ISF
Solving the future

Department of MANAGEMENT SERVICES
Division of Telecommunications

Florida Department of Management Services

MyFloridaNet-3 Business Case

MFN-3 Business Case

August 19, 2024

Strategy | Process | Technology



Table of Contents

1 Executive Summary 4
1.1 Detailed Description of Services 4
1.2 Current Service Performance 5
1.2.1 SLA Report Generation & Review 6
1.3 Goals for Proposed Outsourcing 7
1.4 Outsourcing Authority 7
1.5 Descriptions of Available Options 8
2 Background 9
2.1 Overview and Background of MFN-2 9
2.1.1 MFN-2 Design Overview 10
2.1.2 MFN-2 Services 14
2.1.3 Service Level Agreements (SLA) Overview 27
2.2 Contract Improvements for MFN-3 28
2.2.1 Contract Flexibility to Support Emerging/Evolving Technologies 29
2.2.2 Contract Flexibility to Support Networking Solution Development 29
2.2.3 Decreased Level of Effort and Impacts Associated with Services Migrations 29
2.2.4 Increased Oversight on Last Mile Service Selection 29
2.2.5 Subscriber Consultative Services 30
3 Options and Cost Benefit Analysis 31
3.1 Telecommunications Market Conditions and Trends 33
3.1.1 Statewide Flat Rate versus Mileage-Based Pricing 34
3.1.2 Fixed-term Pricing versus Month-to-Month Charges 38
3.1.3 Use of Private versus Commercial Network Resources 40
3.1.4 Current Telecommunication Technologies 41
3.1.5 Analysis of Results from MFN-2 User Survey 51
3.2 Evaluation of MFN-3 Contracting Options 53
3.2.1 Last-Mile Services 54
3.2.2 Single-Award and Multi-Award Approach for Last Mile Services Comparison 62
3.3 Evaluation of MFN-3 Component Level Options 64
3.3.1 MFN-3 – Backbone Options 65

3.3.2 MFN-3 Last-Mile Access Options 70
3.3.3 Core Services Integration Options 75
3.4 Option Groupings for Cost Benefit Analysis Examples 79
3.4.1 Single-Award Vendor-Owned Core and Backbone Infrastructure (Example 1) 81
3.4.2 Single-Award Vendor-Owned Core and Backbone, Multi-Award Last-Mile Services (Example 2) 88
4 FIRN Sourcing Options 94
5 State Business Processes and Policies 95
6 Performance Metrics Review 96
7 Projected Timeline 144
8 Public Records Law Compliance 146
9 Contingency Plan 147
10 Transition Plan 149
10.1 Transition Plan Overview 149
10.2 Resources 150
10.3 Knowledge Transfer 150
10.3.1 Communication Plan 151
10.3.2 Engineering Review 152
10.3.3 MFN Services Transition Plan 152
10.3.4 Provisioning Planning 156
10.4 Network Operations Center 156
10.5 Administrative Services 157
11 Americans With Disabilities Act Of 1990, As Amended 158
12 Contractual Provisions 159
13 Appendices 160
13.1 Appendix A – Glossary of Key Networking Concepts 160
13.2 Appendix B – MFN-2 User Survey 172

Table of Figures

Figure 1 – MFN-2 Core/Backbone Overview 11
Figure 2 – MFN-2 Core Node Design Details 12

Figure 3 – MFN-2 IAG Design 13

Figure 4 – MFN-2 Typical WAN Service Connectivity 14

Figure 5 – MFN-2 VRF Services 16

Figure 6 – MFN-2 Broadband Service Integration 18

Figure 7 – MFN-2 MAN Services Overview 19

Figure 8: MFN-3 Options 32

Figure 9: Vendor Bid Differential for networkMaryland Project 57

Figure 10: Basis of Estimated Cost Avoidance with Multi-Vendor Last-Mile Services Model 60

Figure 11 – MFN High Level Diagram 64

Figure 12 – MFN Level 2 Functional Diagram 65

Figure 13 – Current MFN-2 Multi-Subscriber Site Solution 71

Figure 14 – Consolidated MFN Multi-Subscriber Site Solution (mini-node) 71

Figure 15 - 10 Year MFN-3 Cost Model Comparison 80

Table of Tables

Table 1 – CPE Management and Ownership Comparison Table 22

Table 2 – Factors Affecting Last Mile Pricing 34

Table 3 – Circuits or Connections for Key Users 35

Table 4 – 10 Year MFN-3 Cost Model Comparison Summary 80

Table 5 - Example 1 Vendor-Owned/Vendor-Managed Single-Award Cost Model Detail 87

Table 6 - Example 2 Vendor-Owned/Vendor-Managed Multi-Award Cost Model Detail 93

Table 7 – MFN-2 Service Level Agreements 97

1 Executive Summary

The State of Florida's MyFloridaNet-2 (MFN-2) contract is the second multi-year contract designed to provide data communications to all Florida State agencies as required under section 282.703 F.S. As MFN-2 reaches the end of its contract term, the State has begun the process of developing requirements for an MFN-3 contract. The State has retained the management consulting firm ISF and the telecommunications firm Skyline to create a business case for MFN-3.

The Department of Management Services (DMS) desires to have a competitive procurement process and outcome for the successor network or networks to the current My Florida Network (MFN-2), to be identified as MFN-3, at both the core level and for last-mile servicing. MFN-3 will continue to service both State of Florida government agencies, as well as K-12 districts statewide under the FIRN framework. The MFN network has been serviced and operated under the MFN-2 contract by L3Harris.

In evaluating options for MFN-3 core and backbone services, the State will continue the successful model implemented for MFN-2. To work toward iterative improvement on the MFN-2 contract, the State is considering the segmentation of last-mile servicing as a separate competitive procurement to promote local competition, increase value to the State, and to encourage cost-avoidance for each circuit purchased by MFN customers. This Business Case provides detailed research and advisement on current market conditions and other considerations to help guide the State's decision-making process in the development of the MFN-3 procurement.

1.1 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.

Services in the MFN portfolio are described as follows:

- MyFloridaNet - is a comprehensive solution providing a rich and flexible enterprise communications infrastructure dedicated for the exclusive use of State of Florida customers. The enterprise infrastructure is based on a core network using routers and Multi-Protocol Label Switching (MPLS) technology managed by a Network Operations Center (NOC) to provide security and robust connectivity. The result is a highly available (HA) and highly reliable (HR) statewide communication network (together HA/HR). MyFloridaNet is made up of layers of service and support that provide the telecommunications capability, infrastructure, and services through the implementation of:
    - Core Access Methods
    - Service Features
    - Service Levels
    - Customer Premises Equipment (CPE)
    - Primary Data Center (PDC)
    - Regional Metropolitan Area Network (MAN)
    - Interstate Transport

- Florida Information Resource Network (FIRN) - FIRN utilizes the structure of MFN to support its service delivery. FIRN supports data communications connectivity and internet access for K-12 schools. Schools pay for FIRN services almost exclusively using federal subsidies known as "E-rate" (averaging 70 percent). E-Rate subsidies come from the Federal Universal Service Fund (FUSF), which is financed through fixed fees charged to every user of interstate telecommunications services throughout the USA. The remainder of the cost is paid by the school using its budget resources. FIRN also includes some E-Rate qualified features, like email and special filtering.

