	Performance Metric	Financial Consequence	Additional SLA Clock Information
Contractor Staffing	SLA-A1	Staffing Positions	<p>a) Key staff positions will be filled within thirty (30) days from Contract execution, in accordance with SOW subsection 2.1</p> <p>b) 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, in accordance with SOW subsection 2.1</p> <p>c) DMS must receive a notification of a vacancy of a key staff position within fourteen (14) days of the vacancy, in accordance with SOW subsection 2.1</p>	<p>a) \$250 per day, per vacancy</p> <p>b) \$250 per day, per vacancy</p> <p>c) \$250 per day, per incident</p>	<p>a) Should DMS invoke the right to review and approve candidates for key staff positions, the SLA clock will be suspended during the DMS review.</p> <p>b) Should DMS invoke the right to review and approve candidates for key staff positions, the SLA clock will be suspended during the DMS review.</p> <p>c) N/A</p>
	SLA-A2	Final Staffing Organizational Chart	The final Staffing Organizational Chart shall be submitted to the Department no later than thirty (30) days from Contract execution, in accordance with SOW subsection 2.1	\$1,000 per day	

Services and Devices for Mobile Communication Services	SLA-B1	Network-to-Network Interconnection Failover	Failover successfully accomplished within 500 seconds, in accordance with SOW subsection 3.6	\$5,000 per connectivity issue incidence  \$5,000 per quarter hour if the failover is not successful and results in downtime of longer than 500 seconds	The SLA is measured by the Contractor's equipment or system logs.  The SLA clock starts when the logs indicate the loss of interconnectivity.  The SLA clock stops when the interconnection with MFN operates without any loss of performance compared to the interconnection performance prior to failover.
	SLA-B2	Network-to-Network Interconnection Performance Upgrade with MyFloridaNet	Required capacity upgrade must be completed within sixty (60) days, in accordance with SOW subsection 3.6	\$3,000 per day	The SLA clock starts when an upgrade is needed as shown and documented in the Contractor's monitoring tools.  The SLA clock is on hold during DMS verification of the upgrade.  The SLA clock stops when the required capacity upgrade has been accepted by DMS.

	SLA-B3	SLA Compliance Report	The report will be provided monthly, two (2) Business Days before the monthly operational meeting, in accordance with SOW subsection 3.18.5	\$1,000 per day	
	SLA-B4	Escalation Activity Report	The report will be provided monthly, two (2) Business Days before the monthly operational meeting, in accordance with SOW subsection 3.19.1	\$1,000 per day	
	SLA-B5	Zero Usage Report	The report will be provided quarterly and provided two (2) Business Days before the January, April, July, and October monthly operational meeting, in accordance with SOW subsection 3.19.2	\$1,000 per day	
	SLA-B6	Escalation Procedure Development and Updates	Developed within thirty (30) days of Contract execution, in accordance with SOW subsection 3.19.3 and section 4.  Updated within three (3) Business Days of email notification from DMS.	\$1,000 per day until developed or until updated	
	SLA-B7	Notification, Planned Maintenance	Notification received two (2) Business Days prior to any planned maintenance, in accordance with SOW subsection 3.20.4 and section 4	\$2,500 per failure to notify	The SLA is measured by the Contractor's logs and emails.  The SLA applies automatically two (2) Business Days prior to any planned maintenance for which notice is not provided.

	SLA-B8	Notification, Emergency Maintenance	Notification received at least thirty (30) minutes prior to the emergency maintenance, in accordance with SOW subsection 3.19.4 and section 4	\$2,500 per failure to timely notify	<p>The SLA is measured by the Contractor's logs and emails.</p> <p>The SLA automatically applies thirty (30) minutes prior to any emergency maintenance for which notice is not provided.</p>
	SLA-B9	Notification, Unplanned Maintenance	Notification received within two (2) hours of the unplanned maintenance, in accordance with SOW subsection 3.19.4 and section 4	\$2,500 per failure to timely notify	<p>The SLA is measured by the Contractor's logs and emails.</p> <p>The SLA automatically applies two (2) hours after any unplanned maintenance for which notice is not provided.</p>

	SLA-B10	Migration of Existing Customers	Customer migration will be completed within one-hundred and twenty (120) days of completion of the Services Infrastructure Checklist, in accordance with SOW subsection 3.23	\$3.00 per day, and per wireless data/voice device, until completed	The SLA clock stops for incumbent Contractors when all End-users are identified as either migrated or no longer receiving services from the Contractor.  The SLA clock stops for non-incumbent Contractors when all End-users identified as purchasing services from the non-incumbent Contractor are migrated.
Contractor Meetings with DMS	SLA-C1	Project Management Monthly Review Meeting	A Project Management Monthly Review Meeting must be conducted within fifteen (15) days of acceptance of the Project Charter and monthly thereafter, in accordance with SOW subsection 3.25.3.	\$250 per day	The SLA clock is on hold if the Department requests the meeting be delayed or cancelled.
	SLA-C2	Project Implementation Phase - Project Kickoff Meeting	A Project Kickoff Meeting must be conducted within fifteen (15) days of acceptance of the Project Charter, in accordance with SOW subsection 3.25.4.	\$250 per day	The SLA clock is on hold if the Department requests the meeting be delayed or cancelled.
Project Management	SLA-D1	Project Charter	A Project Charter is due within four (4) weeks of Contract execution, in accordance with SOW subsection 3.26.1.1	\$1,000 per day	

	SLA-D2	Project Management Plan	A Project Management Plan is due within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.1.2	\$1,000 per day	
	SLA-D3	Readiness Plan	A Readiness Plan is due within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.1.3	\$1000 per day	
	SLA-D4	Communications Management Plan	A Communications Plan is due within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.1.4	\$1000 per day	
	SLA-D5	Risk Management Plan	A Risk Management Plan is due within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.1.5	\$1000 per day	
	SLA-D6	Requirements Management Plan	A Requirements Management Plan is due within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.1.6	\$1000 per day	
	SLA-D7	Disaster Recovery Plan	A Disaster Recovery Plan is due within three (3) months of Contract execution, in accordance with SOW subsection 3.26.1.7	\$1,000 per day	
	SLA-D8	Project Management Implementation Phase Schedule	After acceptance of the Project Charter, a Project Management Implementation Phase Schedule is due every two (2) weeks by noon ET on Fridays, in accordance with SOW subsection 3.26.2.1	\$250 per day	

	SLA-D9	Project Management Tracking Logs	Project Management Tracking Logs must be submitted within two (2) weeks after the Project Kickoff Meeting and every two (2) weeks thereafter, in accordance with SOW subsection 3.26.2.2	\$250 per day	
	SLA-D10	Project Status Reports	Project Status Reports must be submitted within two (2) weeks after the Project Kickoff Meeting and every two (2) weeks thereafter, in accordance with SOW subsection 3.26.2.3	\$250 per day	
	SLA-D11	Guides	Guides must be provided within three (3) months of Contract execution and within one (1) week, or as otherwise specified by DMS, upon requested updates, in accordance with SOW subsection 3.26.3	\$250 per day	
	SLA-D12	Project Closure Documentation	Project Closure Documentation must be provided within one (1) month from the close of the Project Implementation Phase, in accordance with SOW subsection 3.26.4	\$250 per day	
	SLA-D13	Implementation Plan	A Project Implementation Plan must be provided within six (6) weeks of Contract execution, in accordance with SOW subsection 3.26.5.1	\$1,000 per day	
	SLA-D14	Incumbent Contractor Weekly Migration Report	An Incumbent Contractor Weekly Migration Report is due each week during implementation, in accordance with SOW subsection 3.26.5.1.b	\$1,000 per day	

	SLA-D15	Non-incumbent Contractor Weekly Migration Report	A Non-Incumbent Contractor Weekly Migration Report is due each week during implementation, in accordance with SOW subsection 3.26.5.1.c	\$1,000 per day	
	SLA-D16	Individual Customer Specific Migration Plans	Individual Customer-Specific Migration Plans must be provided within four (4) weeks of written notification of the requirement, in accordance with SOW subsection 3.26.5.2	\$500 per day	
	SLA-D17	Services Infrastructure Checklist	The Services Infrastructure Checklist must have all items completed and be accepted by the Department within the timeline agreed to in writing in the Implementation and Migration Plan, in accordance with SOW subsection 3.27	\$10,000 per day	
Public Safety	SLA-E1	Public Safety Service Plans and Devices Report	The Public Safety Service Plans and Devices Report will be provided monthly, two (2) Business Days before the Monthly Operational Meeting, in accordance with SOW section 4.7	\$1,000 per day	
Business Operations	SLA-F1	Invoicing	Complete and accurate invoices must be submitted no later than the 10th day of the month for services in arrears, in accordance with SOW subsection 5.10	\$1,000 per day	The SLA clock stops when the timestamp for when the complete and accurate electronic billing file is submitted to the Department.
	SLA-F2	Application of Billing Credits	Apply each credit in the first available billing cycle after the credit has been determined, in accordance with SOW subsection 5.10	\$1,000 per day	The SLA clock stops based upon the timestamp for when the complete and accurate electronic billing file is submitted to the Department.

Direct Ordering and Billing	SLA-G1	Cost Recovery Payment to DMS	An electronic Cost Recovery Payment will be provided within forty-five (45) days after the end of the calendar quarter to cover the fees collected for the previous quarter, in accordance with SOW subsection 6.2	\$1,000 per day	The SLA clock stops the date the check is deposited into the DMS account.
	SLA-G2	Direct-Billed Accounts Monthly Report	A Direct-Billed Accounts Monthly Report will be provided no later than the 15th of the month on all direct-billed accounts, in accordance with SOW subsection 6.4	\$1,000 per day	
	SLA-G3	Direct-Billed Accounts Quarterly Report	A Direct-Billed Accounts Quarterly Report will be provided no later than the 15th of the month on all direct-billed accounts, in accordance with SOW subsection 6.5	\$1,000 per day	



# Mobile Communications Services

## Business Case

## Table of Contents

1	Executive Summary.....	5
1.1	Purpose.....	5
1.2	Detailed Description of Services.....	5
1.3	Current Service Performance.....	6
1.4	Goals for Proposed Outsourcing.....	6
1.5	Outsourcing Authority.....	6
1.6	Descriptions of Available Options.....	7
1.7	Recommendation Methodology.....	7
2	Background.....	8
3	Revenue, Technology, and Business Model Analysis & Recommendation.....	9
3.1	Description of Current Contract Revenue.....	9
3.2	Mobile Communications Service Technology - Networks.....	13
3.3	Mobile Communications Service Technology - Equipment.....	14
3.4	Mobile Network Operator versus Mobile Virtual Network Operator.....	14
3.5	Leverage Existing State Infrastructure.....	15
3.6	Interoperability.....	15
3.7	Security.....	15
3.8	Operational Support.....	16
3.9	Public Safety.....	17
3.10	Compliance.....	17
3.11	Recommended Communication Services Technology.....	17
4	Market Conditions and Trends.....	18
4.1	Introduction.....	18
4.2	Market Conditions and Trends - Networks.....	18
4.3	Market Conditions and Trends - Equipment.....	19
4.4	Market Conditions Recommendations.....	19
5	Options & Cost Benefit Analysis.....	19
5.1	Business Models for Mobile Communication Services.....	20
5.1.1	Insourcing Mobile Network Operator.....	20

- 5.1.2 Insourcing Mobile Network Operator as MVNO..... 21
- 5.1.3 Combination Insourcing/Outsourcing ..... 22
- 5.2 Evaluation of the Options for Mobile Telecommunication Services..... 22
  - 5.2.1 Descriptions of Available Options for Insource and Outsource..... 22
  - 5.2.2 Description of Options for a Mobile Network Operator..... 23
  - 5.2.3 Description of Options for Forms of Procurement..... 23
  - 5.2.4 Assumptions for Options..... 24
- 5.3 Analysis of Advantages and Disadvantages..... 24
  - 5.3.1 Option 1 - Insourcing (MNO, MVNO)..... 24
  - 5.3.2 Option 2 – Second Brand-MNVO (Air Card Services only) and Branded Reseller-MNVO..... 24
  - 5.3.3 Option 3 – Branded Reseller-MVNO..... 25
- 5.4 Potential Performance Improvements/Service Features..... 25
- 5.5 Cost Benefit Analysis for Each Option..... 26
  - 5.5.1 Financial Model Base Case ..... 27
  - 5.5.2 Option 1 – Insource ..... 27
  - 5.5.3 Option 2 – Insource/Outsource (Second Brand/Hybrid Light MVNO)..... 27
  - 5.5.4 Option 3 – Insource/Outsource (Distribution Channel Only)..... 31
  - 5.5.5 Implementation Timeline for Option 2 & 3 ..... 34
- 6 Recommended Option & Detailed Discussion ..... 35
  - 6.1 Summary of the Three Options Considered in This Business Case ..... 36
  - 6.2 Option 1 – Insource..... 36
  - 6.3 Option 2 – Combination Insourcing and Outsourcing (Current MCS Model) ..... 36
  - 6.4 Option 3 – Combination Insourcing and Outsourcing (Distribution Channel Only)..... 37
  - 6.5 Recommendation ..... 37
- 7 Business Case Recommendations Summary..... 37
- 8 State Business Process & Policies..... 38
- 9 Performance Metrics Review ..... 38
- 10 Projected Timeframe ..... 39
- 11 Public Records Compliance ..... 40
- 12 Contingency Plan..... 40
- 13 Transition Plan ..... 41

14	American With Disabilities Act Of 1990, As Amended.....	41
15	Contract Provisions.....	42

# 1 Executive Summary

## 1.1 Purpose

The Department of Management Services (Department) has gathered information needed for the Department and key stakeholders to make an informed decision related to the Department's options for the procurement of the next generation of mobile communication services (MCS). The goal of the information gathering was to develop a business case providing a recommendation for the best and most appropriate business model and procurement options that provide long-term value to the state.

Inspired Technologies, Inc. was contracted to assist the Department's development of this business case in accordance with Section 287.0571, Florida Statutes (F.S.). The statute requires a business case to evaluate feasibility, cost-effectiveness, and efficiency before the state agency proceeds with any outsourcing of services.

This business case focuses specifically on three key elements of MCS: (1) current technology options for mobile communication services in parallel with the State needs; (2) data analysis on industry business models which are optimal for next generation MCS; and (3) best practice recommendations for implementation of such technology and the appropriate business model. The current MCS contracts are with multiple service providers to provide wireless voice and data services and equipment, including data cards, tablets, telemetry devices, feature phones, smartphones, and Push to Talk (PTT) phones.

In summary, this document provides substantive information that can be utilized to make informed decisions about the future business model and procurement options of MCS.

## 1.2 Detailed Description of Services

*Section 287.0571 (4)(a), F.S. - A detailed description of the service or activity for which the outsourcing is proposed.*

The objective of MCS is to provide SUNCOM customers the ability to purchase wireless voice and data services and equipment, including options for Public Safety Customers. SUNCOM customers are a combination of State of Florida agencies, and Other Eligible Users (OEU), as defined in Chapter 282, F.S. SUNCOM customers are currently able to purchase from multiple service pricing plans which include voice per minute rates for in-state and out-of-state calls, fixed rate plans, unlimited call packages, data-only plans, voice-only plans, voice and data bundled plans, pooling and non-pooling plans, and group mobile-to-mobile rate plans. SUNCOM customers are able to purchase equipment which includes select free standard cell phones, data-cards, hotspot devices, and PTT phones with associated monthly service plans. Additionally, there are options for discounted phones, smartphones, and data-only devices when required. SUNCOM customers are able to purchase accessories including hands-free kits, belt clips and holsters, cases, face plates, batteries, chargers, vehicle power adapters, and car kits.

### 1.3 Current Service Performance

*Section 287.0571 (4)(b), F.S. A description and analysis of the state agency's current performance, based on existing performance metrics if the state agency is currently performing the service or activity.*

In January 2012, the Department entered into contracts, through a competitive procurement, with AT&T Mobility, Sprint, and Verizon Wireless to establish MCS. The total spending under these contracts is approximately \$82 million annually. Verizon Wireless accounts for \$70 million, AT&T Mobility accounts for approximately \$7 million, and Sprint accounts for approximately \$5 million.

Having contracts with three services providers enables a SUNCOM customer to choose the service provider which offers the customer the best options. Wireless service geographic coverage varies by service provider, for example, and letting the customer decide which coverage is most beneficial is a great advantage of the multi-contract procurement model. Also, the service providers are incentivized to continue improving their service offerings and adjust pricing to attract and keep customers.

### 1.4 Goals for Proposed Outsourcing

*Section 287.0571 (4)(c), F.S. The goals desired to be achieved through the proposed outsourcing and the rationale for such goals.*

The Department's goals to be achieved in future contracts are:

- Determine the best long-term value to the State;
- Maintain cost structures with improved service integration;
- Ensure adaptability for future technology, customer needs, and evolving industry standards; and
- Provide the highest levels of customer service.

The current MCS portfolio is utilized throughout the state. As a result, agencies have built processes and dependencies that rely on the portfolio offering that is in service today. Agencies use of these services vary widely depending on the specific mobile communications needs of each specific agency. This requires the MCS vendors to offer a broad array of products and services.

### 1.5 Outsourcing Authority

*Section 287.0571 (4)(d), F.S.- A citation to the existing or proposed legal authority for outsourcing the service or activity.*

Pursuant to Section 282.703, F.S., the Department is to design, engineer, implement, manage, and operate through state ownership, commercial leasing, contracted services, or some combination thereof, the facilities, equipment, and contracts providing SUNCOM Network services, and is to develop a system of equitable billings and charges for telecommunications services. The Department's Division of State Technology (DST) is tasked with this mission of providing superior telecommunications services more cost effectively to state and local governments, educational institutions, libraries, and non-profit organizations by achieving economies of scale with enterprise planning and procurement.

## 1.6 Descriptions of Available Options

*Section 287.0571 (4)(e), F.S. - A description of available options for achieving the goals. If State employees are currently performing the service or activity, at least one option involving maintaining state provision of the service or activity shall be included.*

This business case examines options specifically for the scope of continued support, features, and offerings following the expiration of the current MCS contracts in January 2022. The options evaluated are insourcing, performing an outsourced competitive solicitation, and combinations of both outsource and insource. The options are:

*Insorce* - Is an organization's performing a service internally. Insourcing is a business decision that is often made to maintain control of critical functions or competencies that are essential to the organization's mission.