Further analysis of the path forward for FIRN can be reviewed in Section 4: FIRN Sourcing Options.

MFN-3 is contemplated as a continuation of MFN-2 with a competitive procurement for the core and backbone services vendor. MFN-3 may also split out last-mile servicing as a multi-vendor contract as described in sections 3.2.1, 3.3.2, and 3.4.2.

1.2 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.

While the State currently manages the MFN-2 contract, the operation of the MFN network under this contract is outsourced to a third-party vendor, L3Harris. There are 35 performance metric service level agreements (SLAs) organized into five (5) categories as detailed in Table 7 within section 6 that govern DMS's management of this contract with L3Harris.

In most cases, the current metrics have served DMS well in managing the MFN-2 contract. In certain rare circumstances, SLA penalties to the MFN-2 vendor are lower than the cost to the vendor of providing services. This has led to service not being provided, with the decision made by the vendor to pay the SLA penalty rather than provide service. To address this issue, penalty caps should be re-evaluated in MFN-3 for increase and/or removal to ensure that requested services are delivered to all required MFN subscriber locations.

The Service Levels are currently divided into seven categories which align with elements of the MFN network, as listed in the bullets below:

- Core Network Availability and Performance Degradation
- Internet Access Availability and Performance Degradation
- Local Loop Access, CPE Availability, and Performance Degradation
- Operational
- Remote Access VPN Service
- Security
- Migration

Core Network Availability and Performance Degradation - Service levels for the Core (the MPLS backbone network/routers) are measured in terms of service outage or performance characteristics as defined in the matrix in Section 6. One-minute, one-hour, and two-hour restoral thresholds are defined with associated user credits for service provider non-compliance. Core metrics also measure latency, packet loss and jitter service levels with four-hour and eight-hour restoral performance targets.

Internet Access Availability and Performance Degradation - Service levels for access and Customer Premises Equipment (CPE) are measured by defined service outage or performance characteristics. Access and CPE are subject to four-hour and eight-hour restoral performance targets, as well as service levels for latency, packet loss, and jitter.

Local Loop Access, CPE Availability, and Performance Degradation - Service levels for Local Loop Access and CPE Availability measure service outage, latency, jitter, and packet loss. Thresholds are established for 4-hour restoration of outage, as well as appropriate thresholds for tolerance for latency, jitter, and packet loss.

Operational - General network operations and administration service levels are applied on a per incident basis, for the following activities:

- Installations
- Moves, adds and changes
- CPE configuration changes
- Service outage notification
- Service degradation notification
- Initial problem identification

Remote Access VPN Service - Service levels for restoration in the event of an outage are included in the current MFN-2 SLAs. These define specific expectations for centralized as well as remote site VPN appliances. Associated credits per time period as well as maximum single event credits are well outlined. Additionally, the current SLAs governing VPN services also outline performance metric tolerances for appliance CPU/Memory utilization as well as transport service utilization. DMS should consider further refining these SLAs to account for anomalies in traffic patterns by adding in clarity around how the "average" utilization levels are tracked and reported. Due to the business day nature of most service utilization patterns DMS should consider leveraging a 95th percentile-based calculation method for average utilization determination to avoid ambiguity.

Security – Service levels for notification of cybersecurity incidents and timely mitigation of Direct Denial of Service (DDoS) attacks are indicated with caps on penalties. It may be appropriate to reevaluate penalty caps as part of the MFN-3 contract to account for increased costs in service and associated loss to the State due to the relative impact of security incidents.

Migration – A single service level for timely migration of MFN infrastructure to MFN-2 was initially included to ensure that the initial project migration is completed in a timely manner. A similar metric will be necessary for MFN-3.

1.2.1 SLA Report Generation & Review

The performance degradation raw data is extracted from information provided by the MFN vendor. The MFN NOC Support Staff pull support ticket data. This data is utilized for the creation of the MFN SLA Violations report.

1.3 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.

In evaluating requirements for MFN-3, the State has the opportunity to review changes in modern technology and telecommunications market trends to provide improved service to agency users at the same or lower cost to Florida taxpayers. By continuing to outsource the MFN, the State will continue to provide the best value to State agencies as well as K-12 public education customers through the FIRN framework. The current implementation of MFN is a mature service offering utilized throughout the State. Agencies have built systems and processes that rely heavily on the continued technological structures that are in service today. The degree or intensity to which agencies are using MFN is widely variable depending on specific agency telecommunication needs. As with MFN-2, performance objectives for MFN-3 should continue to be guided by the following principles:

- Improve the core customers service offering and support
- Improve customer service offerings to all Other Eligible Users (OEU)1
- Improve pricing structures for all service layers
- Establish best-in-class statewide network solution
- Establish best value to the state through strategic sourcing, standardization, and process improvement
- Manage administrative costs through improved efficiencies of organizational oversight responsibilities
- Improve service layer capabilities based on DMS customer needs

The MFN-3 procurement should additionally address the following:

- Ending/transition of the current MFN contract to ensure no customer impacting events take place
- Provide improved service features based on evolving technological needs
- Competitively procure MFN-3 through negotiation to drive best value
- Drive down the current cost (approximately $60 million annually)
- Secure increased influence by DMS on decision-making related to last-mile vendor servicing

1.4 Outsourcing Authority

Section 287.0571 (4)(d), F.S.- A citation to the existing or proposed legal authority for outsourcing the service or activity.

Section 282.702(8), F.S., authorizes DMS to establish a telecommunication solution. Specifically, this section allows DMS "To control and approve the purchase, lease, or acquisition and the use of telecommunications services, software, circuits, and equipment provided as part of any other total telecommunications system to be used by the state or its agencies." Based upon this authorization, DMS has twice procured a telecommunications solution known as MFN, with the most recent contract

[1] Other eligible users of State Term Contracts include those local government entities identified in Rule 60A-1.005, Florida Administrative Code.

known as MFN-2. The Department of Management Services is seeking to continue services to state agencies through a competitive procurement of MFN-3 based on the findings of this business case.

1.5 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 two options specifically for the scope of continued support, integration, and installation of telecommunication services and ancillary features/capabilities following the expiration of the current MFN contract. In both options, an outsourced competitive solicitation is envisioned for core and backbone services. The second option envisions segmenting out last-mile servicing to promote local competition, increase value to the State, and encourage cost-avoidance for each circuit purchased by MFN customers.

These options were evaluated and included in this business case because they are within the scope for outsourcing as required by Chapter 287.0571, F.S. and they represent common procurement options utilized by the State for similar needs. The Division of Telecommunications at DMS currently operates multi-vendor contracts for other purposes similar to the method envisioned for last-mile servicing on this contract and will leverage this experience if this option is selected for MFN-3.

For the purpose of this business case, one or more competitive Procurements are envisioned for the MFN-3 contract:

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 and/or complex services are being acquired. The price structure for services is negotiated. Note: MFN was originally procured via ITN.

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.

2 Background

In planning for the future MFN-3 contract, a firm understanding of the existing technology footprint and business requirements is necessary. Respondents to an MFN-3 solicitation will be expected to support agency customers at a level of service and reliability that is achieved through the current-state implementation of MFN-2 documented below.

The overview and background section provides a description of the current services including the current contractor's performance under the MFN-2 contract and any other information necessary to provide the reader with a detailed, foundational understanding of Florida's telecommunications infrastructure.

The contract improvements for MFN-3 section outlines the present telecommunication needs of the MFN subscriber community, to include the existing gaps in services such as a small number of rural circuits that should be accommodated through other technology options or emerging technologies. This section also delves into desired improvements in the areas of contract flexibility, migration processes, oversight, decision-making, and consultation availability.

2.1 Overview and Background of MFN-2

The Department of Management Services (DMS) is the business and workforce arm of Florida government. The department excels in meeting the core business needs of State government and its employees so Florida's state agencies can focus on their core missions. The department serves more than 1 million customers through services for the State of Florida as a whole, including the administration of retirement benefits and health insurance, advising agencies on human resource policy, setting technology policy through Florida Digital Services, and maintaining the State's human resource information system (HRIS), PeopleFirst. DMS oversees the State's procurement procedures and also provides statewide telecommunication services, coordinates real estate construction and management, and monitors Florida's private prisons and fleet of vehicles, amongst other services.

The DMS Division of Telecommunications (DivTel) provides telecommunications services through a technology program known as SUNCOM which includes voice, data, wiring and cabling, and conferencing services. SUNCOM provides these cost-effective services to state and local governments, educational institutions, libraries, and non-profit organizations by achieving economies of scale with enterprise planning and procurement. DivTel data services are offered and available to the following entities:

- State agencies
- State universities and community colleges
- City or county governments in Florida
- Non-profit corporations receiving the majority of their funding from the state or local government
- Select commissions and boards

- Water management districts
- Other eligible users (OEUs)

The Department of Management Services and L3Harris Technologies entered into the MFN-2 contract in 2016 to provide network services for state government and eligible users including Florida county and city governments, school districts, universities, community colleges, and non-profit organizations. MFN-2 is a multi-year contract for Florida's enterprise-wide area network (WAN service), regional metropolitan area networks (MAN), and related telecommunication services. The enterprise infrastructure is based on a Multi-Protocol Label Switching (MPLS) technology providing robust security and network connectivity, designed to offer a highly available (HA) and highly reliable (HR) statewide communication infrastructure. MFN-2 is a comprehensive solution providing a rich and flexible private enterprise communications infrastructure dedicated for the exclusive use of the State of Florida MFN/FIRN subscriber community. This enterprise infrastructure is based on MPLS technology and QoS (Quality of Service) mechanisms providing robust security and connectivity resulting in a highly available and highly reliable statewide communications network. MFN-2 provides service elements such as network core, local loop access, CPE, security, Internet access, NMS tools, design and engineering, and billing and ordering as a complete turn-key solution with flat-rate pricing statewide.

2.1.1 MFN-2 Design Overview

The MFN-2 network is comprised of three (3) primary architectural elements, the Core network, the Internet Access Gateway(s), and the edge/access. [redacted] The Core interconnects each region into a cohesive network communications fabric. Internet access gateways are collocated with two of the core nodes and are a comprehensive security boundary that extends MFN-2 communication into the public Internet. The edge/access environments comprise the infrastructure that extends services from the regional core points of presence to each MFN-2 connected facility. Details on these architectural elements are provided in the sections below.

2.1.1.1 MFN-2 Core Design

[redacted]

[redacted]

[redacted]

-

[redacted]

[redacted]



[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

-

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- WAN service

[redacted]

[redacted]

[redacted]

[redacted]



A MAN service can be ordered as a layer-2 bridged service or a layer-3/2 routed service. Both variants provide the capability of creating a closed user group within a defined MAN boundary. For a single local loop provider, MAN sites have two management connections with unique VLANs terminating at geo-diverse core nodes as well as a third VLAN (data) for the closed user group, in other words, the broadcast domain. If a multi-local loop provider solution is required, customer sites will have two data VLANs back to the core. The management traffic will traverse the data VLAN and be leaked into the Management VRF. This redundant configuration is not available for E-rate customers. MFN-2 MAN service provides speeds ranging from 1.5 Mbps to 100 Gbps.

2.1.2.4 Remote Access VPN Services

A Virtual Private Network (VPN) is an alternative to a private network where the network owner exclusively uses the wired infrastructure. Typically, a VPN is used to traverse a layer 3 network path (Internet or wireless airspace), which is out of the control of the user. User data is encrypted before being sent across that path using an encrypted tunnel. The tunnel protects passing data from being snooped and the encrypted key exchange prevents Man-in-the-Middle attacks. On MFN-2, a VPN may exist between an individual machine and the MFN-2 network, or a remote network and the MFN-2 network. The MFN-2 VPN infrastructure requires strong encryption and authentication of remote users or peer devices and masks information about the private network topology from potential attackers on the public Internet.

MFN-2 supports two major flavors of access to the MFN-2 Intranet; distributed and centralized. Distributed is also known as a site-to-site VPN and can be within the core (private WAN) or over the Internet.

The centralized flavor of VPNs includes three designs:

- LAN-to-LAN
- Client-to-LAN
- Clientless

2.1.2.5 Primary Datacenter Services

MFN-2 provides a reliable, high-speed connection to the State's PDC (primary data center), also known as the SSRC. The PDC service in Tallahassee enables MFN-2 backbone traffic and Tallahassee MAN traffic to flow into the PDC. The design provides three connectivity options: local bridged, local routed, and Statewide routed. The available bandwidth for all options is from 2 Mbps to 100 Gbps. With the substantial traffic requirements of the PDC, MFN-2 has implemented a "mini-node" at this facility where the MFN-2 service provider has provided physically diverse backbone fiber routes from the PDC implemented on the Tallahassee MAN. The service is provided with the same SLA guarantees as provided in the MFN-2 core. Traffic is monitored for malware by the IDS located at each core node.

2.1.2.6 FIRN Services

MFN-2 provides two (2) service offerings for FIRN subscribers. FIRN services are supported over the same MFN-2 core infrastructure but are logically isolated to ensure e-rate applicability for its subscribers. FIRN "Internet Bundled service" provides a basic firewall service bundled with high-speed Internet service for E-rate customers (FIRN). Other bundled security features such as malware protection are also provided as part of the service at no additional cost. Direct Internet Access (DIA) service provides a high-speed Internet-only service for E-rate customers (FIRN). The DIA service offering has direct access to the Internet and does not provide any security monitoring or services.