*Outsource* - Is the contracting out of a service to a third party. Outsourcing can be a way to take advantage of third-party experience and efficiency.

*Combinations of Insorce and Outsource* - Services provided by a combination of existing state employee full-time equivalent (FTE) positions, with vendors providing elements of operations that fall outside of the administrative, physical, or technical capabilities of the Department.

This business case examines a competitive procurement option, an Invitation to Negotiate. In Florida, competitive procurement is governed by Section 287.057, F.S., and Rule 60A-1, Florida Administrative Code. The three types of competitive procurement are:

Invitation to Bid (ITB) – Used when a state agency provides all technical specifications and awards on lowest price.

Request for Proposal (RFP) – Used when a state agency has determined it is not practicable to use an ITB. The state agency provides all technical specifications, and responses are evaluated on the vendor's proposed services and price.

Invitation to Negotiate (ITN) – Used when a state agency determines that negotiations with one or more vendors may be necessary to enable the state agency to receive the best value. The best value is based on factors such as price, quality, design and workmanship. This option works best when highly technical or complex services are being acquired. The price structure for services is often negotiated. The current MCS contracts were solicited as an ITN.

## 1.7 Recommendation Methodology

The Department has multiple contracts for MCS that are nearing expiration. This business case examines options and business models for the evolution of MCS, and the advantages and risks of each. The business case takes into consideration the statutory requirements and evaluates whether to insource these services, outsource these services, or to provide these services using a combination of existing Department resources and outsourcing.

Throughout the document, there are numerous recommendations and discussion points for consideration. The business case recommendations can be found in Section 7 Business Case Recommendations Summary.

## 2 Background

### **Mobile Communication Services Contracts and Portfolio of Products & Services (Prior to 2011):**

Multiple contracts were made available to SUNCOM customers, separately offering wireless data and voice services:

1. Department of Management Services, State Purchasing, State Term Contract
  - Wireless Voice Services Contract with Verizon Wireless for cell phones voice only services.
2. Western State Contracting Alliance, Alternate Source Contract
  - Wireless Voice Services –Contract with AT&T and Sprint/Nextel for cell phones voice only services.
3. Department of Management Services, Division of State Technology, Enterprise Contract
  - Wireless Data Services – Contracts with AT&T Mobility, Sprint and Verizon Wireless for wireless data services (air cards)

### **Mobile Communication Services Contracts and Portfolio of Products & Services (2012 - Present):**

Multiple contracts are made available through the Department's SUNCOM offerings. The current MCS service providers are AT&T, Sprint, and Verizon. Each of these contracts provide for the purchase of wireless voice and data equipment, services, and accessories. Public safety options, discussed further in Section 3.9 below, are available to DMS Customers. MCS services are interoperable with other SUNCOM services, including network integration with MyFloridaNet. State agencies have the option to route MCS traffic through their security perimeter to perform additional screening and filtering. The contracts contain stringent Service Level Agreements (SLAs) to manage vendor's service performance and to perform Key Performance Indicators measurements.

These contracts provide for the purchase of wireless voice and data equipment, services for data-cards, tablets, telemetry devices, feature phones, Smartphones, BlackBerrys, PTT phones and services, and accessories. Service pricing plans include voice per minute rates for in-state and out-of-state calls, as well as several fixed rate plans, unlimited call packages, data-only plans, voice-only plans, voice and data bundled plans, pooling and non-pooling plans, and group mobile to mobile rate plans. These contracts have been renewed to January 2022.

### 3 Revenue, Technology, and Business Model Analysis & Recommendation

#### 3.1 Description of Current Contract Revenue

The financial analysis below is based on total customer revenue.

##### Top 20 Customers in Total Revenue:

CUSTOMER NAME	Category	2014/2015	2015/2016	2016/2017	2017/2018	Total
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES	State	\$ 1,518,850	\$ 3,123,577	\$ 3,461,764	\$ 1,314,405	\$ 9,418,596
CITY OF TAMPA	OEU	\$ 592,943	\$ 1,311,382	\$ 1,456,873	\$ 751,973	\$ 4,113,171
FLORIDA DEPARTMENT OF HEALTH	State	\$ 484,778	\$ 1,026,486	\$ 1,395,200	\$ 788,039	\$ 3,694,504
SCHOOL BOARD OF MIAMI DADE	OEU	\$ 28,143	\$ 1,039,563	\$ 1,242,495	\$ 717,295	\$ 3,027,495
JACKSONVILLE SHERIFF'S OFFICE	OEU	\$ 264,191	\$ 917,121	\$ 994,134	\$ 498,354	\$ 2,673,800
BROWARD SHERIFF'S OFFICE	OEU	\$ 493,039	\$ 881,232	\$ 874,764	\$ 398,797	\$ 2,647,831
ORANGE COUNTY SHERIFF'S OFFICE	OEU	\$ 486,972	\$ 854,222	\$ 841,278	\$ 453,132	\$ 2,635,604
PALM BEACH COUNTY SHERIFF'S OFFICE	OEU	\$ 367,897	\$ 656,829	\$ 815,645	\$ 326,481	\$ 2,166,852
HILLSBOROUGH COUNTY DATA	OEU	\$ 285,547	\$ 653,503	\$ 758,020	\$ 369,678	\$ 2,066,748
CITY OF JACKSONVILLE	OEU	\$ 269,985	\$ 584,671	\$ 507,660	\$ 665,932	\$ 2,028,248
CITY OF TALLAHASSEE	OEU	\$ 321,878	\$ 660,553	\$ 683,448	\$ 346,118	\$ 2,011,997
DEPARTMENT OF CORRECTIONS - OFFICE OF INFORMATION TECHNOLOGY	State	\$ 1,954	\$ 6,527	\$ 811,902	\$ 999,442	\$ 1,819,824
DEPARTMENT OF CHILDREN AND FAMILIES - ORLANDO	State	\$ 394,943	\$ 491,350	\$ 584,548	\$ 344,904	\$ 1,815,744
PINELLAS COUNTY SHERIFF'S OFFICE	OEU	\$ 285,553	\$ 569,949	\$ 556,825	\$ 325,349	\$ 1,737,677
NORTH BROWARD HOSPITAL DISTRICT	OEU	\$ 223,998	\$ 452,970	\$ 519,231	\$ 402,864	\$ 1,599,063
CITY OF MIAMI BEACH DATA	OEU	\$ 170,922	\$ 517,493	\$ 559,048	\$ 340,283	\$ 1,587,746
CITY OF ORLANDO EMERGENCY OPERATIONS CENTER	OEU	\$ 213,344	\$ 475,293	\$ 521,522	\$ 222,511	\$ 1,432,670

JACKSONVILLE ELECTRIC AUTHORITY, CITY OF JACKSONVILLE	OEU	\$ 235,600	\$ 444,121	\$ 477,780	\$ 249,551	\$ 1,407,052
DEPARTMENT OF CHILDREN AND FAMILIES - NORTHEAST ZONE	State	\$ 193,662	\$ 395,866	\$ 645,868	\$ 154,524	\$ 1,389,921
POLK COUNTY SHERIFF'S OFFICE DATA	OEU	\$ 219,271	\$ 490,398	\$ 448,582	\$ 188,246	\$ 1,346,497
<b>GRAND TOTAL</b>		<b>\$ 7,053,470</b>	<b>\$ 15,553,106</b>	<b>\$ 18,156,587</b>	<b>\$ 9,857,877</b>	<b>\$ 50,621,040</b>

*Figure 1 – Top 20 Customers in Total Revenue*

### Top 20 State Customers in Total Revenue:

CUSTOMER NAME	Category	2014/2015	2015/2016	2016/2017	2017/2018	Total
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES	State	\$ 1,518,850	\$ 3,123,577	\$ 3,461,764	\$ 1,314,405	\$ 9,418,596
DEPARTMENT OF HEALTH	State	\$ 484,778	\$ 1,026,486	\$ 1,395,200	\$ 788,039	\$ 3,694,504
DEPARTMENT OF CORRECTIONS - OFFICE OF INFORMATION TECHNOLOGY - TALLAHASSEE	State	\$ 1,954	\$ 6,527	\$ 811,902	\$ 999,442	\$ 1,819,824
DEPARTMENT OF CHILDREN AND FAMILIES - ORLANDO	State	\$ 394,943	\$ 491,350	\$ 584,548	\$ 344,904	\$ 1,815,744
DEPARTMENT OF CHILDREN AND FAMILIES - NORTHEAST ZONE	State	\$ 193,662	\$ 395,866	\$ 645,868	\$ 154,524	\$ 1,389,921
FLORIDA DEPARTMENT OF LAW ENFORCEMENT	State	\$ 187,137	\$ 393,032	\$ 429,967	\$ 222,934	\$ 1,233,070
DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATIONS	State	\$ 164,328	\$ 383,284	\$ 423,833	\$ 258,025	\$ 1,229,470
FLORIDA FISH AND WILDLIFE COMMISSION	State	\$ 153,456	\$ 315,160	\$ 312,445	\$ 185,128	\$ 966,189
DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES	State	\$ 126,728	\$ 309,969	\$ 348,319	\$ 158,630	\$ 943,645
DEPARTMENT OF CHILDREN AND FAMILIES	State	\$ 111,498	\$ 282,740	\$ 388,855	\$ 116,905	\$ 899,998
DEPARTMENT OF FINANCIAL SERVICES - DIVISION OF REHABILITATION AND LIQUIDATED DAMAGES	State	\$ 106,317	\$ 228,075	\$ 251,080	\$ 116,070	\$ 701,542

FLORIDA DEPARTMENT OF CORRECTIONS - DISTRICT 4	State	\$	24,085	\$	154,936	\$	512,859	\$	691,880		
FLORIDA DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES	State	\$	81,873	\$	208,520	\$	226,449	\$	125,385	\$	642,227
DEPARTMENT OF CHILDREN AND FAMILIES - SUNCOAST REGION	State	\$	2	\$	147,862	\$	323,048	\$	154,924	\$	625,835
DEPARTMENT OF CHILDREN AND FAMILIES - OFFICE OF FINANCIAL SUPPORT	State	\$	65,799	\$	152,824	\$	195,937	\$	106,878	\$	521,438
DEPARTMENT OF LEGAL AFFAIRS	State	\$	62,409	\$	166,672	\$	168,173	\$	93,625	\$	490,880
FLORIDA DEPARTMENT OF CORRECTIONS - REGION 3	State	\$	77,026	\$	184,647	\$	208,562	\$		\$	470,236
DEPARTMENT OF CHILDREN AND FAMILIES - CHILDREN'S NETWORK SOUTHWEST	State	\$	72,916	\$	128,726	\$	163,996	\$	76,643	\$	442,280
FLORIDA DEPARTMENT OF CORRECTIONS - REGION 2	State	\$	70,195	\$	203,343	\$	160,558	\$		\$	434,096
DEPARTMENT OF CHILDREN AND FAMILIES - NORTHWEST REGION	State	\$	60,386	\$	139,973	\$	159,447	\$	73,741	\$	433,547
<b>GRAND TOTAL</b>		\$	3,958,342	\$	8,443,569	\$	11,172,809	\$	5,290,202	\$	28,864,922

*Figure 2 – Top 20 State Customers in Total Revenue*

### Top 20 Other Eligible Users (OEU) in Total Revenue:

CUSTOMER NAME	Category	2014/2015	2015/2016	2016/2017	2017/2018	Total
CITY OF TAMPA	OEU	\$ 592,943	\$ 1,311,382	\$ 1,456,873	\$ 751,973	\$ 4,113,171
MIAMI COUNTY PUBLIC SCHOOLS	OEU	\$ 28,143	\$ 1,039,563	\$ 1,242,495	\$ 717,295	\$ 3,027,495
JACKSONVILLE SHERIFF'S OFFICE	OEU	\$ 264,191	\$ 917,121	\$ 994,134	\$ 498,354	\$ 2,673,800
BROWARD SHERIFF'S OFFICE	OEU	\$ 493,039	\$ 881,232	\$ 874,764	\$ 398,797	\$ 2,647,831
ORANGE COUNTY SHERIFF'S OFFICE	OEU	\$ 486,972	\$ 854,222	\$ 841,278	\$ 453,132	\$ 2,635,604
PALM BEACH COUNTY SHERIFF'S OFFICE	OEU	\$ 367,897	\$ 656,829	\$ 815,645	\$ 326,481	\$ 2,166,852
HILLSBOROUGH COUNTY DATA	OEU	\$ 285,547	\$ 653,503	\$ 758,020	\$ 369,678	\$ 2,066,748
CITY OF JACKSONVILLE	OEU	\$ 269,985	\$ 584,671	\$ 507,660	\$ 665,932	\$ 2,028,248
CITY OF TALLAHASSEE	OEU	\$ 321,878	\$ 660,553	\$ 683,448	\$ 346,118	\$ 2,011,997
PINELLAS COUNTY SHERIFF	OEU	\$ 285,553	\$ 569,949	\$ 556,825	\$ 325,349	\$ 1,737,677

NORTH BROWARD HOSPITAL	OEU	\$ 223,998	\$ 452,970	\$ 519,231	\$ 402,864	\$ 1,599,063
CITY OF MIAMI BEACH DATA	OEU	\$ 170,922	\$ 517,493	\$ 559,048	\$ 340,283	\$ 1,587,746
CITY OF ORLANDO - EMERGENCY OPERATIONS CENTER	OEU	\$ 213,344	\$ 475,293	\$ 521,522	\$ 222,511	\$ 1,432,670
JACKSONVILLE ELECTRIC AUTHORITY, CITY OF JACKSONVILLE	OEU	\$ 235,600	\$ 444,121	\$ 477,780	\$ 249,551	\$ 1,407,052
POLK COUNTY SHERIFF'S OFFICE DATA	OEU	\$ 219,271	\$ 490,398	\$ 448,582	\$ 188,246	\$ 1,346,497
CITY OF FORT LAUDERDALE DATA	OEU	\$ 212,148	\$ 377,340	\$ 439,911	\$ 168,516	\$ 1,197,915
WEST PALM BEACH PUBLIC SAFETY	OEU	\$ 172,390	\$ 389,970	\$ 419,190	\$ 169,852	\$ 1,151,402
MARION COUNTY SHERIFF'S OFFICE	OEU	\$ 165,963	\$ 370,710	\$ 373,888	\$ 218,241	\$ 1,128,802
COLLIER COUNTY SHERIFF'S OFFICE	OEU	\$ 191,137	\$ 327,097	\$ 389,192	\$ 185,620	\$ 1,093,046
LEE COUNTY - BOARD OF COUNTY COMMISSIONERS	OEU	\$ 144,059	\$ 333,641	\$ 395,758	\$ 213,754	\$ 1,087,212
<b>GRAND TOTAL</b>		<b>\$ 5,344,979</b>	<b>\$ 12,308,058</b>	<b>\$ 13,275,243</b>	<b>\$ 7,212,547</b>	<b>\$ 38,140,828</b>

*Figure 3 – Top 20 OEU Customers in Total Revenue*

### **3.2 Mobile Communications Service Technology - Networks**

The wireless industry consistently experiences increasing demand for network functionality. With increasingly versatile internet-enabled equipment such as smart phones, televisions, personal computers, and tablets, consumers have a growing need and demand for immediate access to voice, video, and data services.

This demand is driving the wireless industry to support new levels of enterprise productivity for enhanced mobile solutions. Platforms are increasingly open, supporting an explosion of new applications and services directly to the mobile user. Service provider options are multiplying each day as businesses find themselves in a race to capture market share and revenue from new services. Businesses are responding to demand by boosting capabilities and introducing new technology as quickly as possible. Capital investment in network development and infrastructure has risen to unprecedented levels. This includes upgrading core network transport capacity, growing high-capacity access in major metropolitan areas, extending fiber optic lines closer to consumers, adding high-speed residential broadband technology to legacy phone networks, and improving content serving and distribution technologies<sup>2</sup>.

The wireless industry is currently using Fourth-generation, Long-Term Evolution (4G LTE), technology, as defined by the radio sector of the International Telecommunication Union (IUT-R). These standards were set in March 2008. For mobile use, including smartphones, and other internet-enabled equipment, connection speeds need to have a peak download speeds of at least 100 megabits per second, and for more stationary uses such as mobile hotspots, at least 1 gigabit per second. Global capital spending on fifth-generation (5G LTE) technology is increasing much like the marketplace experienced with the evolution of 4G LTE technology. Today, 4G LTE provides the framework for the fastest connection available for wireless networks, which varies based upon wireless carrier and service topology. As the next evolution comes to reality, increased connection speeds and capabilities will improve as well.

5G LTE technology will utilize unique radio frequencies not used currently in 4G. 4G networks use frequencies below 6 GHz, and 5G will likely use extremely high frequencies in the 30 GHz to 300 GHz range. These higher frequencies are less congested with existing cellular data and will support a larger capacity for data. At its peak, 5G can be up to 20 times faster than 4G. Limited 5G demonstrations have taken place, with carriers anticipating the 5G release in test markets in late 2018, increasing the release in 2019 through 2020.

Some projections forecast that demand for additional network capacity will increase 25-fold over the next 3 years<sup>3</sup>. Each major improvement in network speed and capacity generates new services, devices, and applications that raise consumer expectations, using up the added capacity and creating the requirement to add even more capacity. For telecommunications, the standard will be continuous waves of increased demand and increased network capacity.

Improved coverage throughout the state remains a high priority for customers. Customers expect coverage not only in metropolitan areas with multiple carrier options, but also in rural and coastline areas. Currently service is provided by multiple carriers utilizing 3G and 4G LTE technology. Where coverage challenges exist in rural areas, coverage may be reduced to a

single carrier providing 3G technology, which does not provide the latest technical and is sometimes limited in data service capabilities, meaning data applications on smartphones do not work as expected.

Coupled with the demand for improved rural coverage is the demand for improved coverage within buildings. A barrier to this is building penetration, which is continually hampered by thick concrete and steel structures. To address this issue, many buildings are being equipped at the time of new construction or retro fitted with Distributed Antenna Systems (DAS) to extend coverage inside a building. As the evolution from 4G to 5G takes place over the coming years, the state should see improvements in this particular area due to the increased density of towers and small cell deployments, which is a requirement for the implementation of 5G technology.