2.1.2.7 Cloud Connect Services

The MFN-2 Cloud Connect Service (CCS) provides transport connectivity between a supported cloud service provider and MFN-2, allowing the MFN-2 customer sites to access cloud services. CCS provides a more robust connection as compared to an encrypted tunnel over the Internet as it leverages private network service paths with more consistent performance (latency, jitter, packet loss). CCS providers supported on MFN-2 include:

- Amazon Web Services
- Microsoft Azure Government
- Microsoft Azure Private
- Microsoft Azure Public
- Microsoft Office 365

- Oracle

The available bandwidth for all options is from 1 Mbps to 5 Gbps. Cloud Connect services are available in a layer-2 and a layer-3 options.

[redacted]

[redacted]

2.1.2.8 Interstate Services

The MFN-2 infrastructure also offers service connections extending beyond Florida's state boundaries through its Interstate Service offering. These services are available as customized offerings which vary on engineered solutions and prices depending on the specific customer requirements. These services can be leveraged by MFN-2 subscribers for special projects or business needs that require integration with facilities outside of Florida, for example for disaster recovery services and/or specialized SaaS offerings. These solutions are customized based on the specific use case requirements and are supported on a case-by-case basis.

2.1.2.9 Ancillary Services

In addition to the base telecommunications services MFN-2 also provides a suite of services that are considered ancillary. These services assist subscribers with leveraging the base MFN-2 services as well as enhance the offerings to include additional over the top services that enable more cost-effective IT operations. Ancillary services are optional and as such, incur an additional cost beyond the standard service cost. An MFN-2 customer must subscribe to an MFN-2 network service to qualify for ancillary services. The following subsections describe the ancillary services available on MFN-2.

2.1.2.10 Customer Premise Equipment (CPE)

The MFN-2 contract allows for hardware to be provided by the customer outside of the MFN-2 contract or rented by the customer through the MFN-2 contract. Each option has some differences from a contractual standpoint related to installation, configuration, monitoring, and maintenance. CPE may be acquired from the MFN-2 contract for locations with service and includes CPE maintenance and installation. CPE may not be rented through the MFN-2 contract for sites that do not have services.

The table below provides some comparisons between the managed and owned options.

Table 1 – CPE Management and Ownership Comparison Table

	MFN-2 Acquired CPE & MFN-2 Managed	MFN-2 Acquired CPE & Customer Managed	Customer Provided CPE & Customer Managed	Customer Provided CPE & MFN-2 Managed
MFN-2 configured	YES	YES	NO	NO
MFN-2 installed	YES	YES	NO	NO
Customer configured	N/A	N/A	YES	YES
Customer installed	N/A	N/A	YES	YES
NOC/SOC Support	YES	YES	YES	YES
Configuration Management	YES	YES	YES	YES
Maintenance	YES	YES	NO	NO
MFN-2 customer portal access	YES	YES	YES	YES

Note: Short definitions for terms in the table:

- **MFN-2 Acquired CPE** - Customer Premise Equipment that is being rented through the MFN-2 contract.
- **Customer Provided CPE** - Hardware the customer has acquired outside of the MFN-2 contract

Note: For all scenarios that include Customer Provided CPE, Simple Network Management Protocol (SNMP) access for MFN-2 is encouraged and required to provide adherence to SLAs as well as monitoring (NOC/SOC) support, and configuration management.

2.1.2.10.1 MFN-2 Acquired CPE

CPE may be acquired from the MFN-2 contract for locations with service and includes CPE maintenance and installation.

2.1.2.10.2 Customer Provided CPE Option

Customers may utilize existing routers that have been tested and approved. Utilizing existing routers on the MFN-2 network must ensure the router is not End-of-Life (EOL) or End-of-Support (EOS) as determined by the manufacturer. The customer must also ensure the existing CPE is upgraded to the current approved MFN-2 IOS. It is also strongly encouraged that any customer manager CPE has read-only access for the service provider that allows the service provider to ensure SLA performance targets are met.

2.1.2.10.3 Maintenance

All devices rented via the MFN-2 contract must have MyFloridaNet-2 maintenance which provides a four-hour CPE restoral SLA. The 4-hour SLA restoration point will depend on the ability to have read-only SNMP access to the MFN-2 NOC/SOC for fault detection.

MFN-2 CPE maintenance and associated SLAs are not available for purchase under MFN-2 for standalone CPE. Customers are required to coordinate CPE repairs themselves. MFN-2 CPE management is available and at the customer's direction the MFN-2 NOC will monitor, backup configurations, and notify the customer when CPE or other outages are detected. MFN-2 installation services are not available for CPE purchased outside the MFN contract.

CPE maintenance includes the following:

- 24 x 7 x 4-hour replacement of hardware parts and service restoral
- Access to the CPE Vendor Technical Assistance Centers, engineering resources, as well as MFN-2 NOC/SOC
- IOS software updates on rented CPE - Any software update on customer managed CPE is the responsibility of the customer

2.1.2.10.4 Installation

As part of the CPE subscription installation of MFN-2 acquired CPE includes staging, configuration, and installation. For all customer provided CPE the customer is responsible for configuring and installing the hardware. All customer provided CPE must be certified and approved by the MFN-2 CPE roadmap.

2.1.2.10.5 Configuration Management

As long as the MFN-2 NOC has read-only SNMP access to the CPE the MFN-2 NMS tool will store the last 25 copies of each router's configuration along with the User ID of who made each change. MFN-2 NMS allows the MFN-2 NOC/SOC the ability to perform side-by-side comparison of configurations for troubleshooting purposes. Unmanaged customers must enable the MFN-2 NMS access to their routers to be able to request access to stored configurations via the NOC/SOC.

2.1.2.10.6 After Hours Maintenance

The MFN-2 NOC/SOC will troubleshoot to the extent possible any circuit related issues. Any issues that require on-site access will require the customer to provide access to the site to receive CPE or allow for technician access to the CPE or the site in general. To ensure there are no issues with site access that could delay service restoration and to meet associated SLAs it is important that the customer identify and keep up to date on-site contacts for sites that require after-hours service restoral.

2.1.2.11 Ancillary General Services

General ancillary services are for all customers and include Telecommunication Service Priority (TSP), Demarcation Extension Service, After-Hour Installation Services, and Expedited Installation Services. For E-rate eligible customers only, general ancillary services also include Email Service, Web Hosting Service, Emergency Webpage, Data Storage Service and District Support. Additional details on each of these general services are provided in the corresponding sections below.

2.1.2.11.1 Telecommunication Service Priority

The TSP program authorizes National Security and Emergency Preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. The two primary uses for TSP are:

- Installing new service
- Restoring existing service

TSP customers must provide their associated TSP Authority Code which is then validated by DMS for eligibility. Once validated TSP is then applied to the associated customer within the MFN-2 infrastructure.

2.1.2.11.2 Demarcation Extension Service (Copper Only)

Demarcation extension service includes the necessary equipment, wiring, cabling, inspection, and installation to extend the service demarcation within a customer facility per MFN-2 customer requirements. The MFN-2 service provider is responsible for maintaining and managing the demarcation extension for the life of the contract at no additional cost. There are options for extension associated with both copper and fiber cabling with varying costs.

2.1.2.11.3 After-Hours Installation Service

The MFN-2 service provider provides after-hours installations between 5:01 pm and 11:00 pm local time Monday through Friday. Holiday and weekend support for installation is provided with pricing on an individual case basis. These services are available upon request by the target customer and incur additional charges.

2.1.2.11.4 Expedited Installation Service

Expedited installation service allows customers to schedule service delivery prior to the normal installation intervals. MFN-2 customers can request expedited installations based on a standard fee schedule provided by the MFN-2 service provider. The MFN-2 service provider does not charge expedited service fees if expedited service date is not met.

2.1.2.11.5 Special Construction

Special construction includes the necessary equipment, wiring, cables, inspection, and installation labor to provide connectivity for MFN-2 services. The MFN-2 service provider is responsible for maintaining and managing the special construction for the life of the contract. Under the current MFN-

2 contract, service connections associated with bandwidth rates up to 12 Mbps will not incur charges to the customer. Service bandwidth speeds above 12 Mbps may incur additional costs and are negotiated on a case-by-case basis. If local loop access facilities exist from any provider to the target facility, there is no charge for special construction. If local loop access facilities do not exist to the facility from any provider, special construction charges may be incurred.

2.1.2.11.6 Email Service for E-rate Eligible Clientele

Under MFN-2, the service provider (L3Harris) provides an email service offering for E-rate eligible customers. The email solution has the option of filtering in accordance with the Children's Internet Protection Act (CIPA) guidelines. This includes measures in place to guard against hacking, intrusion, or misuse of email addresses and complies with State, Federal, and E-rate record retention requirements. Email and content filtering services are not eligible for E-rate reimbursement.

2.1.2.11.7 Web Hosting for E-rate Eligible Clientele

Under MFN-2, the service provider (L3Harris) provides highly reliable, scalable, convenient, and easy to use web hosting for E-rate eligible customers. The website storage capacity is 20 MB per user and includes:

- Website traffic
- Disk space for applicant provided content
- FTP transfer or web interface to upload files
- DNS if required

The Web hosting portal is similar in look and feel to the MFN-1 FIRN portal. Website administration support is available Monday – Friday, 8 am – 5 pm Eastern time. Web hosting services are not eligible for E-rate reimbursement.

2.1.2.11.8 E-rate Emergency Webpage

The MFN-2 emergency Webpage service allows E-rate customers to disseminate important information during emergencies and disasters. A backup emergency webpage server provides failover so that webpage server availability is greater than or equal to 99.99%. Customer representatives typically access the emergency server webpage content through the MFN-2 Public VRF. Off-net access is also possible over the same Internet portal used to provide the emergency webpages to the web.

2.1.2.11.9 E-rate Data Storage

The MFN-2 Data Storage service provides a secure, high performance, local vault device at the customer location to provide a seamless interface to industry standard backup applications. The service provides easy integration with existing software, and adherence to existing backup policies. It also includes duplicate data storage off premises that allows for the replication of the data from the local vault device at the customer location to a secure vault at a secured offsite facility. This service is only available to e-rate MFN-2 subscribers.

2.1.2.11.10 E-rate District Support

Ad hoc District Support services are available on a subscription basis and are not E-rate eligible for reimbursement. District Support includes but is not limited to:

- Established single point of contact
- Emergency DNS and webhosting which provides customer with complete service for managing web services
- Headquarters/District level consultation in all areas related to services provided
- Email support
- Dispatches as required to support ad hoc services including assistance related to customer's LAN
- 24x7x365 NOC support for customer's internal network of sites not under MFN-2 provider.
    - Limited to those services which can be provided by L3Harris such as proactive network monitoring, trouble tickets, DNS support, IP address management, two-hour response time to reported trouble, and performance monitoring and reporting

2.1.2.12 Ancillary Managed Security Services

MFN-2 ancillary Managed Security Services (MSS) are available to all MFN-2 customers and include security event monitoring and reporting, security device full lifecycle management service, vulnerability management and compliance service, log retention services, next generation content filtering/URL blocking service, security response and consulting, and security advisor feed. An MFN-2 eligible customer must subscribe to an MFN-2 network service such as WAN, MAN, or Broadband to qualify for subscription to MSS. Additional details on each of these service offerings are provided in the corresponding sections below.

2.1.2.12.1 Security Event Monitoring and Log Monitoring

The MFN-2 Security Event Monitoring and Reporting service includes:

- Firewall event monitoring and reporting
- Session Border Controller monitoring and reporting
- Network Intrusion Detection or Prevention (IDS or IPS) monitoring and reporting
- Device monitoring and reporting (servers, routers, switches)

2.1.2.12.2 Security Device Lifecycle Management Service

The MFN-2 Security Device Lifecycle Management service offers a fully managed solution for lifecycle management of customer-owned, customer facility premise-based security appliances. In addition to monitoring the availability and performance of the security appliances, this service also offers integration with the enterprise SIEM, ArcSight, and is monitored 24x7x365 by the MFN-2 NOC/SOC.

2.1.2.12.3 Vulnerability Management and Compliance Service

The MFN-2 Vulnerability Management and Compliance service identifies exposures and weak spots in customer environments by performing continual, accurate, external, and internal scanning across the MFN-2 network. Customer vulnerability results are integrated into the MFN ArcSight reporting system.

2.1.2.12.4 Log Retention Service

The MFN-2 Log Retention service supports a wide range of sources, allowing the capture and aggregation of millions of logs generated every day by critical information assets such as servers, routers, firewalls, databases, applications, and other systems.

2.1.2.12.5 Next Generation Content Filtering and URL Blocking Service

The MFN-2 Next Generation Content Filtering/URL Blocking service helps end-users enforce their protection policies and block inappropriate, illegal, and dangerous web content. This service can block access to multiple categories of objectionable web content, providing the necessary combination of control and flexibility to protect important resources.

2.1.2.12.6 Security Response and Consulting

MFN-2 provides customers access to a threat intelligence research team that aids customers in identifying threats and developing preventative countermeasures based on information collected from monitoring events world-wide.

2.1.2.12.7 Security Advisor Feed

The MFN-2 Security Advisor Feed provides customers with a weekly report of security threats, trends, and actionable information based on aggregated security intelligence feeds.

2.1.3 Service Level Agreements (SLA) Overview

To ensure the highest levels of reliability, availability, and delivery expectations on the MFN-2 contract are achieved for both the infrastructure and services provided, a set of SLAs have been put in place. These service levels are applicable on a per incident basis applying to all service provider managed access types, except for broadband local access. Customer credits are provided based on the defined guaranteed response times and associated performance measurements in the contract.