### **3.3 Mobile Communications Service Technology - Equipment**

Equipment available under the current MCS contracts includes cellular phones, smartphones, data-cards, tablets, telemetry devices, feature phones, and push-to-talk phones. Associated accessories are also available, which includes hands-free kits, belt clips and holsters, cases, face plates, batteries, chargers, vehicle power adapters, and car kits.

During the duration of new MCS contracts, equipment must be compatible with the latest generation of wireless communication. The Department will need to ensure access to future releases of cellular phones and other internet-enabled equipment are compatible with 5G networks and other future generations of wireless networks. This should include devices that are band 14 enabled or otherwise appropriate for Public Safety Customers.

As the industry continues to see growth and development of new cellular phone features with other internet-enabled technology, emerging technologies may be incorporated into future cellular phone releases including facial recognition technology, augmented reality, improved durability, and longer battery life<sup>1</sup>.

### **3.4 Mobile Network Operator versus Mobile Virtual Network Operator**

A mobile network operator (MNO) is a wireless telecommunications provider that owns, manages, and controls all elements necessary to implement, sell, and deliver mobile services to the customer. These elements include radio spectrum allocation, network infrastructure, billing support resources, customer service resources, handset management, provisioning of software, and distribution channels for product and service delivery. In addition to obtaining market share by offering its own services an MNO may also allow or sell access to network services at wholesale rates to mobile virtual network operators (MVNO).

MVNO platforms do not supply spectrum, network routing and interconnectivity, but they provide application services, customer care, billing, handset management, and distribution channels for products and services. Also, commonly handled within the MVNO framework are “second brands” of incumbent MNOs and “branded resellers” that resell an MNO’s products and services

---

<sup>1</sup> <https://mobilebusinessinsights.com/2018/01/future-technology-of-mobile-phones-what-can-you-expect-to-see-at-mobile-world-congress-2018/>

under their own brand and are essentially a specialized marketing and sales distribution channel.

The current DMS MCS model is essentially an MVNO hybrid of second brands and branded reseller. DMS acts as a branded reseller for all products in the MCS platform except for air card services. For the air card services platform DMS provides customer support, billing, handset management, and distribution and sales.

### **3.5 Leverage Existing State Infrastructure**

Currently there is no state telecommunications infrastructure that is used for the mobile communication services platform.

### **3.6 Interoperability**

Network interoperability has become increasingly important in the telecommunications industry. The basic idea behind interoperability is the ability for two or more networks, systems, devices, applications or components to communicate. With respect to the telecommunications industry, interoperability refers to the interworking of telecom services over multi-vendor, multi-carrier inter-connections. As networks continue to grow and diversify with the 5G and IoT era on the horizon, it is important they can interoperate to enable end-to-end communication.

Devices can interoperate with other devices either by adhering to a common protocol standard, abiding by a published interface standard or situating a gateway between them capable of translating each device's protocols. These common protocol standards serve as a platform for manufacturers, which note all the necessary components for interoperability into various systems and products.<sup>2</sup> Although interoperability has improved in the telecommunications industry, service providers are continuing to work towards interconnection of 5G and IoT devices through network infrastructure enhancement and uniformity of standards.

### **3.7 Security**

Service Providers must provide device and network security, and responsiveness to ever changing security risk in today's telecommunication environment. Threats to the government's use of mobile devices are real and exist across all elements of provider networks and mobile devices. The stakes for government users are high. Government mobile devices — despite being a minor share of the overall market — present an avenue to attack back-end systems containing data on Floridians in addition to sensitive information relevant to government functions. Mobile devices hold significant amounts of sensitive information, whose compromise could adversely impact State and OEU operations. Additionally, databases controlled by the State and OEUs hold tremendous amounts of personally identifiable information that could be used to compromise financial wellbeing, privacy, or identity.

Threats range from advanced attacks, to organized crime using advanced fraud technologies, to simple theft of mobile phones. The threats to government users of mobile devices include the

---

<sup>2</sup> RCRWireless News (April 2018) *The Role of Network Interoperability in Telecommunications*. Retrieved on January 28, 2019 at <https://www.rcrwireless.com/20180419/the-role-of-network-interoperability-in-telecommunications-tag27-tag99>

same threats that target consumers, e.g., call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data. Government users may be subject to additional threats simply because they are government employees.

Areas of security vulnerability include:

- Mobile device technology stack, including mobile operating systems and lower level device components
- Mobile applications
- Networks (e.g., cellular, Wi-Fi, Bluetooth) and services provided by network operators
- Device physical access
- Enterprise mobile services and infrastructure, including mobile device management, enterprise mobile app stores and mobile application management

Guidance and best practice is identified for providers and customers through the U.S. Department of Commerce, National Institute of Standards and Technology, other government agencies, non-government organizations and private industry. Although security has improved, significant improvements still need to be made in this area as well as hardening on the new 5G network protocols, which are currently in development<sup>3</sup>.

### **3.8 Operational Support**

Operational support has transformed to meet the consumer's increasing needs related to increasing complex technology. Many service providers are now able to allow customers to self-manage account profiles and utilize self-service tools via online portals. This allows customers to self-manage inventory management, security management, policy management, and support management, which is not always appropriate for all customers depending on their technical staff and complexity of their needs. Customer care and operational support is provided in all service levels of the MNO and MVNO framework except for the branded reseller platform which focuses only on distribution.

The Department should require operational support for all operational needs including billing and technical support. The expectations of a service provider include trouble ticket systems, access to skilled technicians, access to skilled billing staff, policy enforcement, quality control and assurance, monitoring tools, and performance reporting. Service provider should allow customers the option to self-manage accounts. Service provider should function to a world class standard of customer focused service delivery, consistently striving for customer satisfaction that evolves with the technology over time.

---

<sup>3</sup> United States Department of Homeland Security (April 2017). *Study on Mobile Devices*. Retrieved on August 15, 2017 at <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

### **3.9 Public Safety**

Mobile technology continues to play a key role in today's public safety network. Service providers are working with the public safety community on enhanced emergency and first responder features.

FirstNet was established by the Middle Class Tax Relief and Job Creation Act of 2012 ("Act"). Under the Act, FirstNet is responsible for ensuring that all components of the Nationwide Public Safety Broadband Network (NPSBN), are built, deployed, operated, and maintained. The NPSBN provides services to public safety entities throughout the nation.

FirstNet is an independent federal authority with a statutory duty and responsibility to take all actions necessary to ensure the building, deployment, and operation of the NPSBN based on a single, national network architecture.

Mobile providers are now working to build out public safety networks, including FirstNet, dedicated to first responders. Key elements of the public safety networks are developed to enable first responders to communicate and coordinate during emergencies, large events, or other situations where commercial networks can become congested. Therefore, focus has been placed on priority and preemption, which allows providers to shift commercial traffic to other areas of their respective networks, allowing first responders seamless communication.

### **3.10 Compliance**

The Federal Communications Commission (FCC) mandates all mobile network operators and all mobile virtual network operators comply with standards and requirements defined for all telecommunications service providers. Compliance with all Federal Americans with Disabilities Act (ADA), Health Insurance Portability and Accountability Act (HIPAA) and Communications Assistance for Law Enforcement Act (CALEA) must be maintained. In addition to Federal mandates, state and local regulatory requirements must also be met to provide services within a given geographic region as appropriate.

### **3.11 Recommended Communication Services Technology**

The following recommendation is provided for the MCS platform:

1. The Department should embrace solutions that allow the MCS contracts to easily evolve with changing technology and industry offerings without delays in service offerings.
2. The Department should ensure providers are ready to offer mobile communication network capabilities to all users with minimal cost related to new mobile devices and demonstrate a commitment to offer the latest generation of technology throughout the life of the contract.

3. The Department should work with service providers to ensure network and mobile device security continues to develop in accordance with security related standards and best practices.
4. The Department should support customers in managing security practices within their control.
5. The Department should ensure providers are able to offer a wide variety of equipment and accessories, fulfilling the diverse needs of the MCS customers.
6. The Department should ensure providers are able to offer world class customer service.
7. The Department should ensure public safety spectrum networks are offered by service providers to appropriate eligible users.

## 4 Market Conditions and Trends

*Section 287.0571 (4)(g), F.S. A description of the current market for the contractual services that are under consideration for outsourcing.*

### 4.1 Introduction

This analysis is intended to meet the statutory requirement of Section 287.0571(4)(g), F.S., which requires “a description of the current market for the contractual services that are under consideration for outsourcing.” Information used for this analysis was gained through a number of methods and sources including:

- Discussions with the Department’s staff and management;
- Review of extensive data and information provided by the Department regarding SUNCOM operations and billing;
- Review of current MCS contracts including amendments;
- Research on evolving mobile communication service offerings of large providers;
- Review of industry research

### 4.2 Market Conditions and Trends - Networks

The mobile communications industry has evolved drastically over the past 10 years as data driven customers with numerous technical devices consume more bandwidth. During this time, mobile network operators (MNO) have expanded their service offerings and overhauled their price plans to meet explosive demand, while rising capital expenditures underline the ongoing need to upgrade network capabilities. The mobile communications industry will continue to evolve over the next few years and beyond. Boundaries will blur among product categories as a

range of industry actors shape customer demand. New partnerships will play an ever more important role in driving new technology and innovation.

The push for the next evolution of mobile technology is the consumers desire to seamlessly transition between voice and data capabilities ubiquitously as they move from location to location utilizing mobile and Wi-Fi services. As seen in the migration from 3G to 4G, the 5G technology is predicted to drastically increase data usage per user. Future networks will require fast rollouts, significant capacity, agile, flexible, on-demand and software-oriented telecommunication technologies.

### **4.3 Market Conditions and Trends - Equipment**

Demand for internet-enabled equipment, including smartphone, tablets, laptops, and public safety equipment, continues to grow. Market penetration by cheaper imports is increasing. These imports are both manufactured and distributed by foreign companies, as opposed to domestic smartphones, which are still manufactured by foreign companies but marketed and distributed by domestic companies. Foreign manufacturers are actively producing lower-priced smartphone models to siphon off a share of the lucrative US smartphone market. Thus, buyers have a wider range of products and prices to choose from, which boosts competition and buyer power. In addition, the influx of imports has forced larger suppliers to develop their own cheaper alternatives to remain competitive at the low end of the market.

Buyers of internet-enabled equipment have also been benefiting from low price volatility during the past three years. Although smartphones are costly, low price volatility indicates that buyers need not worry about sudden price shifts. Furthermore, even though vendors release newer and costlier versions of smartphones annually, increasing market saturation will limit price growth in the coming years as consumers become less willing to pay more for cosmetic updates.

### **4.4 Market Conditions Recommendations**

The following recommendations are based on market conditions:

1. The Department should consider established wireless carriers, and wireless carriers that are emerging in the market that could possibly provide lower cost options.
2. The Department should consider tiered volume-based options with wireless carriers, creating the opportunity for discounts.
3. The Department should consider a wide range of equipment to cover basic and high-end mobile capabilities.

## **5 Options & Cost Benefit Analysis**

*Section 287.0571 (4)(h), F.S. A cost-benefit analysis documenting the direct and indirect specific baseline costs, savings, and qualitative and quantitative benefits involved in or resulting from the*

*implementation of the recommended option or options. Such analysis must specify the schedule that, at a minimum, must be adhered to in order to achieve the estimated savings. All elements of cost must be clearly identified in the cost-benefit analysis, described in the business case, and supported by applicable records and reports. The State agency head shall attest that, based on the data and information underlying the business case, to the best of his or her knowledge, all projected costs, savings, and benefits are valid and achievable. As used in this section, the term "cost" means the reasonable, relevant, and verifiable cost, which may include, but is not limited to, elements such as personnel, materials and supplies, services, equipment, capital depreciation, rent, maintenance and repairs, utilities, insurance, personnel travel, overhead, and interim and final payments. The appropriate elements shall depend on the nature of the specific initiative. As used in this paragraph, the term "savings" means the difference between the direct and indirect actual annual baseline costs compared to the projected annual cost for the contracted functions or responsibilities in any succeeding State fiscal year during the term of the contract.*

Consideration of options for procurement of MCS was performed after careful review of mobile telecommunications markets and trends, from both a State of Florida perspective and nationally. Based on this understanding of markets and trends; the following analysis reviews a variety of factors, such as: budgets, resources, stability, reliability, cost, risks, time to implement, and simplification opportunities.

## **5.1 Business Models for Mobile Communication Services**

### **5.1.1 Insourcing Mobile Network Operator**

The business case is required to consider as an option insourcing of MCS, examining whether feasibility, cost-effectiveness, and efficiency is not better obtained by the Department directly delivering services. Insourcing would require the assets, capabilities and staff to construct and operate a Mobile Network Operations (MNO) platform for the State of Florida. This would require DMS to become one of the largest mobile telecommunications operators in Florida, in direct competition with service providers such as AT&T, Sprint, T-Mobile, and Verizon.

The Department would be required to:

- Negotiate interoperability with other national providers to allow for roaming;
- Establish a radio access network and acquire license for the use of needed spectrum. Since 1994, the Federal Communications Commission (FCC) has conducted auctions of licenses for electromagnetic spectrum. The Department would need to become a qualified bidder. The electromagnetic spectrum the Department would require would not necessarily be available for purchase through auction. The recent FCC Auction 73: 700 MHz Band received bids for geographic areas including the State of Florida, with gross bids of \$19.2 billion<sup>4</sup>;
- Establish of network-to-network interfaces with every local incumbent local exchange carrier in the State of Florida, as well as for other originating and terminating carriers such as long-distance service providers.
- Purchase and implement voice transport infrastructure services, including the design and buildout of cell phone towers across the State of Florida. The costs would include

<sup>4</sup> <https://www.fcc.gov/auction/73>

an initial investment in obtaining land through purchase or lease, building new cell phone towers, and ongoing operation and maintenance costs associated with the towers;

- Purchase and install operational support systems which support all back-office systems associated with operating the MCS network, including administrative and other reports, facilities and maintenance, rating and billing functions;
- Purchase and install business support systems which support all front office systems associated with operating the MCS network, including customer service representatives;
- Provide professional staffing for management functions not present today at the Department including regulatory filings, FCC reporting, Public Service Commission reporting, carrier relations and the like;
- Provide operations staffing for a statewide network including billing, provisioning, maintenance and repair, and the Network Operations Center;
- Establish a NOC, which includes the staffing mention above, and also contact center voice equipment and services. A NOC required for these services would include highly skilled multi-lingual contact center agents, and escalation to technically skilled contact center agents. There would also be a cost for the office space required for the contact center agents and supervisors; and
- Negotiate contracts with device manufacturers for the purchase of devices.

Under this option, the costs to establish a large new statewide MNO are overwhelming and involve considerable risk. For these reasons this insource option is not recommended and is not considered further in this business case.

### **5.1.2 Insourcing Mobile Network Operator as MVNO**

A second “insourcing” consideration is the development of a Mobile Virtual Network Operator (MVNO). An MVNO provides mobile services to end-users without owning its own frequency spectrum or network infrastructure, as it buys such capacity from a host MNO.

As an MVNO, the Department would not own and operate a network but would still be required to:

- Purchase and install operational support systems which support all back-office systems associated with operating the MCS network, including administrative and other reports, facilities and maintenance, rating and billing functions;
- Purchase and install business support systems which support all front office systems associated with operating the MCS network, including customer service representatives;
- Provide professional staffing for management functions not present today at the Department including regulatory filings, FCC reporting, Public Service Commission reporting, carrier relations and the like;
- Provide operations staffing for a statewide network including billing, provisioning, maintenance and repair, and the Network Operations Center;
- Establish a NOC, which includes the staffing mention above, and also contact center voice equipment and services. A NOC required for these services would include highly skilled multi-lingual contact center agents, and escalation to technically skilled contact center agents. There would also be a cost for the office space required for the contact center agents and supervisors; and
- Negotiate contracts with device manufacturers for the purchase of devices.

Under this option, the costs to establish an MNVO are lower than an MNO, but are substantial and involve considerable risk. For these reasons this insource option is not recommended and is not considered further in this business case.

### 5.1.3 Combination Inourcing/Outsourcing

The Department is acting as a “second brand MVNO” for air cards, and as a “branded reseller MVNO” for all other equipment and services. Today, the Department operates its air card platform as a second brand-MNVO by providing customer care including device activation. DMS originally selected this model to ensure security for air cards. These security techniques include IP address management and isolation of customer traffic via closed user groups. Closed user groups are the segregation of traffic into steams which are only visible to that specific customer. DMS also provides billing and device management for its air card platform. However, the remaining MCS platform is provider managed and the Department only provides a distribution channel for those products and services.

**Second Brand-MVNO** is a model that provides customer care, billing, handset management, and distribution. This platform allows for market participation without spectrum and technical value add including interconnectivity and application development.

**Branded Reseller-MVNO** is a model where the MVNO provides only the distribution channel for products and services. All other support functions are handled by another MVNO or MNO. This is the most flexible and risk adverse platform in the MVNO model.

## 5.2 Evaluation of the Options for Mobile Telecommunication Services

The following is the evaluation of options available to the state for services similar to MCS:

### 5.2.1 Descriptions of Available Options for Insource and Outsource

*Section 287.0571 (4)(e), F.S. - A description of available options for achieving the goals. If State employees are currently performing the service or activity, at least one option involving maintaining State provision of the service or activity shall be included.*

This business case examines three options specifically for the scope of continued support, integration, and installation of MCS and ancillary features/capabilities following the expiration of the current MCS contracts.

#### **Insource, Outsource, Insource/Outsource Combination**

*Insource* - Is an organization’s performing a service internally. Inourcing is a business decision that is often made to maintain control of critical functions or competencies that are essential to the organization’s mission.

*Outsource* - Is the contracting out of a service to a third party. Outsourcing can be a way to take advantage of third party experience and efficiency.

*Combinations of Insource and Outsource* - Services provided by a combination of existing state employee full-time equivalent (FTE) positions, with vendors providing

elements of operations that fall outside of the administrative, physical, or technical capabilities of the Department.

## 5.2.2 Description of Options for a Mobile Network Operator

The options for procurement of MCS capability that are evaluated in this business case are:

1. An option based on insourcing whereby the Department creates a Mobile Network Operator and manages all mobile communication functions, like the operations of a competitive mobile network carrier. For reasons described above, Sections 5.1.1 and 5.1.2, are not further considered in this business case. (MNO, MVNO) – **Option 1**
2. An option based on a combination of insource/outsource whereby the Department outsources the significant mobile communication functions and uses a second brand MVNO platform to manage customer care, billing, and equipment management for air card service only and provides only a distribution channel for the mobile network provider's products and services. This is DMS' current model (Second Brand-MNVO and Branded Reseller-MVNO). – **Option 2**; and,
3. An option based on a combination of insource/outsource whereby the Department outsources all the mobile communication functions and acts only as a brand reseller providing only a distribution channel for the mobile network provider's products and services, including air cards. (Branded Reseller- MVNO) – **Option 3**

## 5.2.3 Description of Options for Forms of Procurement

**Competitive Procurement** - Section 287.057, F.S., and Department of Management Services (DMS) Rule 60A-1, Florida Administrative Code, provides:

*Invitation to Negotiate (ITN)* – Used when the agency knows the desired end result but is not sure how to get there; or, there are many ways to get to the end result; or, the qualifications of the provider and quality is more important than price. This option works best when highly technical or complex services are being acquired. The price structure for services is negotiated.

*Invitation to Bid (ITB)* – Used when the agency knows exactly what it wants. Price is the determining factor in the award.

*Request for Proposal (RFP)* – Used when the agency has a general idea of what it wants. Services and price are evaluated.

These procurement options are within the scope for outsourcing as required by Chapter 287.0571, F.S., and represent common procurement options utilized by the state for similar needs. This business case recommends an ITN as the best procurement option but leaves that determination to Executive Leadership. The services contemplated within this business case are highly technical which limits the Department's ability to establish precise specifications or specifically define the services and identify necessary deliverables. Pricing will not be the sole determining factor in determining a contract award and the Department desires the ability to negotiate the best method of service delivery.

## 5.2.4 Assumptions for Options

The financial modeling presented in this business case uses the “combination insource/outsource” framework.

## 5.3 Analysis of Advantages and Disadvantages

*Section 287.0571 (4)(f) - An analysis of the advantages and disadvantages of each option, including, at a minimum, potential performance improvements and risks.*

Advantages and disadvantages, including risks, for the alternative options as compared to continued separate mobile communication services contracting, and to each other, are as follows. Additional risk analysis are contained within each option and discussed in Sections 5.3.2 and 5.3.3. Potential performance improvements are discussed in Section 5.4.

### 5.3.1 Option 1 - Insourcing (MNO, MVNO)

For reasons described in Section 5.1.1 and 5.1.2, this option is not considered further in this business case.

### 5.3.2 Option 2 – Second Brand-MNVO (Air Card Services only) and Branded Reseller-MNVO

Option 2 is a combination of insource/outsource functionality whereby DMS outsources the physical network associated with the mobile telecommunications services platform and collaborates with the service provider on service plans for contract cost and user pricing. The Department insources billing, and hardware management of the air card service, and provides the distribution channel for the vendor’s products and services (excluding air cards).

#### **Advantages**

- Continues current operating mode, practices, and service provisioning;
- Customers experience the same usage patterns and usage-based charging patterns as under current MCS contracts;
- Minimizes additional capital expenditures by DMS and MCS customers, since investment, capacity, and technology evolution are managed by the service provider;
- Customers experience the same billing and administration;
- Provides greater assurance of achieving required SLAs managed by selected service provider.

#### **Disadvantages or Potential Concerns**

- Reporting capabilities may be limited in information, which hampers DMS analysis on services.

#### **Risks**

- DMS identified no risk with this option.

### 5.3.3 Option 3 – Branded Reseller-MVNO

This option is a combination of insource/outsource functionality where DMS outsources the physical network, operations, and billing. In this model DMS acts as a branded reseller providing only a distribution channel for the vendor's products and services.

#### Advantages

- Customers experience the same usage patterns and usage-based charging patterns as under current MCS contracts
- Potential for lower overall pricing based on aggregation of usage and negotiation of commitment levels and pricing for tiered levels of utilization, similar to the mobile wireless data pricing model;
- Minimizes additional capital expenditures by DMS and MCS customers, since investment, capacity and technology evolution are managed by the service provider;
- Provides greater assurance of achieving required SLAs managed by selected service provider.

#### Disadvantages or Potential Concerns

- DMS would be required to create a process with the Vendor for the management of closed user groups.
- Customers have to review air card charges on their bill without DMS review.

#### Risks

- Since DMS would no longer control the service, there would be an implementation and transition risk when transitioning air card services.
- There is a potential security risk if DMS does not administer the air cards and the closed user groups.

## 5.4 Potential Performance Improvements/Service Features

The Department should consider the following service improvement and service features.

- Future contracts should continue to allow for evolution of service and equipment technology, enabling the contract to evolve with new technology.
- Future contracts should continue to allow platform flexibility, scalability, and support for industry standards, enabling a seamless integration of third-party technologies and applications.
- Future contracts should have higher statewide coverage through multiple carriers. Providers should offer multiple solutions, including equipment for coverage and building penetration. Equipment offerings for improving building penetration should be vendor neutral and at minimum to no cost for customers.
- Future contracts should require detailed reporting capabilities allowing DMS to evaluate the entire product and service offerings for future MCS platform evaluation.

- Future contracts should continue to require a combination of feature rich equipment and basic low-cost options and provide a comprehensive suite of enhanced services fulfilling the customer's diverse needs.
- Future service delivery should include voice services over Wi-Fi service connections.
- Future service delivery should have a consideration of technology evolutions in public safety communication services.
- Future service delivery should provide the capability for all aspects of the service to be partitioned to provide a scope-of-view and scope-of-command, allowing network administrators (user agents) to manage all their devices.
- Future contracts should include a high standard of measurable, achievable and motivational Service Level Agreements for DMS and its customers, supported by a tool set for monitoring service levels, and backed up by appropriate financial consequences.
- Future contracts should continue to require a waiver of vendor's service activation fees.
- Future contracts should provide for service plans for both work and personal accounts.
- Future contracts should provide discounts for volume purchases.
- Future contracts should allow for frequent equipment upgrades at minimal to no cost to customers.
- Future contracts should provide options for equipment and lower cost devices from emerging brands.
- Future contracts should increase the standard for operational support, achieving a world class standard of customer service delivery.
- Future contracts should increase the standard for equipment warranties, simplicity of repair, and replacement for faulty equipment.
- Future contracts should require detailed commitment on data utilization, allowing for limited and unlimited data, data limits, data throttling, waivers on data limits for Public Safety plans, and sharing data limits in aggregation across devices.

## **5.5 Cost Benefit Analysis for Each Option**

The Department of Management Services uses a margin percentage to markup costs from the MCS services provider and related ancillary service devices to recover internal DMS costs. The optional services and features of MCS are material to the financial analysis on a separate basis, and are not addressed as separate line items, but instead are included in service model revenues.

The financial analysis compares the options and provides financial metrics to determine which options will:

1. Maintain low costs for DMS in procuring and managing services;
2. Maintain low costs for agencies utilizing MCS; and
3. Provide the greatest benefit for the least cost.

The financial analysis included:

1. Revenue – both air card revenue and all other revenue

2. Direct Costs – direct costs of vendor payments for air cards, infrastructure adjustment, salary and benefits, data processing, and non-salary overhead.
3. Indirect Costs - included salaries and benefits, expenses, contracted services.
4. Net Revenue – includes potential rebates and other adjustments
5. Net Revenue, Post Rebate-Operations Balance – adjusted for customer rebates with a buffer for maintain operational payment and cost control

The analysis forecast the models with the cost recovery rate at either one, one and a half, two, or two and a half percent, which is adjusted in the net revenue with varying customer rebates. An operations revenue buffer of \$850,000 annually is assumed to be maintained for operational payment and cost control.

### **5.5.1 Financial Model Base Case**

This business case analysis first establishes a baseline of DMS' current business and financial environment for MCS, determined from historical business and financial data provided by DMS staff, including historical volumes, costs, revenues and vendor contracts. In modeling the various business case options, historical data was utilized to build an understanding of the fiscal flow of revenue and cost for the service. The model reviews the total volume, revenue, and cost for the services utilized by the agencies through this contract.

Service Forecasts were developed over the 10-year period from the date of MCS contract execution corresponding to fiscal year 2021-2022 through fiscal year 2031-2032, which includes a 5-year renewal period. Based on projections for DMS' MCS Services, direct and indirect costs were forecasted over the 10-year period. These projections were compared against the baseline scenario (which forecasted no changes to existing contracts, pricing, or DMS' business model) to determine the potential cost savings to DMS and to its customers. Options 2 and 3 were also compared against each other to determine which Option resulted in the lowest cost.

Over time, DMS may achieve cost savings to the state through migration and integration of newer technologies solution that achieve improved abilities to pass on reductions to the end customers.

### **5.5.2 Option 1 – Insource**

For reasons described Section 5.1.1 and 5.1.2, this option is not considered further in this business case.

### **5.5.3 Option 2 – Insource/Outsource (Second Brand/Hybrid Light MVNO)**

Option 2 represents the current MCS platform. DMS acts as a branded reseller for all products in the MCS platform except for air card services. For the air card services platform DMS provides customer support, billing, device management, distribution and sales. In the mobile communication market, DMS is acting a second brand or light mobile virtual network operator (MVNO) for air card, and as a “branded reseller MVNO” for all other equipment and services. This platform is an intermediate model between a branded reseller (Option 3) and a fully defined light MVNO. It allows control of distribution channels, increased level of control over back office processes, billing, device management, and value-added services definition and operations for

air card services. The current MCS platform manages many of these aspects as they relate to MCS air card services. Currently there are 7,956 air card devices that have been issued.

### 5.5.3.1 Technology Requirements

Option 2 envisions current technology requirements to remain the same as it is in the current contracts, however future contracts should allow for flexibility to allow for emerging technologies throughout the life of the contract. All MCS products and services are technically supported by the mobile communications provider except for air card services. Today air card services are supported by both the mobile communications provider and DST. Support regarding the air card device or service is handled by the mobile communications provider. Support for system configuration and closed user group access is provided by DST.

The current MCS contract addresses the following technical requirements.

- Voice Services
- Wireless Data Services
- Transmitted Data Security
- Closed User Group (Supported by DMS internally)
- State Provided IP Addresses (Public and Private)
- Wireless Device IP Routing Scheme
- Service Provider Furnished Public Routable IP Address Space
- Entity Specific Circuit
- Wireless Router and/or WWAN Modem
- Emergency Operations Features
- Security Feature Set
- Service Grade
- Authentication
- Activity User Log
- Text Message Service
- Message Logging
- Tracking Geographical Device Services
- Wireless Applications
- Voice and Data Coverage Maps
- Roaming
- Network Neutrality
- Priority Connection Services
- Applicable Test Plan
- Data Monitoring Suite
- Voice Monitoring Suite
- Voice Handheld Devices
- Minimum Technical Requirements
- Data Devices
- Text Devices
- Helpdesk Services

- Network Trouble Reporting
- Client Testing and Evaluation
- Operational and User Guides
- Escalation Requirements and Procedures
- Planned Outage Notification
- Unplanned Wireless Outage Notification
- Existing Wireless Data Customer Migration

### **5.5.3.2 Billing**

Option 2 envisions billing to remain the same as it is in the current state. All MCS products and services are directly billed from the mobile communications provider except for air card services. Today air card services are managed and billed within DST and this accounts for on average 385 invoices a month.

### **5.5.3.3 Customer Service**

Option 2 envisions customer service to remain the same as it is in the current state. All customer service needs related to MCS products and services are handled by the mobile communications provider except for air card services. Today select air card services are managed within DST. This select service is considered the closed user group and currently makes up 148 air card users. Support and maintenance of this user group service is handled by DMS internally.

### **5.5.3.4 DMS Role**

The DMS role will remain the same as it is in the current MCS platform. DST will continue to work with its MCS customers and service providers to provide the best mobile communications network.

### **5.5.3.5 Direct & Indirect Cost**

In addition to the Direct and Indirect Costs listed in Section 5.5 above, Option 2 envisions DMS staffing time for the air card billing process, in addition to the DMS staffing time required for contract management and monitoring that would be required for both 2 and 3.

### **5.5.3.6 Overall Cost**

To comply with the statutory requirement to “develop a system of equitable billings and charges for telecommunications services” stated in subsection 282.703(2), F.S., SUNCOM uses administrative cost recovery rates which are assessed for each SUNCOM service. Approximately 93.7 percent of SUNCOM’s costs are payments to contracted telecommunications vendors. The remaining 6.3 percent of SUNCOM’s costs are the costs of engineering, designing, procuring, ordering, installing, monitoring, auditing, invoicing, and managing these SUNCOM services. These support services are funded through the imposition of the administrative cost recovery rates, which are added to vendor charges for SUNCOM services. Some SUNCOM services bear more of these costs than others based upon the relative share of support service resources committed to sustaining the service, and so have a higher rate. The underlying goal of the cost recovery model is to ensure the solvency of the Communications Working Capital Trust Fund. Since 2012, the rate charged

to SUNCOM's Wireless Data Service customers have been between two and a half to three percent of the Customer's monthly invoice amount.

Quarterly, DivTel reviews a report showing the profitability of services based on service utilization and service costs. To address any inequity identified upon review of these figures, rate reductions and customer credits are used. A customer credit is a one-time liquidation of excess revenue without any associated rate reduction. Customer credits are issued to air card customers when a service achieves unanticipated excess revenue over expenses. Through customer credits, SUNCOM can ensure equitable billings without risking its ability to sustain a service over the longer term. The SUNCOM'S Wireless Data Service is a stable service with low overhead and air card customers have received customer credits over the years.

A reduction in the cost recovery rates associated with SUNCOM's telecommunications services results in recurring cost avoidance to the existing customers of the affected service. Such a reduction also represents costs avoided by future customers of the service. The recurring nature of the fiscal impact associated with a cost recovery rate reduction requires that adequate consideration be given to both existing and future market conditions associated with the SUNCOM service. With the maturity and growth of SUNCOM's Wireless Data Service, we are experiencing an increase in revenues.

#### **5.5.3.7 Potential Savings**

It is anticipated that over the life of the new MCS contract that cost avoidance will be achieved through leveraging State buying power and continuing to maintain lower costs than available commercially, including volume discounts, and the continued availability to the State of emerging and evolving technology surrounding mobile communications.

#### **5.5.3.8 Transition Costs/Considerations**

There are minimal transition cost risks considered in Option 2 as this option leaves MCS in its current state. Should the future procurement not result in a contract, or contracts, with one of the current incumbent providers, there may be costs associated with transition for end users with "locked" devices (devices that only work on a specific provider's network), along with DMS staff and customer time.

#### **5.5.3.9 Total Estimated Cost over 10 Years**

Overall Cost for Option 2 is expected to be \$36.7 million over the 10-year period from execution of the MCS contract in July 2020 through FY 2031-32.

#### **5.5.3.10 Risk Analysis**

Risk analysis of MCS platform remaining in its current state.

In maintaining the current model of multiple contracts for MCS with the possible entrance of new providers and new emerging technology may create significant risks and required efforts on both the enterprise and customer side. Some of the emerging technology may include 5G network and related technology offerings, emerging public safety integration, device transitioning, and future technological innovations.

The most significant risks and required efforts are on the customer side of transitioning to a new or different MCS platform. Each agency will be required to assess current capabilities and requirements for transition to a new or different MCS platform. Standards, methods, and practices for transition to a new or different MCS platform have been developed through experience by all large carriers who have accomplished this transition for other enterprise customers besides the State of Florida. Furthermore, some additional training of agency IT staff may be required, but it is anticipated that this can be provided over time.

Also, with this option the lack of visibility of detailed reporting information regarding customers, device type, usage of service type, plans and features, and other valuable informational data may not be consistently provided and reported. This reporting data is needed for future analysis of the MCS contract to ensure the most advantageous services and pricing for the State of Florida.

#### **5.5.3.11 Mitigation Plan**

Mitigation of negative consequences of MCS platform remaining in its current state is provided by the following factors:

1. The industry will be adapting to emerging technologies as the standard platform for mobile telecommunication services.
2. The current MCS business process and platform experience can be leveraged in any new technology and vendor transitions.
4. The onboarding process of a potential new MCS service provider is expected to occur over a fairly short time period.
5. The MCS business process would remain on an existing and operating network with which all users are familiar. Current users are familiar with the day to day operation of MCS.
6. Existing MCS contracts remain in place throughout the transition period.
7. Development and implementation of stringent SLAs to manage service provider's service performance, including technical, service delivery and financial requirements.

#### **5.5.3.12 Implementation Timeline for Option 2 & 3**

The schedule that, at a minimum, must be adhered to in order to achieve the estimated savings is indicated below in the MCS timeline, which has been combined for both Options 2 & 3 as they would be the same timeline projection. See Section 5.5.5 for the draft timeline.

#### **5.5.4 Option 3 – Insource/Outsource (Distribution Channel Only)**

This option represents the lightest MVNO business model, where DMS would only provide its distribution channel to the mobile network operator (MNO) while the MNO provides the rest of the business, from access network to the definition of the mobile service offer. This is the model that requires the lowest investment and overhead for DMS. However, most of the business services remain with the network provider. Therefore, this option provides very limited control of the business and value proposition of the service.

#### **5.5.4.1 Technology Requirements**

All technology responsibilities are outsourced to the mobile communications provider in Option 3. This includes all technology requirements as outlined in Option 2 and includes air card services.

#### **5.5.4.2 Billing**

All billing responsibilities are outsourced to the service provider in Option 3.

#### **5.5.4.3 Customer Service**

All customer service responsibilities are outsourced to the service provider in Option 3.

#### **5.5.4.4 DMS Role**

The DMS role in Option 3 is to only provide a distribution channel for the service provider.

#### **5.5.4.5 Direct & Indirect Cost**

In addition to the Direct and Indirect Costs listed in Section 5.5 above, Option 3 envisions 2 FTE for the management of the MCS contract and services.