SLA Categories include:

- Core network availability and performance degradation

- Internet access availability and performance degradation
- Local loop access and CPE availability and performance degradation
- Operational
- Remote access VPN service
- Security

Services excluded from SLAs:

- Customer managed CPE SLAs only apply if customer provides access
- When CPE maintenance is not purchased through MFN-2
- Broadband local access if exempt from outage and performance degradation SLAs
- During scheduled maintenance

2.2 Contract Improvements for MFN-3

Requirements for the MFN-3 contract can be broadly delineated into technology focused requirements, and business focused requirements. The technology requirements for MFN-3 are consistent with the existing technology requirements associated with MFN-2. The service offerings currently available through MFN-2, as written in the MFN-2 contract, should meet the telecommunication needs of the MFN subscriber community. However, the implementation of MFN-2 has surfaced several issues that primarily relate to issues with SLA violations. There are also several rural circuits that may be better supported by emerging technologies.

For those subscribers that are currently supported, it is expected that the need for bandwidth will increase to the degree that MFN subscribers continue to incorporate video conferencing, live streaming, artificial intelligence, and other digitization strategies. Subscribers will also continue to adopt SaaS service offerings and other cloud hosted applications and services that will further contribute to overall bandwidth demand. The "services" currently offered under MFN-2 will remain consistent with the expected requirements under MFN-3. While there may be needs to add additional "over the top" or "value-add" services in the future, the current foundational service offerings priced competitively with the market will continue to be required offerings for MFN-3.

In addition to translating the current MFN-2 requirements to MFN-3, DMS has identified several areas of improvement that are desired. These additional contracting considerations are detailed in the sections below.

2.2.1 Contract Flexibility to Support Emerging/Evolving Technologies

DMS identified that the current MFN-2 contract is restrictive with respect to the ability to add emerging technologies and tailor the service offerings to ensure DivTel can influence the solutions built to support MFN subscribers. MFN-3 would benefit from more open contracting terms that would permit DMS and the selected contractor to engage in a partnership, in contrast with the current transactional relationship. Emerging technologies could include new potential services like low earth orbit (LEO) satellite services and other last mile integration options.

2.2.2 Contract Flexibility to Support Networking Solution Development

Under the current MFN-2 solution, security services are engineered and provided directly by the MFN contractor. The transactional nature of the current MFN contract limits the level of influence and/or control by DMS on the security solutions and their engineering. The current transactional nature of the MFN-2 contract requires that all requirements for services be determined up front leaving the contractor to then design and implement a system to meet them. There is a low degree of flexibility in the current arrangement for a more collaborative approach to the solution development. Since the solution is completely outsourced, the vendor has full authority in terms of system design and architecture. MFN-3 would benefit from direct oversight and decision-making on which security solutions are implemented as well as how they are integrated into the MFN architecture. For MFN-3, direct selection of security solutions by DMS should be considered.

2.2.3 Decreased Level of Effort and Impacts Associated with Services Migrations

The migration efforts associated with MFN-1 as well as MFN-2 have proven costly and labor intensive for both Florida and the MFN contractors. Contract changes have resulted in a complete redeployment of the entire MFN infrastructure. While these migrations have helped to ensure upgrades to the infrastructure, the one-time nature of these migrations have a significant impact on staff and business disruption to the state during the migration periods. MFN-3, as well as future iterations, would benefit greatly if they could avoid these required wholesale migrations. Upgrades and infrastructure upgrades are still a required component of the MFN but a solution to allow these upgrades to occur organically over time vs. the previous contract change mandated instances would be much easier to support and less costly overall to both Florida and the MFN contractor.

2.2.4 Increased Oversight on Last Mile Service Selection

The current service model under MFN-2 does not afford DMS much influence over last mile vendor selection as these relationships are directly between the MFN contractor and its selected business partners. Under MFN-2 the MFN contractor makes all decisions regarding what last mile service provider is selected for extending connectivity to each MFN connected facility. MFN-3 should provide for more involvement and authority by DMS in this selection process. Under the current MFN-2 solution there have been situations where the cost for delivering service to an MFN facility is found to be higher than the penalties enacted on the vendor for not delivering the services. MFN-3 should address this to ensure that DMS can service all subscriber requirements. The vendor selection

oversight and authority would also provide DMS with increased ability to protect the MFN subscribers from continuous extended outages in rural areas associated with poorly designed last mile service provider infrastructures. DMS could choose to migrate such sites with repeated outages to vendors with infrastructure designs more aligned with the MFN business needs despite potential cost differentials. MFN-3 should permit DMS to be directly involved in last mile vendor selection decisions.

2.2.5 Subscriber Consultative Services

MFN-3 would benefit from having the ability for subscribers to request and obtain design consulting and implementation services for network communications solutions that leverage the MFN. Subscriber consultative services are currently available when ordering WAN services, however, additional value will be realized if access to these consultative service offerings is expanded. Whether a subscriber is ordering new services or looking to redesign existing services, for example LAN services or rearchitecting reconfiguring an existing network, end subscribers will benefit from expanding these offerings. Often, subscribers lack the internal expertise required to effectively leverage the services provided by MFN. Having the ability to request assistance from MFN to design and implement solutions that leverage the MFN to meet a subscriber's requirements would serve to improve subscriber satisfaction with the MFN. This additional support would ensure subscribers leverage MFN correctly as well as help to increase the state's overall effective use of the investments in the MFN. This would also provide the potential to identify additional ancillary services that could be added to the overall MFN service portfolio as common requirements are found between MFN subscribers through these consultative engagements.

3 Options and Cost Benefit Analysis

This section details the options that warrant consideration by DMS with respect to the next generation of MFN, beginning with a discussion of current telecommunications market trends. The options presented are complex in nature with respect to how they interrelate. The choices made with respect to some of the presented options can result in changes in applicability for others. The options in consideration by DMS are described in detail as individual components, and then are arranged into two groupings for the cost benefit analysis.

This analysis differentiates two outsourced contracting approach variations that pertain to last-mile and ancillary services:

1. Single Vendor
2. Multi-Vendor

In the single vendor approach, one vendor is sourced to own and operate the entire scope of the MFN-3 contract. In the multi-vendor approach, a purchasing vehicle with multiple contract categories is setup to enable multiple vendors to provide services for last mile servicing and certain professional services, while a single vendor is still selected to own or manage core MFN-3 services. Therefore, there are two categories of options provided in this analysis:

1. Current-State, Single-Vendor
2. Single-Vendor Core and Backbone, with Multi-Vendor Approach for Last Mile and Ancillary Services

Within each of the two categories of options, there are multiple selections that can be considered by DMS that fall into the following 3 component types:

1. Backbone Options
    a. Shared vs. Dedicated Infrastructure
    b. Backbone PoP Facility Options
2. Last-Mile Access Service Options
    a. Last mile service diversification
    b. Mini-node Deployments for Multi-Tenant Facilities
    c. SDWAN
3. Core Services Integration Options
    a. Direct ISP Peering with MFN Subscriber SaaS/Content Service Networks
    b. Direct MFN Integration with Cloud Services

See Figure 8 below which depicts the component level selections that apply to all three categories of options discussed in this document:

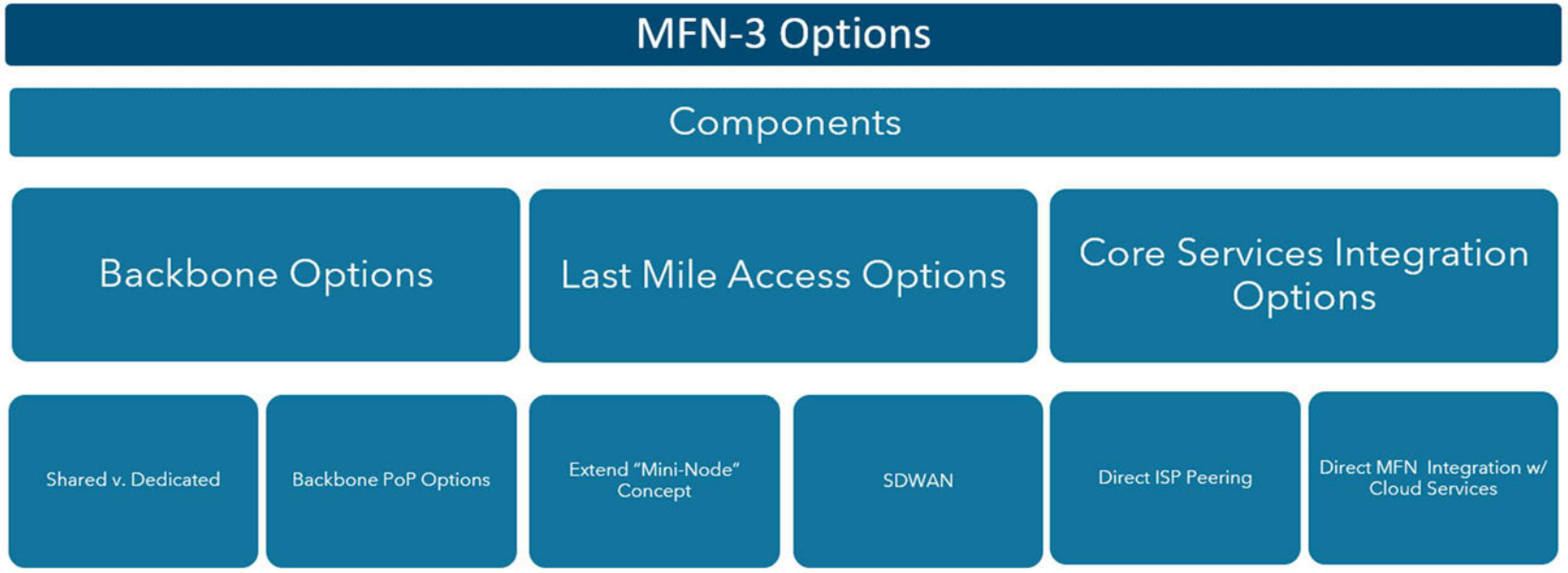


Figure 8: MFN-3 Options

The MFN-2 solution is a fully outsourced model. Under this model, the MFN service provider contracted by DMS is the owner and operator of the solution and the MFN subscribers leverage the solution in an as-a-service manner. The contractor is the owner of record for all associated MFN equipment, physical Points of Presence (PoPs), software, systems, and leased services leveraged to support the MFN services delivered to the subscribers under the associated contract. The MFN outsourcing model allows DMS some influence in the execution of SLAs which govern the outputs of the MFN solution, with less influence available for the architecture and solution design after the contract has been executed.

Greater influence can and should be asserted during the MFN-3 contract procurement process. In negotiating the updated architecture for MFN-3, several design considerations are described in section 3.3 that will be helpful for discussions with prospective vendors. Section 3.2 begins by explaining the concept of last-mile services and describes the potential benefits of separating last-mile services into a multi-vendor procurement vehicle.

3.1 Telecommunications 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.

The Department of Management Services (DMS) will implement a competitive procurement process for the successor network or networks to the current My Florida Network (MFN-2), to be identified as MFN-3, for both the core and backbone services and for last-mile servicing. Several options and emerging technologies should be considered in determining approaches to MFN-3 servicing. These key matters are addressed below, beginning with analysis of:

- Statewide flat-rate pricing versus mileage-based pricing
- Fixed-term pricing versus month-to-month charges
- Use of private infrastructure versus commercial/public infrastructure options

This analysis is followed by a discussion of current technologies and market conditions that have influenced the expected bandwidth and servicing requirements provided by the MFN-3 deployment.

3.1.1 Statewide Flat Rate versus Mileage-Based Pricing

The present rate structure for MFN-2 provides simplified flat-rate pricing[6]. However, the actual costs for last mile service delivery at facilities vary based on factors described in Table 2 – Factors Affecting Last Mile **Pricing** below.

Table 2 – Factors Affecting Last Mile Pricing

Factors Affecting Pricing	Description
Technology Mix	Pertains to copper, fiber, or hybrid, for example.
Placement Mode and Structure Costs	Pertains to underground, buried, or aerial.
Terrain Factors	Pertains to presence of rock, depth to rock, rock hardness, depth to water, and soil type, for example.
Density of Demand	A measure of the overall demand for service within the target geographic footprint used to determine potential ROI for initial infrastructure investment.
Cable Distances	Pertains to location of the premises in relation to existing telecommunications facilities.
Availability of Conduit Access	The availability of existing conduit infrastructure that can be leased or used by a carrier to install communications cabling infrastructure.
Unit Costs and Sizes of Cable and Terminating Equipment	Cable costs from all traffic and demand.
Labor and Contractor Costs	To include property taxes and other operating and overhead expenses related to the corporate organization.
Proximity to Railroad and Other Restricted Right of Way	Locations that are close to rail or other limited right of way areas often result in significant expense added as crossing such regions are very restricted and subject to governance by external parties.

Density of demand and cable distances are recognized as important cost-drivers for local loops, but they are not the only cost-drivers. A population's presence/density does not necessarily guarantee a telecommunications capacity and capability. The true costs for delivering telecommunication services to each facility are therefore highly variable. MFN-2 has required that these costs be normalized so that a standard common service rate is applied for every circuit ordered. This provides benefits to government organizations and the MFN, including:

- Reduction in billing complexity due to a more streamlined flow down billing distribution between DMS and MFN subscribers

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

- Ease of cost estimation and budgeting for planning/forecasting purposes
- Perceived "geographic fairness" from an equitable "treatment" in terms of service costs independent from service delivery locations
- Increased "incentive" to support service build outs in currently un/underserved regions as cost structure is shared across all delivered services proportionately to bandwidth rates. As such, there is no perceived "penalty" for services in less infrastructure dense areas.

The benefits associated with a flat rate telecommunications contract solution, such as MFN, are very attractive to government entities. Unlike many commercial entities that can choose facility locations with less constraints, government entities often must locate servicing offices and support infrastructure based on population distance and/or geographic requirements. Below is a listing of connection instances for key agency customers and other eligible users.