#### **5.5.4.6 Overall Cost**

To comply with the statutory requirement to “develop a system of equitable billings and charges for telecommunications services” stated in subsection 282.703(2), F.S., SUNCOM uses administrative cost recovery rates assessed for each SUNCOM service. Approximately 93.7 percent of SUNCOM’s costs are payments to contracted telecommunications vendors. The remaining 6.3 percent of SUNCOM’s costs are the costs of engineering, designing, procuring, ordering, installing, monitoring, auditing, invoicing, and managing these SUNCOM services. These support service rates are funded through the imposition of the administrative cost recovery rates, which are added to vendor charges for SUNCOM services. Some SUNCOM services bear more of these costs than others based upon the relative share of support service resources committed to sustaining the service, and so have a higher rate. The underlying goal of the cost recovery model is to ensure the solvency of the Communications Working Capital Trust Fund. Since 2012, the rate charged to SUNCOM’s Wireless Data Service customers has been between two and a half to 3 percent.

Quarterly, DivTel reviews a report showing the profitability of services based on service utilization and service costs. In order to address any inequity identified upon review of these figures, rate reductions and customer credits are used. A customer credit is a one-time liquidation of excess revenue without any associated rate reduction. Customer credits are issued when a service achieves unanticipated excess revenue over expenses. Through customer credits, SUNCOM can ensure equitable billings without risking its ability to sustain a service over the longer term. The SUNCOM’S Wireless Data Service is a stable service with low overhead and has received customer credits over the years.

A reduction in the cost recovery rates associated with SUNCOM’s telecommunications services results in recurring cost avoidance to the existing customers of the affected service.

Such a reduction also represents costs avoided by future customers of the service. The recurring nature of the fiscal impact associated with a cost recovery rate reduction requires that adequate consideration be given to both existing and future market conditions associated with the SUNCOM service. With the maturity and growth of SUNCOM's Wireless Data Service, we are experiencing an increase in revenues.

#### **5.5.4.7 Potential Savings**

It is anticipated that over the life of the new MCS contract that cost savings will be achieved through leveraging State buying power realizing lower costs than available commercially, including volume discounts, and the continued availability to the State of emerging and evolving technology surrounding mobile communications.

#### **5.5.4.8 Transition Costs/Considerations**

There are minimal transition cost risks considered in Option 3 as this option leaves MCS in its current state with the exception of air cards, which become the responsibility of the service provider. Should the future procurement not result in a contract, or contracts, with one of the current incumbent providers, there may be costs associated with transition for end users with "locked" devices (devices that only work on a specific provider's network), along with DMS staff and customer time.

#### **5.5.4.9 Total Estimated Cost over 10 Years**

Overall Cost for Option 3 is expected to be \$36.7 million over the 10-year period from execution of the MCS contract in July 2020 through FY 2031-32. DMS's participation in administering air cards is an incidental cost and does not impact the overall cost for Option 3.

#### **5.5.4.10 Risk Analysis**

This paragraph presents a risk analysis of DMS providing only a distribution channel for MCS services and having the vendor manage the entire MNO value chain. The risk differential between Option 2 and 3 are minor.

The risks in Option 3 would encompass the risks outlined for Option 2 in Section 5.5.3.10, with the addition of migration of the closed user group (private network access to MyFloridaNet).

Also, with this option the lack of visibility of detailed reporting information is a risk. Data regarding customers, device type, usage of service type, plans and features, and other valuable informational data may not be consistently provided and reported. This reporting data is needed for future analysis of the MCS contract to ensure the most advantageous services and pricing for the State of Florida.

#### **5.5.4.11 Mitigation Plan**

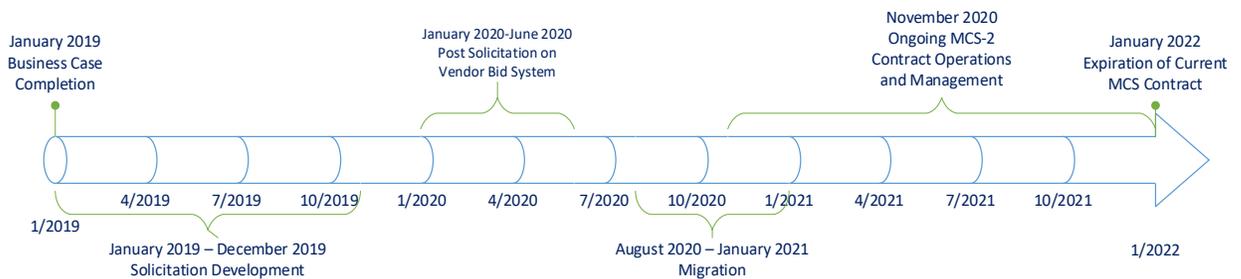
Mitigation of negative consequences of DMS providing only a distribution channel for MCS services and having the service provider manage the entire MNO would encompass the following:

1. Development and implementation of stringent SLAs to manage service provider’s service performance, including technical, service delivery and financial requirements.
2. Work with the service provider and required resources to implement, troubleshoot, manage, and monitor the transition of the closed user group air card services. This would include training and other oversight needed for successful migration.
3. Work with customers and required resources to manage the MCS transition, including training and other oversight.
4. The industry will be adapting to emerging technologies as the standard platform for MCS.
5. The current MCS business process and platform experience can be leveraged in any new technology and service provider transitions.
6. The onboarding process of a potential new MCS service provider is expected to occur over a fairly short time period.
7. The MCS business process would remain on an existing and operating network with which all customers are familiar. Current users are familiar with the day to day operation of MCS.
8. Existing MCS contracts remain in place throughout the transition period as an alternative.

**5.5.5 Implementation Timeline for Option 2 & 3**

The schedule that, at a minimum, must be adhered to in order to achieve the estimated savings as indicated below in the MCS timeline, which has been combined for both Options 2 & 3 as they would be the same timeline projection. The image below is a placeholder until final timeline is developed with Executive Leadership. Changes to this timeline are expected to have minimal impact on the estimated savings resulting from the execution of Contracts.

**Mobile Communication Services Draft Timeline**



- January 2019 Business case completion
- January 2019 – December 2019\* Solicitation development
- January 2020\* - June 2020\* Post solicitation on Vendor Bid System
- July 2020\* Sign contract
- August 2020\* - January 2021\* Migration
- November 2020 MCS-2 operations and management begins
- January 2022 Expiration of current MCS contract
- July 2025 Completion of the initial five-year term
- July 2030 Expiration of the MCS-2 contract, if renewed in full

*\*These dates are subject to change following internal review processes.*

## **6 Recommended Option & Detailed Discussion**

The recommended option for this portion of the business case is in accordance with Subsection 287.0571(4), F.S., which outlines the requirements for contracting with private sector vendors as they can effectively and efficiently provide services and reduce the cost of government. This statute requires analysis of feasibility, cost-effectiveness, and efficiency before proceeding with outsourcing of services.

A detailed analysis for this decision provides the following key findings:

1. An analysis of the mobile communications market concludes that the MCS platform being provided today is following the correct technological path in terms of capability and service delivery;
2. The MCS reporting and analysis information regarding device type, usage of service, and other data needs to be more detailed and provided to DMS on a monthly basis;
3. An MCS platform enables a connected enterprise characterized by access to people and information virtually anytime and anywhere for faster communication and greater collaboration using a variety of devices or mediums;
4. The mobile communications industry is ever evolving and with multiple providers instead of a single service provider approach, DMS is able to provide the customer with new technology at competitive pricing;
5. As the mobile communications market continues to evolve, review of SLA requirements will need to be a priority for DMS contract management to ensure MCS customers receive the best possible service solution;
6. Improved customer awareness of the capabilities of the service offering portfolio will extend the adoption of MCS to a broader customer base;
7. Innovative technology offerings to DMS customers will provide the opportunity for growth of the MCS platform;
8. The assumption of growth of MCS services will directly result in an increase for data consumption by all customer segments;
9. The telecommunication advancements in Public Safety are continuously evolving and creating new service offerings specific to Law Enforcement, EMS, and other First Responder networks.

## **6.1 Summary of the Three Options Considered in This Business Case**

In summary the three options considered for the next generation for Florida's mobile communications services platform are outlined below. The current services are provided by DMS, Verizon, AT&T, and Sprint.

The three options are:

1. Option 1 - Insourcing of Mobile Communications Services and support functions. For reasons described in Section 5.1.1 and 5.1.2, this option is not considered further in this business case.
2. Option 2 - Combination of Insourcing and Outsourcing (Current MCS Model) whereby DMS outsources all of the mobile telecommunication services except for the management, support, and billing of air card services.
3. Option 3 - Combination of Insourcing and Outsourcing whereby DMS outsources all of the mobile telecommunication services and acts only as a distribution channel for the service provider.

Each of these three options has been evaluated about the following attributes as supported by Section 5.6:

- Risks, disadvantages, pros and cons;
- Assumptions and constraints; and
- The schedule of key events.

## **6.2 Option 1 – Insource**

The Department of Management Services would request the establishment and funding for state FTE positions and physical assets to support mobile communication operations as appropriate. Upon approval, DMS would establish an internal mobile communications services organization composed of these full-time state employees based upon the choice of services to insource and outsource. These positions would be incorporated into the department's Legislative Budget Request (LBR) for funding each fiscal year. The level and appropriateness of outsourcing will be determined by what services are deemed attainable through state resources.

## **6.3 Option 2 – Combination Insourcing and Outsourcing (Current MCS Model)**

For this option, DMS would release an ITN to qualified vendors and negotiate a new contract for the identified MCS service features based upon existing mobile communications service portfolio, which includes Public Safety specific services, with consideration for emerging technology/capabilities. This option is predicated on DMS maintaining support and management of all air card services. This option is the current MCS platform. Option 2 – Combination Insource and Outsource, provides the low risk to the state while allowing competitive market

forces to keep the total cost of service delivery low. This option leverages DMS' existing staffing and service capabilities.

#### **6.4 Option 3 – Combination Insourcing and Outsourcing (Distribution Channel Only)**

For this option, DMS would release an ITN to qualified vendors and negotiate a new contract for the identified MCS service features based upon existing MCS portfolio, which includes Public Safety specific services, with consideration for emerging technology/capabilities. This option outsources all mobile communication services and operations to the service provide while DMS acts only as a distribution channel. Support for air card services would be maintained by DMS until adequate time has been provided for a migration of services to the provider. This option leverages DMS' existing staffing and service capabilities.

#### **6.5 Recommendation**

It is recommended that DMS issue a combination insourced and outsourced competitive procurement as an Invitation to Negotiate (ITN) as outlined by Option 2. This procurement should identify and incorporate the evolution of new mobile communication technologies and service offerings.

With the evolution of a Public Safety mobile communication network, consideration should be given to a multiple ITN approach.

### **7 Business Case Recommendations Summary**

The following section is provided as an overall summary of recommendations collected from throughout the business case. They represent key points that should be considered as DMS moves forward with its chosen path for MCS.

Recommendations include:

1. DMS issue a combination insourced and outsourced competitive procurement as an Invitation to Negotiate (ITN) to maintain its currently structured mobile communications services portfolio as outlined by Option 2.
2. The MCS solution should continue to allow for evolution of service and equipment technology, enabling the contract to evolve with new technology.
3. Internal support for closed user group should work with all providers to establish a private network access to MyFloridaNet.
4. Timely review of services and offerings which allows DMS to provide the most advanced mobile communication services. Market technology such as signal boosters and wearable technology are driving the need for data consumption and consumer demands.

5. Prioritize the review of current SLA requirements to ensure MCS customers are receiving the best possible service in a continuously evolving market.
6. DMS develop and implement SLAs that require consistent and timely reporting of device type, usage of service type, plans and features, and other valuable informational data is necessary. This reporting data is needed for service evaluation and monitoring, and future analysis of the Mobile Communication Services contract to ensure the most advantageous services and pricing for the State of Florida.
7. DMS maintain the necessary resources and support staff needed to manage the MCS air card users, closed user group, and its potential growth of new users. Service delivery for this offering must be managed end-to-end within the delivery configuration to ensure proper network administration is maintained. Further, all back-office functions (customer service requests and invoicing) must be properly maintained by DMS resources.
8. Create a report template to be distributed and used monthly by all contracted service providers to ensure consistency and ease of review.
9. DMS maintain the necessary resources and support staff needed for contract management and SLA monitoring to ensure proper service quality for the State of Florida.
10. Tiered or bulk pricing offerings should be explored.
11. The MCS procurement should have the goals of improved SLAs, improved reporting, and continued low pricing.

## 8 State Business Process & Policies

*Section 287.0571 (4)(i), F.S. A description of differences among current state agency policies and processes and, as appropriate, a discussion of options for or a plan to standardize, consolidate, or revise current policies and processes, if any, to reduce the customization of any proposed solution that would otherwise be required.*

In the context of the SUNCOM service portfolio, there are no impacts to existing state agency processes or policies that are not currently being managed effectively by DMS. The intended service delivery maintains a current steady state of services to all SUNCOM customers and as such the new MCS procurement does not present any additional burden on the state.

## 9 Performance Metrics Review

*Section 287.0571 (4) (j), F.S. A description of the specific performance standards that must, at a minimum, be met to ensure adequate performance.*

The current MCS contracts contain Service Level Agreements (SLAs). After review of these SLAs, the performance standards and measurements that should be met to ensure adequate performance includes:

Escalations – any future contract(s) should continue to require escalation procedures to maintain a high level of customer service to Customers.

Migration – any future contract(s) should continue to require migrations be completed within 120 days of Contract execution to maintain a high level of customer service to Customers, and a robust standard of project management.

Maintenance – any future contract(s) should continue to require notification for planned and unplanned maintenance that could affect service delivery to maintain a high level of customer service to Customers.

Appliance Failover – any future contract(s) should continue to require rapid failover to the secondary IPsec Virtual Private Network (VPN) appliance to maintain connectivity to MFN.

In addition to current SLAs, the following recommended performance standards will ensure adequate performance:

Contractor Staffing – any future contract(s) should ensure that key staffing positions are filled with personnel with the appropriate experience and qualifications with remedies for identified deficiencies.

Contractor meetings – any future contract(s) should ensure that the Department is able to adequately monitor the contracts. Ongoing operational and topic specific meetings are an appropriate tool to assist with such monitoring.

Project Management – any future contract(s) should ensure that the Department is able to adequately monitor the transition from current to future contracts. The transition should be conducted in an optimal way to achieve the standards of transition.

Billing and Reporting – any future contract(s) should ensure that the Department is able to receive invoices, credits, and reporting on cost recovery and direct billed accounts in a timely manner with all required information. Additionally, future contract(s) should require Public Safety specific reporting on Customer utilization.

Public Safety – any future contract(s) that offer public safety specific options should require a high standard of coverage across the State, compliance with industry standards for Public Safety LTE communication, and offer deployable technologies for emergency situations. Additionally, the future contract(s) should ensure Public Safety Customers have local control to enact priority and preemption of their service, a local control portal, and Public Safety specific customer support.

## 10 Projected Timeframe

*Section 287.0571 (4)(k), F.S. The projected timeframe for key events from the beginning of the procurement process through the expiration of a contract.*

The MCS procurement to contract expiration timeline is suggested to be established for five years, with a renewal/evaluation interval at year five, at which time new negotiations for service features and reduced pricing should take place. This contract should be put in place prior to the expiration of existing MCS contracts to allow for any migration of services needs to be met with a new portfolio of services.

See 5.5.5 for the presentation of the projected timeline and key events.

## 11 Public Records Compliance

*Section 287.0571 (4) (l), F.S. A plan to ensure compliance with the public records law.*

The procurement and a subsequent awarded contract should state that any and all records produced are subject to Ch. 119, Florida Statutes. The service provider shall allow DMS access to all documents, papers, letters, or other material subject to Ch. 119, Florida Statutes for which public record requests are made or received by the department.

## 12 Contingency Plan

*Section 287.0571 (4) (m), F.S. A specific and feasible contingency plan addressing contractor nonperformance and a description of the tasks involved in and costs required for its implementation.*

Using multiple providers as a strategy to achieve maximum coverage also minimizes the need for contingency planning related to contractor nonperformance. Having multiple contracts facilitates end-users discontinuing services from a nonperforming provider. DMS anticipates continuing its contract strategy where there are no term commitments for devices, therefore any costs related to Contractor nonperformance would be limited to the cost of moving any locked phones for one provider to another.

Future contracts should maintain provisions to address the termination for cause in the event of non-performance by the Contractor and remedies for non-performance consistent with those available in rule 60A- 1.006, F.A.C.

DMS should include SLAs in the contract in the event the service provider does not meet established performance expectations. The SLAs should provide incentive for a contractor to cure problems with performance before an event of default occurs.

Suggested Remedies for DMS for Default and Obligations upon Termination:

- Terminate the contract by providing the service provider with appropriate written notice of the effective date of termination;
- Seek equitable relief and/or institute legal proceedings against the service provider to collect payment of any money owed including, but not limited to, re-procurement costs, system replacement costs, and liquidated damages; and initiate proceedings to have service provider placed on the Suspended Vendor

list;

- Once placed on the Suspended Vendor list, state agencies will be advised not to do business with the service provider without written approval from State Purchasing until the state receives reimbursement for all re-procurement costs.

Recommended Termination Assistance Services:

- Service provider must cooperate fully with DMS and any new service provider;
- All processes and procedures performed by the service provider must be explained and appropriate documentation provided for each service layer under contract;
- Answer questions related to the migration and transition of services; and
- Termination assistance services rendered prior to the termination date of the contract will be at no additional cost to DMS. Services rendered after termination of the contract will be at a reasonable rate.

### 13 Transition Plan

*Section 287.0571 (4) (n), F.S. A state agency's transition plan for addressing changes in the number of agency personnel, affected business processes, employee transition issues, and communication with affected stakeholders, such as agency clients and the public. The transition plan must contain a reemployment and retraining assistance plan for employees who are not retained by the state agency or employed by the contractor.*

Subsection 287.0571(4)(n), F.S., requires a business case to address issues that may arise when work currently being done by state employees is transferred to a contractor. There is no expectation of a need to reemploy or retrain agency personnel. The DMS staff that perform services related to MCS are expected to not have changes to their roles under Option 2. Therefore, utilizing Option 2 does not require reemployment or retraining assistance and no transition plans for employees are necessary.

### 14 American With Disabilities Act Of 1990, As Amended

*Section 287.0571 (4) (o)F. S. A plan for ensuring access by persons with disabilities in compliance with applicable state and federal law.*

The Americans with Disabilities Act (ADA) prohibits discrimination on the basis of disability in employment, state and local government, public accommodations, commercial facilities, transportation, and telecommunications. To ensure that the service provider is compliant with state and Federal ADA laws, the procurement should request that the service provider outline a plan to identify and address any ADA concerns. Future contracts should include the requirement to comply with the provisions in Part II of Chapter 282, Florida Statutes, specifically relating to accessibility of information and technology for those with disabilities.

## **15 Contract Provisions**

This business case does not address specifics of the contract provisions as set forth in section 287.0571(5), F.S., as they will be fully defined in the ITN. The ITN will take into consideration all other sections of the business case to aid in the development of the contract language as appropriate.



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

Ron DeSantis, Governor  
Jonathan R. Satter, Secretary

**ITN No.: DMS-19/20-006**  
**Attachment E – Definitions and Acronyms**

All personal pronouns used in the Contract, whether used in the masculine, feminine, or gender-neutral, shall include all other genders; the singular shall include the plural; and the plural shall include the singular. The following definitions and acronyms apply to the Contract in addition to the definitions in Chapter 287, Florida Statutes (F.S.), and Rule Chapter 60FF-1, Florida Administrative Code (F.A.C.). In the event of a conflict, the definitions provided in this document will prevail.

Access	When capitalized, this means review, inspect, transmit, approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any State Data, regardless of type, form, or nature of storage; Access to a computer system or network includes local and remote access.
Business Days	Monday, Tuesday, Wednesday, Thursday, and Friday, excluding weekends and State paid holidays as set forth in section 110.117, F.S.
Contractor	The Responsive and Responsible Respondent(s), awarded a Contract, if any, pursuant to this ITN. This definition supersedes the definition in section 287.012(7), F.S.
CPNI	Customer Proprietary Network Information. The definition of CPNI is the Title 47 U.S. Code § 222(h) (2019) definition.
CRR	Cost Recovery Rate. The Department's monthly cost recovery charge applied to Customer invoices.
CSAB	Communications Service Authorization and Billing system. <a href="https://portal.suncom.myflorida.com/start/#/login">https://portal.suncom.myflorida.com/start/#/login</a>
Customers	The entities that are provided services under this Contract, including State agencies, which are required to use the SUNCOM Network, and other entities authorized to use the SUNCOM Network in accordance with Chapter 282, F.S.
End-user	The individual that utilizes the device that consumes the resources defined by the monthly plan. The End-user's employer is the Customer.
EUPL	End User Price List
HA/HR	Highly-available and Highly-reliable. Systems, services, and implementations designed to eliminate planned downtime and prevent unplanned downtime; methods utilize specific hardware, software, and processes; typically implemented in mission critical services.
IP	Internet Protocol
IPsec	An Internet Engineering Task Force standard. Text from RFC 4301 - IPsec creates a boundary, between unprotected and protected interfaces, for a host or a network. Traffic traversing the boundary is subject to the access controls specified by the user or administrator responsible for the IPsec configuration.

**ITN No.: DMS-19/20-006**  
**Attachment E – Definitions and Acronyms**

IPsec Tunnel	Tunnels are a design technique utilized by telecommunications service providers to manage traffic. IPsec tunnels are used to create closed user groups to enforce segregation of traffic. IPsec tunnels are a specific type of tunnel which provides security services for IP packets through encryption, authentication, and protection against replay.
MFN	MyFloridaNet
OEU	Other Eligible Users. The entities provided services under this Contract that are not State agencies and are not required to use the SUNCOM Network but are otherwise authorized to use the SUNCOM Network in accordance with Chapter 282, F.S. These include, but are not limited to, political subdivisions of the State, including counties, municipalities, school districts, and water management districts. Also included are, private nonprofit elementary and secondary schools conditioned upon certain requirements, universities, libraries of community colleges, and nonprofit corporations.
Person	When capitalized in Sections 9 and 13 of Attachment B, Draft Contract, this means the Contractor's employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other person operating under the Contractor's direction with Access to State Data or who enters either the premises or facilities where State Data is stored or accessible.
Reply	A formal response to this ITN.
Respondent	An entity that submits a Reply to this ITN.
SLA	Service Level Agreement
SLA Clock	Service Level Agreement Clock. The SLA clock refers to how a deliverable will be measured in terms of time for completion as stated in the particular SLA.
SNMP	Simple Network Management Protocol
State	The State of Florida
State Data	All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received by the Contractor in its performance under this Contract.
Subcontractor	A third party performing work under the Contract at the direction of the Contractor, including affiliates, partners, teammates, and all other third-party vendors.
VPN Concentrator	Virtual Private Network Concentrator. A device, or collection of devices, built to manage secure connections within or between infrastructures.
VRF	Virtual Routing and Forwarding
WDS	Wireless Data Service
WVS	Wireless Voice Service



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

**Ron DeSantis, Governor**  
Jonathan R. Satter, Secretary

**Addendum No. 1 to the following Invitation to Negotiate (ITN):**

**Mobile Communication Services**

**DMS-20/21-006**

Date: November 9, 2020

To: Prospective Respondents to ITN No.: DMS-20/21-006

From: Caitlen Boles, Procurement Officer

Subject: Timeline Update

1. ITN No: DMS-20/21-006, subsection 1.8, Timeline of Events, the table is hereby amended as follows:

<b>TIMELINE OF EVENTS</b>		
<b>Events</b>	<b>Event Time (ET)</b>	<b>Event Date</b>
ITN posted on the VBS.		October 7, 2020
Deadline to submit questions to the Procurement Officer.	3:00 PM	October 28, 2020
Department's anticipated posting of answers to Respondent's questions on the VBS.		<del>November 9, 2020</del> <b>November 16, 2020</b>
Deadline to submit Reply and all required documents to the Procurement Officer.	2:00 PM	<del>November 23, 2020</del> <b>November 30, 2020</b>
Public Opening. Conference Room 101 4050 Esplanade Way Tallahassee, Florida 32399-0950  <b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/198062149">https://global.gotomeeting.com/join/198062149</a>	3:00 PM	<del>November 23, 2020</del> <b>November 30, 2020</b>

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
<p><b>You can also dial in using your phone.</b>            United States (Toll Free): <u>1 877 309 2073</u>            United States: <u>+1 (646) 749-3129</u></p> <p><b>Access Code:</b> 198-062-149</p> <p><b>Join from a video-conferencing room or system.</b>            Dial in or type: 67.217.95.2 or inroomlink.goto.com            Meeting ID: 198 062 149            Or dial directly: 198062149@67.217.95.2 or 67.217.95.2##198062149</p> <p>New to GoToMeeting? Get the app now and be ready when your first meeting starts:  <a href="https://global.gotomeeting.com/install/198062149">https://global.gotomeeting.com/install/198062149</a></p>		
Anticipated Evaluations Phase.		December 1, 2020 <b>December 4, 2020</b> to December 30, 2020
Anticipated Negotiations Phase.		January 4, 2021 to April 12, 2021
<p>Negotiation Team Public Meeting            Conference Room 101            4050 Esplanade Way</p> <p><b>Please join my meeting from your computer, tablet or smartphone.</b>  <a href="https://global.gotomeeting.com/join/432429477">https://global.gotomeeting.com/join/432429477</a></p> <p><b>You can also dial in using your phone.</b>            United States (Toll Free): <u>1 877 309 2073</u>            United States: <u>+1 (646) 749-3129</u></p> <p><b>Access Code:</b> 432-429-477</p> <p><b>Join from a video-conferencing room or system.</b>            Dial in or type: 67.217.95.2 or inroomlink.goto.com            Meeting ID: 432 429 477            Or dial directly: 432429477@67.217.95.2 or 67.217.95.2##432429477</p> <p>New to GoToMeeting? Get the app now and be ready when your first meeting starts:  <a href="https://global.gotomeeting.com/install/432429477">https://global.gotomeeting.com/install/432429477</a></p>	10:00 AM	April 19, 2021

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
Anticipated date to post Notice of Intent to Award on the VBS.		April 26, 2021
Anticipated Contract Execution.		May 2021

**FAILURE TO FILE A PROTEST WITHIN THE TIME PRESCRIBED IN SECTION 120.57(3), FLORIDA STATUTES, OR FAILURE TO POST THE BOND OR OTHER SECURITY REQUIRED BY LAW WITHIN THE TIME ALLOWED FOR FILING A BOND SHALL CONSTITUTE A WAIVER OF PROCEEDINGS UNDER CHAPTER 120, FLORIDA STATUTES.**

Any protest concerning this agency decision or intended decision must be timely filed with the Agency Clerk. Protests may be filed by courier, hand delivery, or U.S. mail at Department of Management Services, Office of the General Counsel, Attention: Agency Clerk, 4050 Esplanade Way, Suite 160, Tallahassee, FL 32399-0950. Protests may also be filed by fax to 850-922-6312, or by email to [agencyclerk@dms.fl.gov](mailto:agencyclerk@dms.fl.gov). It is the filing party's responsibility to meet all filing deadlines.



4050 Esplanade Way  
Tallahassee, FL 32399-0950

Ron DeSantis, Governor  
Jonathan R. Satter, Secretary

**Addendum No. 2 to the following Invitation to Negotiate (ITN):**

**Mobile Communication Services**

**DMS-19/20-006**

Date: November 16, 2020  
To: Prospective Respondents to ITN No: DMS-19/20-006  
From: Caitlen Boles, Procurement Officer  
Subject: Respondent Questions and Department Answers

---

ITN No: DMS-19/20-006, is hereby amended as follows (deletions are shown by strikethrough and additions are underlined):

1. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 3.3.1, the third sentence, is hereby amended as follows:

For closed user groups, the Contractor must configure both 1) public IP addresses owned by the State and Other Eligible Users and 2) private IP addresses furnished by the State DMS and Other Eligible Users.

2. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 3.9, paragraph 2, is hereby amended as follows:

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.

3. ITN No: DMS-19/20-006, Attachment A: Statement of Work, section 3.12, paragraph 4, is hereby amended as follows:

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

4. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 3.14.3, paragraph 3, is hereby amended as follows:

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 type requested) 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.

5. ITN No: DMS-19/20-006, Attachment A: Statement of Work, section 3.17.1.e, is hereby amended as follows:

e. ~~Maintenance~~ Notifications, SLA B7, B8, B9 (Subsections 3.19.4)

6. ITN No: DMS-19/20-006, Attachment A: Statement of Work, section 3.19.4, is hereby deleted in its entirety and replaced as follows:

4. Notifications. Electronic notifications are required during instances of significant service impact, including performance degradation, over a generalized area. **Attachment C, SLA-B7.** Electronic notifications are required in advance of maintenance activities when the activity may cause a significant service impact, including performance degradation, over a generalized area. Notifications must include an impact statement, date, time, and estimated duration of the service impact. **Attachment C, SLA-B8 and SLA-B9.**

7. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 3.23.1, is hereby amended as follows:

1. Provide all reporting activities listed in SOW subsection 3.26.5, Project Management – Implementation Plan and Customer Specific Migration Plans 3.27.5(1)(b) and SOW subsection 3.27.5(1)(c).

8. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 3.26.3, is hereby amended as follows:

The Contractor shall create the following two (2) 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 one (1) 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 one (1) 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.

9. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 4.5, is hereby amended as follows:

DMS Demonstration Devices. Upon DMS request, in addition to any other test devices required by this SOW, the Contractor shall provide up to ten (10) wireless demonstration public safety devices ~~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 thirty (30) ~~sixty (60)~~ Business Days. Any demonstration equipment, forms, and processes shall be provided, managed, and maintained by the Contractor.

Customer Demonstration Devices. The number of demonstration public safety devices the Contractor elects to provide to Customers is at the discretion of the Contractor. The Contractor will coordinate directly with any other Customer ~~State agencies~~ regarding public safety service demonstration equipment, notifying the Department in advance of these activities.

10. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 5.8, Work Orders, is hereby amended to delete the following:

**Attachment C, SLA-G1.**

11. ITN No: DMS-19/20-006, Attachment A: Statement of Work, subsection 5.10, Invoicing Requirements, is hereby amended as follows:

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. **Attachment C, SLA-F2.** Both the handbill and electronic files for the CSAB portion must be received no later than the 10th calendar day of each month.

12. ITN No: DMS-19/20-006, Attachment A: Statement of Work, Section 5.12, Audit of Contractor Invoices, is hereby amended with the following text added:

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 two (2) one (1) billing cycles from receipt of dispute. If Contractor has not resolved audit exceptions within two (2) one (1) billing cycles, the charges will be adjusted as determined by DMS.

13. ITN No: DMS-19/20-006, Attachment A: Statement of Work, Section 6.6, Customers Liability is hereby amended with the following text added:

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

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK**

14. ITN No: DMS-19/20-006, Attachment C: Service Level Agreements, SLA-B7, SLA-G2, and SLA-G3 are hereby amended as follows:

Service Category	SLA Number	Deliverable Title	Performance Metric	Financial Consequence	Additional SLA Clock Information
Services and Devices for Mobile Communication Services	SLA-B7	Notification, Significant Service Impact <del>Planned</del> Maintenance	Notification of <u>significant service impact received one (1) hour after beginning of impact, in accordance with SOW subsection 3.19.4 and section 4.</u> <del>received two (2) Business Days prior to any planned maintenance, in accordance with SOW subsection 3.20.4 and section 4</del>	\$2,500 per failure to notify	The SLA is measured by the Contractor's logs and emails.  The SLA applies automatically <u>one (1) hour after the determination of significant service impact, two (2) Business Days prior to any planned maintenance for which notice is not provided.</u>
Direct Ordering and Billing	SLA-G2	Direct-Billed Accounts Monthly Report	A Direct-Billed Accounts Monthly Report will be provided no later than the <u>30<sup>th</sup> 15<sup>th</sup></u> of the month on all direct-billed accounts, in accordance with SOW subsection 6.4	\$1,000 per day	
Direct Ordering and Billing	SLA-G3	Direct-Billed Accounts Quarterly Report	A Direct-Billed Accounts Quarterly Report will be provided no later than the <u>30<sup>th</sup> 15<sup>th</sup></u> of the month on all direct-billed accounts, in accordance with SOW subsection 6.5	\$1,000 per day	

**Enclosure:**  
Questions and Answers

**FAILURE TO FILE A PROTEST WITHIN THE TIME PRESCRIBED IN SECTION 120.57(3), FLORIDA STATUTES, OR FAILURE TO POST THE BOND OR OTHER SECURITY REQUIRED BY LAW WITHIN THE TIME ALLOWED FOR FILING A BOND SHALL CONSTITUTE A WAIVER OF PROCEEDINGS UNDER CHAPTER 120, FLORIDA STATUTES.**

Any protest concerning this agency decision or intended decision must be timely filed with the Agency Clerk. Protests may be filed by courier, hand delivery, or U.S. mail at Department of Management Services, Office of the General Counsel, Attention: Agency Clerk, 4050 Esplanade Way, Suite 160, Tallahassee, FL 32399-0950. Protests may also be filed by fax to 850-922-6312, or by email to [agencyclerk@dms.fl.gov](mailto:agencyclerk@dms.fl.gov). It is the filing party's responsibility to meet all filing deadlines.

**Invitation to Negotiate  
Mobile Communication Services  
ITN No. DMS-19/20-006  
Questions and Answers**

The Department's answers to timely submitted questions are below.

Question Number	Section	Page Number	Question	Answer
1	ITN, 3.6.1	12	<p>We are in the telecommunications business and have the ability to provide cellular voice, data and sms services as required by this ITN.</p> <p>Section 3.6.1 requires minimum compliance with "Consolidated Communications Marketplace Report – 2018, paragraph 6, page 4, and paragraph 44, page 37, is presumed to meet this coverage requirement."</p> <p>This renders this ITN open to only AT&amp;T, T-Mobile and Verizon.</p> <p>Am I reading this correctly?</p>	<p>No. Please see the entirety of ITN Section 3.6.1, including:</p> <p>"A Respondent not listed in the above-mentioned FCC report as a nationwide service provider must submit documentation showing that it has been independently verified by a government entity as meeting these coverage requirements."</p>
2	N/A	N/A	Would it be possible to supply the SOW and required forms in Microsoft Word format for recently released ITN # DMS-19/20-006?	Vendors may contact the Procurement Officer in writing via email to request Attachment A, Statement of Work (SOW), in Microsoft Word format. Only the SOW will be provided in Microsoft Word format.
3	N/A	N/A	Would the State please provide a word version of each ITN document?	Please see Answer No. 2.
4	ITN, 1.3	4	When will the new agreement commence – May 2021 or after expiration of existing agreement?	The anticipated contract execution date is May 2021 to allow time for migration to new Contract(s), if awarded.
5	ITN, 1.3	4	Will the agreements run concurrently?	Yes. The Department expects any Contracts entered into as a result of this ITN to be concurrent.
6	ITN, 1.8	5	Will the State please consider extending the final deadline one month due to the complexity of the RFP?	No.

Question Number	Section	Page Number	Question	Answer
7	ITN, 1.8	6	Will the State provide answers to Respondents questions as available (before 11/9)? Respondents would like answers ASAP to confirm about ability to support requirements.	These answers to Respondent's timely submitted questions are being posted in accordance with Section 1.8, Timeline of Events, of the ITN.
8	Attachment A – Statement of Work	N/A	For requirements that do not allow comment, how should Respondents provide clarifications regarding our ability to support the request?	See ITN section 4.4, Negotiations.  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
9	Attachment A – Statement of Work: 4.4 & 4.8	54-55	Requirement 4.4 only references 3GPP and does not synch with 4.8 NPSTC standards. Does the State require Respondents to certify NPSTC compliance prior to (or during) the proposal stage?	Subsection 4.4 requires public safety service plans and devices to adhere to the 3GPP standard. Subsection 4.8 requires the Contractor to demonstrate that a PTT device or service adheres to the NPSTC standard before it can be advertised or marketed as 'mission critical.'  Respondents are not required to certify NPSTC compliance in their Replies.
10	Attachment A – Statement of Work & Attachment C – Service Level Agreements	SLA-F2	Please confirm which requirement SLA-F2 applies.	SLA-F2 applies to SOW subsection 5.10.  Please see Section 11 of Addendum No. 2.
11	Attachment A – Statement of Work & Attachment C – Service Level Agreements	SLA-G1	Please confirm SLA-G1 applies to 6.2 (not 5.8).	Confirmed, SLA-G1 applies to SOW subsection 6.2.  Please see Section 10 of Addendum No. 2.
12	Attachment A – Statement of Work: 5.8	60	Does 5.8 Work Orders have an associated SLA? If yes, please confirm SLA#.	No.
13	ITN, 3.6.1	12	The State of Florida's minimum qualification requirement for 3.6.1, for being a facilities-based mobile wireless service provider with a network that covers at least 90% of the nation's non-rural population, significantly limits competition. Many potential bidders, who have proven their ability to	Section 3.6.1 will remain the same.

Question Number	Section	Page Number	Question	Answer
			add value to large enterprise and Government customers, do not have the proper FCC certifications. <b>We are a facilities based network provider with POPs all over the country and we have relationships with all major wireless providers which gives us carrier-agnostic wireless coverage of well over 90% of the nation's non-rural population.</b> We believe <b>there are additional companies</b> that can add significant value that may not have proof of the volume of coverage. Can the State of Florida revise this requirements to be less restrictive to encourage more competition?	
14	N/A	N/A	Would D.M.S. accept responses from a Mobile Virtual Network Operator (MVNOs) if it creates more competition amongst all of the respondents and ultimately better competitively priced services for SUNCOM customers?	Mobile Virtual Network Operators (MVNOs) are not precluded from submitting a Reply.  The Department interprets facilities-based mobile wireless service providers for the purpose of this procurement to include vendors that provide the services using their own network facilities and spectrum for which it holds a license, manages, or for which it has obtained the right to use via a spectrum leasing arrangement.
15	Attachment A – Statement of Work: 1.1.5 & 4.2		Under sections 1.1.5 and 4.2 which center around public safety. Would D.M.S. disqualify vendors who don't have access to Firstnet and other Wireless Priority Access on smartphones or is this an optional subsection that would only apply to Suncom customers in the area of Public Safety?	No. Section 4.2 is optional. Providing public safety specific devices, as referenced in section 1.1.5, is optional.
16	3.18	35	What is the maximum SLA penalty that can be applied in any given month? Maximum CAP?	There is no cap on the amount of SLAs that may be applied in a given month.
17	3.18.5	36	What will serve as validation for the contractor that this report was received on time by DMS?	The Contract does not specify how receipt of this report will be acknowledged. However, as stated in Section 4.4.1, Negotiations Process – General

Question Number	Section	Page Number	Question	Answer
				Overview, “[t]he Department reserves the right to negotiate different terms, additional terms, and related price adjustments if the Department determines that such changes would provide the best value to the State. Additional operational requirements may be defined and clarifications required.
18	3.19.1	37	What will serve as validation for the contractor that this report was received on time by DMS?	The Contract does not specify how receipt of this report will be acknowledged. However, as stated in Section 4.4.1, Negotiations Process – General Overview, “[t]he Department reserves the right to negotiate different terms, additional terms, and related price adjustments if the Department determines that such changes would provide the best value to the State. Additional operational requirements may be defined and clarifications required.
19	3.19.4	37	What will serve as validation for the contractor that this message was received on time by DMS?	The Contract does not specify how receipt of this report will be acknowledged. However, as stated in Section 4.4.1, Negotiations Process – General Overview, “[t]he Department reserves the right to negotiate different terms, additional terms, and related price adjustments if the Department determines that such changes would provide the best value to the State. Additional operational requirements may be defined and clarifications required.
20	3.19.4	37	How will discrepancies between Contractors time stamping and DMS time stamping be resolved?	The Contract does not specify how receipt of this report will be acknowledged. However, as stated in Section 4.4.1, Negotiations Process – General Overview, “[t]he Department reserves the right to negotiate different terms, additional terms, and related price adjustments if the Department determines that such changes would provide the best value to the State. Additional operational requirements may be defined and clarifications required.

Question Number	Section	Page Number	Question	Answer
21	2	4	In ATTACHMENT B - DRAFT CONTRACT, the "Contract and Documents Hierarchy" is not consistent with the actual ITN Attachments A through E. For example, Section 2 (1-7) identifies Attachment A as "Definitions and Acronyms" whereas, it is Attachment E in the ITN Attachments. It also refers to Attachment C as "Contractor's Pricing" with three Exhibits whereas Attachment C is "Service Level Agreements" in the ITN documents. Please provide further clarification.	Section 2, Contract Documents and Hierarchy, of the Draft Contract specifies the order of precedence for the resulting Contract(s), if any. The documents are not intended to match the ITN attachments and are updated prior to Contract execution to follow the typical naming convention (e.g., A, B, C, etc.).
22	6.6	65	The document indicates that there are 66 total pages but there are only 65 pages provided in Attachment A. Is there a missing page?	This is a clerical error and Attachment A: Statement of Work should read 65 pages.
23	6.6	65	There are no instructions at the end of Section 6 "Direct Ordering and Billing". Did The State intend to include specific instructions or a "Read, understands, and will comply" statement at the end of the section?	Please see Section 13 of Addendum No. 2.
24	1.8	6	In ITN Document, under the "Timeline of Events", the respondent requests a two month extension to January 29, 2021 based on holiday staffing issues.	No.
25	4.5	54	What is the limit on the number of device demos required? Currently, the Vendor is contracted for up to 10 demo devices.	Please see Section 9 of Addendum No. 2.
26	4.8	55	Does the statement; "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." include the statements 3GPP MCPTT compliant?	3GPP MCPTT compliance is not required for NPSTC compliance, but the Department reserves the right to discuss additional compliance requirements during negotiations in accordance with ITN section 4.4, Negotiations.

Question Number	Section	Page Number	Question	Answer
27	4.8	55	Does the reference to "the Department" refer to NPSTC or State of Florida DMS?	State of Florida, DMS
28	4.8	55	Please confirm that is the correct use for compliance testing. <a href="https://www.npstc.org/documents/Functional%20Description%20MCV%20v5.doc">https://www.npstc.org/documents/Functional%20Description%20MCV%20v5.doc</a> - Included In Question Attachment 1 - Question Attachment 1 - Mission Critical Voice Communications	Confirmed.
29	ITN, 1.8	5	Will the State please consider extending the deadline for questions two weeks due to the complexity of the RFP?	No.
30	ITN, 1.8	5	Will Respondents be able to ask follow-up questions on the complete Respondent answers scheduled to be release on 11/9?	No. Respondents invited to participate in negotiations will be permitted to ask additional questions during the negotiations phase.
31	Attachment A – Statement of Work, 2	13-16	Will the State agree to add "or equivalent experience" to each Key Staff Position descriptions as follows:  The (POSITION) shall possess the following minimum qualifications, <u>or equivalent experience</u> :  2.2 Key Staff Position - Account Manager 2.3 Key Staff Position - Project Manager 2.4 Key Staff Position - Business Operations Manager 2.5 Key Staff Position - Engineering and Design Manager 2.6 Key Staff Position - Operations and Security Manager	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.

Question Number	Section	Page Number	Question	Answer
32	Attachment A – Statement of Work, 2	13	<p>Will the State agree to modify the language “The (POSITION) or designated backup(s) must be available twenty-four (24) hours a day, 365 days of the year” to state the following: <u>“24x7x365 support will be available through a Care team.”</u></p> <p>Key staff may not be available 24/7/365 but Contract will provide this level of support through its Care team.</p>	<p>See ITN section 4.4, Negotiations,</p> <p>However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.</p>
33	Attachment A – Statement of Work, 2.3	14	<p>Will the State agree to remove minimum qualification #5 from Section 2.3 Key Staff Position - Project Manager? While the Respondent will agree to meet all other qualifications for this Key Staff Position, it is respectfully requested that the certification requirement be removed to allow more flexibility in staffing.</p>	<p>See ITN section 4.4, Negotiations,</p> <p>However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.</p>
34	Attachment A – Statement of Work, 3.3	18	<p>Please confirm the CSAB portal services are only available to State agencies on one centralized DMS account?</p>	<p>The CSAB portal and its functionality is available to all Customers; both State agencies and OEUs.</p>
35	Attachment A – Statement of Work, 3.3	18	<p>Will the State agree to modify this sentence in Section 3.3 to delete the phrase “owned by the State and Other Eligible Users” and replace the language with “public IP address owned by Contractor”?</p> <p>The revised language would read as follows: “The Contractor must configure both 1) public IP addresses owned by Contractor <del>the State and Other Eligible Users</del> and 2) private IP addresses furnished by DMS and Other Eligible Users.</p>	<p>Please see Section 1 of Addendum No. 2.</p>
36	Attachment A – Statement of Work, 3.4	19	<p>Please confirm OEU’s are not permitted to order and bill through their own instance in the-CSAB portal.</p>	<p>The CSAB portal and its functionality is available to all Customers; both State agencies and OEUs.</p>

Question Number	Section	Page Number	Question	Answer
37	Attachment A – Statement of Work, 3.5	20	What are the Direct-Billed OEU's permitted to do and/or order within the State CSAB?	OEU's are not restricted from ordering from the CSAB portal, its functionality is available to all Customers. This can be further discussed in negotiations.
38	Attachment A – Statement of Work, 3.6	24	Please confirm the State will continue to own and maintain all of the MFN equipment and circuitry.	Confirmed.
39	Attachment A – Statement of Work, 3.6	24	Please confirm the Respondent will maintain equipment and capacity on the Respondent side.	<p>Please see subsection 3.6 (page 21). "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."</p> <p>Please see subsection 3.15 (page 33). "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."</p> <p>See also Figure 4, IPsec VPN Interconnection into MyFloridaNet on page 22 of the SOW; the Contractor is financially responsible for its interface to the internet.</p>
40	Attachment A – Statement of Work, 3.9	28	<p>Will the State agree to modify the following portion of this requirement: "including wireless modems (before and after installation, if requested by the Customer)"?</p> <p>The Respondent will assist with the deployment and ongoing deployment / kitting support for bulk orders of (50) or more. Basic power on / connectivity testing including a QA process sampling for application load is performed for bulk orders by our kitting and staging partners. The State will have support available to</p>	Please see Section 2 of Addendum No. 2.

Question Number	Section	Page Number	Question	Answer
			troubleshoot issues related to connectivity, CUG, Failover, etc.	
41	Attachment A – Statement of Work, 3.12	29	The Respondent respectfully requests the following be removed from this requirement: “The Contractor will provide DMS a copy of the Contractor’s associated security procedures upon request.” Respondent security procedures are considered proprietary. Respondent will communicate details where necessary.	Please see Section 3 of Addendum No. 2.
42	Attachment A – Statement of Work, 3.14.3	32	Is this requirement per agency and per event?	Per event, not per agency.  Please see Section 4 of Addendum No. 2.
43	Attachment A – Statement of Work, 3.14.3	32	Does the State intend to keep or return devices to the Respondent after the emergency event?	Return.
44	Attachment A – Statement of Work, 3.15	33	Please confirm the State will be financially responsible for the MFN equipment and circuitry including VPN concentrators, circuits, and infrastructure components.	Please see subsection 3.15 (page 33). “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.”  See also Figure 4, IPsec VPN Interconnection into MyFloridaNet on page 22 of the SOW; the Contractor is financially responsible for its interface to the internet.
45	Attachment A – Statement of Work, 3.17	34	Please further describe what statistics on products/services from a high level to a detailed level the State is looking for Respondents to provide.	The Department will provide additional information at the time of request when the items specified in section 3.17.2 are requested from the Contractor.
46	Attachment A – Statement of Work, 3.17	34	What information does the State wish to receive regarding device trends?	Please see Answer No. 45.

Question Number	Section	Page Number	Question	Answer
47	Attachment A – Statement of Work, 3.19	37	Please confirm the DMS will funnel escalations from agencies and OEU to the Respondent as opposed to individual agencies and OEU escalating directly to the Respondent.	OEUs, State agencies, and DMS may contact the Contractor(s) directly.
48	Attachment A – Statement of Work, 3.19	37	<p>If there is a customer impacting outage as a result of any planned maintenance, those notifications will be provided by Respondent under the unplanned maintenance notification process. Will the State agree to modify SOW subsection 3.19 to modify (4) with the following revised language?</p> <p>Notifications. Notifications must be provided for <del>planned</del>, emergency, and unplanned maintenance. The Contractor shall send an electronic notification which informs DMS of 1) <del>a planned maintenance which may potentially cause a service outage;</del> 2) emergency maintenance when it may cause a service outage and when there is an outage impacting a generalized area; and 2) 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. <b>Attachment C, SLA-B7, B8, and B9.</b></p>	Please see Section 6 of Addendum No. 2.
49	Attachment A – Statement of Work, 3.23	41	SOW subsection 3.23(1) states that the Contract shall “Provide all reporting activities listed in SOW subsection 3.27.5(1)(b) and SOW subsection 3.27.5(1)(c).” Can the State please confirm that the citations to subsection 3.27.5(1)(b) and 3.27.5(1)(c) are the correct subsections? There does not appear to be subsections with these numbers in the SOW.	Please see Section 7 of Addendum No. 2.

Question Number	Section	Page Number	Question	Answer
50	Attachment A – Statement of Work, 3.23 (7)	41	Will the State agree to revise SOW Subsection 3.23(7)(c) to revise the statement “Migration does not include new Customers or Customers changing their services after migration” to state, “Migration does not include new Customers, <del>or</del> Customers changing their services after migration, or non-State agencies that opt to purchase under a different contract vehicle.” Non-State agencies and are not required to use this Contract and Contractors, both incumbent and non-incumbent, should not be required to migrate those Customers to this new Contract if the non-State agency opts to utilize a different contract vehicle.	See ITN section 4.4, Negotiations.  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
51	Attachment A – Statement of Work, 3.26.2	47	Respondent respectfully requests the following be removed from this requirement: “costs and calculated earned value metrics Cost Performance Index (CPI) and Schedule Performance Index (SPI),”.  This portion of the requirement is not applicable to a fixed-priced wireless contract.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
52	Attachment A – Statement of Work, 3.26.2	47	Respondent requests that the State clarify that the Contractors have up to 18 months to complete the Project Implementation Phase.	Contract Nos. DMS-10/11-008A – C expire January 19, 2022. The Contract(s), if any, resulting from this ITN are anticipated to be executed in May 2021. This leaves eight (8) months for implementation. The timeframe for each awarded Contractor’s implementation will be agreed upon in the Implementation and Migration Plan.
53	Attachment A – Statement of Work, 3.26.3	48	Please clarify the State’s expectations for the Operations Guide. What type of topics and information would the State like included in the Guide?	During the Implementation Phase, some details related to “engineering, operational, and business processes” will need to be agreed upon between the Department and the Contractor(s). Once those standard operating procedures are written, they are to be collected and published as the Operations Guide. “At a minimum, the guide must include

Question Number	Section	Page Number	Question	Answer
				<p>ordering, troubleshooting, trouble reporting, service provisioning, SLA monitoring, and invoicing processes.”</p> <p>A specific example of a topic to be included in the guide will be the answer to the question, “How should the Contractor notify the State when a device is not available at the point of order?”</p> <p>See also Section 8 of Addendum No. 2.</p>
54	Attachment A – Statement of Work, 3.26.5 (c)	49	Please define ‘non-incumbent’.	Non-incumbent Contractors would be any vendors the Department contracts with as a result of this ITN that do not currently have an MCS Contract with the Department.
55	Attachment A – Statement of Work, 4	53	Specific to 4. Public Safety Service Plans and Devices, are Respondents permitted to not bid on this section of the ITN?	Yes.
56	Attachment A – Statement of Work, 4	53	Should the Respondent be unable to meet all Public Safety specifications as written, will there be an opportunity for Respondent to add specified services after award should those specifications be met?	Contract terms may be negotiated in accordance with ITN Section 4.4, Negotiations; however, Contract terms can only be changed after Contract execution via amendment, in accordance Section 19.10, Modification and Severability, of Attachment B, Draft Contract.
57	Attachment A – Statement of Work, 4	53	Should the Respondent be unable to meet all Public Safety specifications as written, would DMS allow Respondent’s Public Safety solutions onto the contract to allow local entities to purchase such using the FL MCS contract, if they so deemed these solutions meet their needs?	<p>See ITN section 4.4, Negotiations,</p> <p>However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.</p>
58	Attachment A – Statement of Work, 4	53	Should the Respondent need development time to meet the Public Safety specifications as written, could the Respondent be allowed a 12 month time period after award to meet such expectations, knowing no sales would occur until the specifications are met?	<p>See ITN section 4.4, Negotiations,</p> <p>However, no modifications are guaranteed, and Replies must be submitted as if the current terms apply.</p>

Question Number	Section	Page Number	Question	Answer
59	Attachment A – Statement of Work, 4	53	Should the Respondent meet several of the Public Safety specifications and provide significant advantages in price or other capabilities, will it still be considered as an option for the State?	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and replies must be submitted as if the current Contract terms apply.
60	Attachment A – Statement of Work, 4.5	54	What aspects of the Public Safety offer is the State looking to be demonstrated?	Test devices required by section 4.5 (wireless demonstration equipment) could be any device the awarded Contractor(s) are proposing for addition in their catalogs as a public safety device.
61	Attachment A – Statement of Work, 4.7	55	The Respondent requests the State strike 'device type' from this requirement. Responder does not always have access to this data, such as in a BYOD scenario.	The Contractor will not be required to provide information that is not available.
62	Attachment A – Statement of Work, 5.3	58	Please confirm the State's definition of inventory for this requirement (services or equipment)?	Inventory is described in subsection 5.9, Inventory.
63	Attachment A – Statement of Work, 5.9	58	How should the Respondent notify the State when a device is not available at the point of order?	This level of detail related to this business process will be developed during the implementation process.
64	Attachment A – Statement of Work, 5.5	59	Please provide a sample CSAB Service Catalog.	The requested information can be found on the Contractor's EUPLs, which are uploaded into the CSAB Service Catalog. The Department's current EUPLs can be accessed at: <a href="https://www.dms.myflorida.com/business_operations/telecommunications/suncom2/voice_services/mobile_communication_services">https://www.dms.myflorida.com/business_operations/telecommunications/suncom2/voice_services/mobile_communication_services</a>
65	Attachment A – Statement of Work, 5.6	59	Will the State please confirm the 0.7% transaction fee that all vendors must collect for sales made on the MyFloridaMarketPlace (MFMP) online procurement system is not subject to the rules/requirements in section 5.6?	Confirm.

Question Number	Section	Page Number	Question	Answer
66	Attachment A – Statement of Work, 5.9	6.1	Please confirm the State wants a view into only the active inventory on CSAB for the DMS account, as opposed to Contractor’s available device inventory.	The State is not requiring a view into the Contractor’s available device inventory.
67	Attachment A – Statement of Work, 5.10	61	Is the State willing to agree to remove the phrase “based on a calendar month” from this requirement? The Respondents bill-cycles don’t align with the calendar month.	A full month cycle of service is needed. Bill cycle does not have to begin on the 1 <sup>st</sup> of each month and end on the 30 <sup>th</sup> .
68	Attachment A – Statement of Work, 5.10	61	Is the State willing to agree to modify the timeframe for the following sentence “for electronic files for the CSAB portion must be received no later than <del>the 10th calendar day</del> of each month” to “15 business days” from this requirement? The Respondents billing process requires the additional time to complete our internal steps.	Ten (10) calendar days after the bill cycle completes for DMS CSAB accounts; however, if billed directly to Customer, no billing detail is needed for DMS.
69	Attachment A – Statement of Work, 5.11	61	Is this Substantiating Detail File specific to the CSAB bill file or required for all accounts purchasing under the contract?	The invoice substantiation file is specific to CSAB individual bills required under the Contract.
70	Attachment A – Statement of Work, 5.11	61	Please provide definition for unique ID?	CSAB inventory number.
71	Attachment A – Statement of Work, 5.12	62	The Respondent respectfully asks for the following modification to this requirement: “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 two (2) <del>one (1)</del> billing cycle from receipt of dispute or the Contractor will advise the DMS staff if additional time is required. <del>If Contractor has not resolved audit exceptions within one (1) billing cycle, the charges will be adjusted as determined by DMS.</del> ”	Two bill cycle – If Contractor has not resolved audit exceptions within two (2) billing cycles, the charges will be adjusted as determined by DMS.

Question Number	Section	Page Number	Question	Answer
72	Attachment A – Statement of Work, 5.16	62	Is the State willing to agree to remove the phrase “based on a calendar month” from this requirement? The respondent bill-cycles don’t align with the calendar month.	Please see Answer No. 67.
73	Attachment A – Statement of Work, 6	63	In regards to “By acceptance of an MFMP purchase order” does this refer to standard punch-out CXML PO specification?	MFMP purchase order routing is typically discussed once the Department and Contractor begin testing the MFMP punchout catalog during the Implementation Phase. The Contractor has two (2) options for order routing: email or electronic via the Ariba Network. If the Contractor elects to use email order routing, orders will be sent as an attachment using HTML format. If the Contractor elects to use electronic order routing, orders will be sent via cXML.
74	Attachment A – Statement of Work, 6.3 & 6.4	64	Please define “Customer corporate identifier”.	The corporate identifier is found in reports and statements (bills) associated with direct-billed accounts. This static entry is created by the Contractor. It allows Customers and DMS to recognize reports and statements as generated under the Contract.
75	Attachment A – Statement of Work, 6.4	64	Can the State please provide a template for this report?	There is no template for the Direct-Billed Monthly Report. It is provided by the Contractor and subject to DMS final approval.
76	Attachment A – Statement of Work, 6.5	65	Can the State please provide a template for this report?	There is no template for the Direct-Billed Quarterly Report. It is provided by the Contractor and subject to DMS final approval.
77	Attachment A – Statement of Work, 6.5	65	The Respondent requests the State strike ‘device type’ from the Quarterly Reporting of Direct-Billed Accounts. Responder does not always have access to this data, such as in a BYOD scenario.	Please see Answer No. 61.
78	Attachment C – Service Level Agreements	1	Respondent requests a limitation on financial penalties be included in Attachment 3, Service Level Agreement to limit each individual SLA to a cap of not more than 2% of monthly revenue per SLA, with an aggregate monthly cap across	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.

Question Number	Section	Page Number	Question	Answer
			all SLAs in Attachment 3 of not more than 5% of monthly revenue under the Contract.	
79	Attachment C – Service Level Agreements	1	Will the State confirm that one, multiple, or recurring violations of an SLA will not be considered a breach of the Contract?	Please see Attachment B – Draft Contract, section 11.2. “One, multiple, or recurring violations of a SLA may be considered a breach of the Contract and may result in a suspension or cancellation of PO(s) or CSA(s). The Department reserves the right to determine when violation(s) of SLAs constitute a breach of the Contract or will result in a suspension or cancellation of PO(s) or CSA(s). The Department’s determination of a breach of the Contract or suspension or cancellation of PO(s) or CSA(s) will depend on the number and severity of the SLA violation(s), disruption to service, Contractor’s response, and other factors.”
80	Attachment C – Service Level Agreements	1	Regarding SLA language and penalties, the ITN is not allowing any method of negotiation. Will the State reconsider, or is the only other contractor option a no-bid?	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and replies must be submitted as if the current Contract terms apply.
81	Attachment C – Service Level Agreements	1	Will SLA penalty amounts be individually negotiated with each vendor, or contract consistent for all vendors?	The Department’s intent is to have consistent SLAs across all Contracts, if multiple Contracts are awarded. However, the Department reserves the right to negotiate all terms with vendors individually.  See also ITN section 4.4, Negotiations.  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
82	Attachment C – Service Level Agreements, SLA-B1	2	The Respondent respectfully requests the following changes to the financial consequence for this SLA:	See ITN section 4.4, Negotiations.

Question Number	Section	Page Number	Question	Answer
			\$500 <del>\$5,000</del> per connectivity issue incidence <del>\$5,000 per quarter hour if the failover is not successful and</del> that results in downtime of longer than 500 second	However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
83	Attachment C – Service Level Agreements, SLA-B3	3	Respondent respectfully requests reducing the financial consequence from \$1000 / day for the SLA Compliance Report to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
84	Attachment C – Service Level Agreements, SLA-B4	3	Respondent respectfully requests reducing the financial consequence from \$1000 / day for the Escalation Activity Report to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
85	Attachment C – Service Level Agreements, SLA-B5	3	Respondent respectfully requests reducing the financial consequence from \$1000 / day for the Zero Usage Report to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
86	Attachment C – Service Level Agreements, SLA-B6	3	Respondent respectfully requests reducing the financial consequence from \$1000 / day for the Escalation Procedure Development and Updates to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
87	Attachment C – Service Level Agreements, SLA-B7	3	If there is a customer impacting outage as a result of any planned maintenance, those notifications will be provided by Respondent under the unplanned maintenance notification process. As such, Respondent requests that SLA-B7 Notification, Planned Maintenance be removed in its entirety?	Please see Section 14 of Addendum No. 2.

Question Number	Section	Page Number	Question	Answer
88	Attachment C – Service Level Agreements, SLA-B7	3	If SLA-B7 is not removed, Respondent respectfully requests reducing the financial consequence from \$2500 / day for Planned Maintenance to \$500 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
89	Attachment C – Service Level Agreements, SLA-B8	4	Respondent respectfully requests reducing the financial consequence from \$2500 / day for Emergency Maintenance to \$500 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
90	Attachment C – Service Level Agreements, SLA-B9	4	Respondent respectfully requests reducing the financial consequence from \$2500 / day for Unplanned Maintenance to \$500 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
91	Attachment C – Service Level Agreements, SLA-B10	5	Will the State agree to revise SL-B10 to remove the existing Performance Metric and replace it with the following: “The SLA clock stops for incumbent Contractors when all End-users are identified as either migrated, <del>or</del> no longer receiving services from the Contractor, <u>or for non-State agencies having selected another contract vehicle</u> . The SLA clock stops for non-incumbent Contractors when all End-users identified as purchasing services from the non-incumbent Contractor are migrated <u>or for non-State agencies having selected another contract vehicle</u> .”	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
92	Attachment C – Service Level Agreements, SLA-D17	8	Respondent respectfully requests SLA-D17 be removed in its entirety because most tasks in the checklist have individual SLAs already assigned.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and replies must be submitted as if the current Contract terms apply.

Question Number	Section	Page Number	Question	Answer
93	Attachment C – Service Level Agreements, SLA-F1	8	The Respondent respectfully requests the removal of this SLA due to the ambiguity of 'complete and accurate'.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
94	Attachment C – Service Level Agreements, SLA-F1	8	Respondent respectfully requests reducing the financial consequence from \$1000 / day for delayed invoices to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
95	Attachment C – Service Level Agreements, SLA-F2	8	The Respondent respectfully requests the removal of this SLA. The financial consequence could far exceed most credits and the Respondent's standard business practice it to apply credits within two (2) billing cycles.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
96	Attachment C – Service Level Agreements, SLA-G1	9	Please confirm the fees cited as previous in the following Performance Metric should be for the current quarter:  "An electronic Cost Recovery Payment will be provided within forty-five (45) days after the end of the calendar quarter to cover the fees collected for the previous quarter, in accordance with SOW subsection 6.2"	This is correctly stated in Attachment C, SLA-G1.  For example, the Cost Recovery Payment for the calendar quarter January through March is due by May 15 <sup>th</sup> , which is within forty-five (45) days after the end of the calendar quarter.
97	Attachment C – Service Level Agreements, SLA-G2	9	The Respondent respectfully requests the following change to this requirement:  A Direct-Billed Accounts Monthly Report will be provided no later than the 30 <sup>th</sup> 15 <sup>th</sup> of the month on all direct-billed accounts, in accordance with SOW subsection 6.4	Please see Section 14 of Addendum No. 2.

Question Number	Section	Page Number	Question	Answer
98	Attachment C – Service Level Agreements, SLA-G2	9	Respondent respectfully requests reducing the financial consequence from \$1000 / day for delayed invoices to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.
99	Attachment C – Service Level Agreements, SLA-G3	9	The Respondent respectfully requests the following change to this requirement:  A Direct-Billed Accounts Quarterly Report will be provided no later than the 30 <sup>th</sup> <del>45<sup>th</sup></del> of the month on all direct-billed accounts, in accordance with SOW subsection 6.5	Please see Section 14 of Addendum No. 2
100	Attachment C – Service Level Agreements, SLA-G3	9	Respondent respectfully requests reducing the financial consequence from \$1000 / day for delayed invoices to \$250 / day.	See ITN section 4.4, Negotiations,  However, no modifications are guaranteed, and Replies must be submitted as if the current Contract terms apply.



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

**Ron DeSantis, Governor**  
Jonathan R. Satter, Secretary

**Addendum No. 3 to the following Invitation to Negotiate (ITN):**

**Mobile Communication Services**

**DMS-20/21-006**

Date: March 29, 2021

To: Prospective Respondents to ITN No.: DMS-20/21-006

From: Caitlen Boles, Procurement Officer

Subject: Timeline Update

1. ITN No: DMS-20/21-006, subsection 1.8, Timeline of Events, the table is hereby amended as follows:

<b>TIMELINE OF EVENTS</b>		
<b>Events</b>	<b>Event Time (ET)</b>	<b>Event Date</b>
ITN posted on the VBS.		October 7, 2020
Deadline to submit questions to the Procurement Officer.	3:00 PM	October 28, 2020
Department's anticipated posting of answers to Respondent's questions on the VBS.		November 16, 2020
Deadline to submit Reply and all required documents to the Procurement Officer.	2:00 PM	November 30, 2020
Public Opening. Conference Room 101 4050 Esplanade Way Tallahassee, Florida 32399-0950  <b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/198062149">https://global.gotomeeting.com/join/198062149</a>  <b>You can also dial in using your phone.</b> United States (Toll Free): 1 877 309 2073	3:00 PM	November 30, 2020

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
United States: <u>+1 (646) 749-3129</u>  <b>Access Code:</b> 198-062-149  <b>Join from a video-conferencing room or system.</b> Dial in or type: 67.217.95.2 or inroomlink.goto.com Meeting ID: 198 062 149 Or dial directly: 198062149@67.217.95.2 or 67.217.95.2##198062149  New to GoToMeeting? Get the app now and be ready when your first meeting starts: <a href="https://global.gotomeeting.com/install/198062149">https://global.gotomeeting.com/install/198062149</a>		
Anticipated Evaluations Phase.		December 4, 2020 to December 30, 2020
Anticipated Negotiations Phase.		January 4, 2021 to <del>April 12, 2021</del> <b>April 29, 2021</b>
Negotiation Team Public Meeting Conference Room 101 4050 Esplanade Way  <b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/170310357">https://global.gotomeeting.com/join/170310357</a>  <b>You can also dial in using your phone.</b> United States (Toll Free): <u>1 866 899 4679</u> United States: <u>+1 (571) 317-3116</u>  <b>Access Code:</b> 170-310-357  <b>Join from a video-conferencing room or system.</b> Dial in or type: 67.217.95.2 or inroomlink.goto.com Meeting ID: 170 310 357 Or dial directly: 170310357@67.217.95.2 or 67.217.95.2##170310357  New to GoToMeeting? Get the app now and be ready when your first meeting starts: <a href="https://global.gotomeeting.com/install/170310357">https://global.gotomeeting.com/install/170310357</a>	10:00 AM	<del>April 19, 2021</del> <b>May 3, 2021</b>
Anticipated date to post Notice of Intent to Award on the VBS.		<del>April 26, 2021</del> <b>May 10, 2021</b>

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
Anticipated Contract Execution.		May 2021

**FAILURE TO FILE A PROTEST WITHIN THE TIME PRESCRIBED IN SECTION 120.57(3), FLORIDA STATUTES, OR FAILURE TO POST THE BOND OR OTHER SECURITY REQUIRED BY LAW WITHIN THE TIME ALLOWED FOR FILING A BOND SHALL CONSTITUTE A WAIVER OF PROCEEDINGS UNDER CHAPTER 120, FLORIDA STATUTES.**

Any protest concerning this agency decision or intended decision must be timely filed with the Agency Clerk. Protests may be filed by courier, hand delivery, or U.S. mail at Department of Management Services, Office of the General Counsel, Attention: Agency Clerk, 4050 Esplanade Way, Suite 160, Tallahassee, FL 32399-0950. Protests may also be filed by fax to 850-922-6312, or by email to [agencyclerk@dms.fl.gov](mailto:agencyclerk@dms.fl.gov). It is the filing party's responsibility to meet all filing deadlines.



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

**Ron DeSantis, Governor**

**Addendum No. 4 to the following Invitation to Negotiate (ITN):**

**Mobile Communication Services**

**DMS-19/20-006**

Date: April 27, 2021

To: Prospective Respondents to ITN No.: DMS-19/20-006

From: Caitlen Boles, Procurement Officer

Subject: Timeline Update

1. ITN No: DMS-19/20-006, subsection 1.8, Timeline of Events, the table is hereby amended as follows:

<b>TIMELINE OF EVENTS</b>		
<b>Events</b>	<b>Event Time (ET)</b>	<b>Event Date</b>
ITN posted on the VBS.		October 7, 2020
Deadline to submit questions to the Procurement Officer.	3:00 PM	October 28, 2020
Department's anticipated posting of answers to Respondent's questions on the VBS.		November 16, 2020
Deadline to submit Reply and all required documents to the Procurement Officer.	2:00 PM	November 30, 2020
Public Opening. Conference Room 101 4050 Esplanade Way Tallahassee, Florida 32399-0950  <b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/198062149">https://global.gotomeeting.com/join/198062149</a>  <b>You can also dial in using your phone.</b> United States (Toll Free): 1 877 309 2073	3:00 PM	November 30, 2020

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
United States: <u>+1 (646) 749-3129</u>  <b>Access Code:</b> 198-062-149  <b>Join from a video-conferencing room or system.</b> Dial in or type: 67.217.95.2 or inroomlink.goto.com Meeting ID: 198 062 149 Or dial directly: 198062149@67.217.95.2 or 67.217.95.2##198062149  New to GoToMeeting? Get the app now and be ready when your first meeting starts: <a href="https://global.gotomeeting.com/install/198062149">https://global.gotomeeting.com/install/198062149</a>		
Anticipated Evaluations Phase.		December 4, 2020 to December 30, 2020
Anticipated Negotiations Phase.		January 4, 2021 to <del>April 29, 2021</del> <b>May 26, 2021</b>
Negotiation Team Public Meeting Conference Room 101 4050 Esplanade Way  <b>Please join my meeting from your computer, tablet or smartphone.</b> <a href="https://global.gotomeeting.com/join/170310357">https://global.gotomeeting.com/join/170310357</a>  <b>You can also dial in using your phone.</b> United States (Toll Free): <u>1 866 899 4679</u> United States: <u>+1 (571) 317-3116</u>  <b>Access Code:</b> 170-310-357  <b>Join from a video-conferencing room or system.</b> Dial in or type: 67.217.95.2 or inroomlink.goto.com Meeting ID: 170 310 357 Or dial directly: 170310357@67.217.95.2 or 67.217.95.2##170310357  New to GoToMeeting? Get the app now and be ready when your first meeting starts: <a href="https://global.gotomeeting.com/install/170310357">https://global.gotomeeting.com/install/170310357</a>	10:00 AM	<del>May 3, 2021</del> <b>May 27, 2021</b>
Anticipated date to post Notice of Intent to Award on the VBS.		<del>May 10, 2021</del> <b>June 1, 2021</b>

TIMELINE OF EVENTS		
Events	Event Time (ET)	Event Date
Anticipated Contract Execution.		May 2021 <b>June 2021</b>

**FAILURE TO FILE A PROTEST WITHIN THE TIME PRESCRIBED IN SECTION 120.57(3), FLORIDA STATUTES, OR FAILURE TO POST THE BOND OR OTHER SECURITY REQUIRED BY LAW WITHIN THE TIME ALLOWED FOR FILING A BOND SHALL CONSTITUTE A WAIVER OF PROCEEDINGS UNDER CHAPTER 120, FLORIDA STATUTES.**

Any protest concerning this agency decision or intended decision must be timely filed with the Agency Clerk. Protests may be filed by courier, hand delivery, or U.S. mail at Department of Management Services, Office of the General Counsel, Attention: Agency Clerk, 4050 Esplanade Way, Suite 160, Tallahassee, FL 32399-0950. Protests may also be filed by fax to 850-922-6312, or by email to [agencyclerk@dms.fl.gov](mailto:agencyclerk@dms.fl.gov). It is the filing party's responsibility to meet all filing deadlines.