Table 3 – Circuits or Connections for Key Users

Agency or Other Eligible Users	Circuits or Connections
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Agency or Other Eligible Users	Circuits or Connections
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Agency or Other Eligible Users	Circuits or Connections
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Florida's delivery of services to residents through these agencies and partners are driven by the necessity of being accessible to customers and its operational resources, which covers a broad range of location types in both metropolitan areas and rural areas. Such breadth of location, distance, and other factors listed above affect overall pricing. The MFN must operate within its budget to ensure geographically spread-out communities are provided with the ability to conduct business and deliver services, while public sector agency users of MFN are empowered to connect to their constituents and stakeholders.

The underlying costs for service delivery by the vendor vary significantly. This places the burden and associated financial risks of normalizing those costs on the vendor. Vendors must ensure they operate MFN at a net positive budget. For static environments with little change in terms of facilities and/or services/service levels, the risk can more easily be mitigated as the costs are fixed and known, and normalization of costs can be more accurately calculated. For more dynamic environments where changes in facility locations and required services change frequently, the costs to deliver services can change dramatically depending on several variables that are not easily constrained. The cost variability risk can be transferred by the vendor back to the State by requiring up front, or non-recurring, capital costs to establish the new services. This has negative impacts on the overall benefit of the flat rate pricing solution to the State. Vendors could raise the overall rate structure to provide sufficient funding levels to mitigate the risk and offload the "up front" financial burden of service instantiation. The highly variable density of demand contributing to costs and lack of control inputs (e.g., the ability to influence subscriber decisions) represents a significant risk to potential MFN vendors. Typically, the significant risks demand that vendors have significant capital reserves to mitigate, resulting in the financial burden being shifted onto the MFN subscriber community.

In addition to the above considerations regarding flat rate pricing, telecommunication pricing can change significantly over time. The pricing for fixed broadband services[7] has shown a consistent decline in price of 4.8% year over year (5.8% when expressed as a percentage of per capita income). Flat rates are typically set during the planning/proposal stage of a contract such as MFN which, based on historical MFN procurements, tend to take at least a year before the contract is awarded and another 2 years before the full transition occurs. This 3-year time period before the full contract services are instantiated represents a cost decline of 13.7%. That differential extends to 21.8% at 5 years, 38.9% at 10 years, and 62.6% at 20 years. Bandwidth needs will increase year over year during the term of the contract. Upgrades and new service needs will also occur. It is therefore important for flat rate pricing contracts such as MFN to support some level of rate renegotiation or periodic true up,

[7] https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2020/ITU_ICTPriceTrends_2020.pdf, Accessed on 1/11/2024

supported by a level of transparency in how the proposed adjustments are developed. Reflecting this, in Section 7: Projected Timeline, a renegotiation for last-mile services is contemplated at a two-year interval.

Contracts that do not normalize rates to a common predetermined rate structure and instead employ a per-site cost plus model do not have this concern, as pricing for new services is continually bid and awarded based on current market conditions. Under such models the service vendors are required to provide transparency to the State in the costs they incur from last mile partners to deliver a service and are permitted to charge a specific percentage overhead fee for those costs which is specified within the governing master contract agreement. Static long-term services, however, will suffer from the same overall trending deficit in value. For example, a 100Mbps service may initially be installed under an MRC (monthly recurring cost) structure of $500 under a 2-year term commitment. At year 2 this service transitions to month-to-month as the required commitment term has elapsed. If the service is renegotiated at year 2, the State would potentially be able to obtain the same or a replacement circuit for less MRC, as the cost of bandwidth for telecommunications services has observed a downward pattern over time. In such a case the new cost may be $300/MRC for this example. If the circuit were not re-negotiated at year 2, the total cost to the State for 5 years would be $30,000 while the costs if renegotiated would be $22,800 (a 31% difference). It is, therefore, also important that service rates are re-evaluated on an agreed upon cadence so that Florida can obtain more consistent value over time as compared with market trends.

3.1.2 Fixed-term Pricing versus Month-to-Month Charges

Commercial carriers must evaluate many factors when determining costs for service delivery to a specific facility. Servicing a facility will often require some level of construction and/or implementation costs to the carrier to establish facilities to the location, engineer the site solution, and implement and provision the services. In addition, carriers must assess what, if any, impact the requested service(s) will have on aggregation and core facilities which may also require augmentation. All of these contributing elements factor into the costs the carriers then propose to the customers. Carriers typically leverage two (2) primary methods of addressing these costs factors:

- Upfront special construction costs and/or non-recurring fees
- Amortization of the investments required over time based on term-based contracts for service

Under the first option, carriers pass along the additional costs they incur to deliver their services to the customer directly through requiring up-front capital. These costs are typically referred to in the telecommunications industry as non-recurring costs (NRC) for service delivery and/or "special construction" fees[8]. Carriers can also use a combination of these fee elements, but in any case, they typically pass these costs directly on to the customer in some form.

[8] In the context of MFN-2, "special construction" costs have specific contractual requirements and are only permitted in certain last-mile buildouts by carriers. This deliverable addresses industry trends and discusses special construction costs generally. Additional analysis of current-state MFN-2 special construction requirements and recommended future-state special construction requirements will be presented in a later deliverable and as part of the final business case.

Carriers may not pass along all costs as the required construction to build out services to a facility may pose additional future benefit to the carrier. For example, a new facility may be in the center of a business park or development area that supports other potential customers. The carrier may choose to only attribute a portion (or not any) of the incurred construction costs to establish connectivity facilities to the site, with the expectations that they will be able to leverage that investment further to support other potential customer requirements, allowing them to spread the costs between customers.

Under the second option the carrier may choose to increase the monthly costs proposed to the customer beyond their "standard cost structure" to amortize their investment. This is an immediate benefit to the customer in that the carrier does not impose large upfront capital expenses on the customers, but instead amortizes those costs over time through increased monthly recurring costs. This represents a financial risk to the carrier in that the customer could terminate service in a time frame that prevents it from recouping the full investment. To alleviate this risk, carriers often request term commitments with associated financial penalties for early termination of service by the customer. This represents a method for shared risk between the carrier and customer, providing a financial incentive for long-term planning. There can be clauses in such contracts that permit early termination of service without penalty in specific situations:

- Force majeure such as acts of God, nature, or war resulting in the destruction or unavailability of the facility
- Service SLA's violations
- Replacement service contracted at equal or higher value in another location

Amortizing implementation costs over time can be considered a benefit to MFN in that large initial capital investments can be avoided. Often the costs associated with obtaining telecommunications services to a planned new facility are overlooked when budgets are developed. This can result in a budgetary shortfall with respect to the project in that sufficient funds to support the special construction costs levied by the commercial carriers are not available. Multi-year term commitment options for service are a convenient mechanism for the State to shift this capital burden onto the carriers in exchange for higher month to month bill rates until the carrier recoups that investment. This advantage is predicated on the expectation that after the term limit expires, pricing is renegotiated or recompeted, if necessary, on the open market to ensure the State obtains the best value for the service. If recompeted, the costs for migration should also be considered as a portion of the total cost of solution in determining best value.

Based on a review of a previous survey to the MFN subscriber community and analyst experience, subscriber agencies appreciate the convenience of month-to-month contracts. Government agencies should strive to plan their facilities and staff changes with a clear roadmap with associated timelines. Telecommunications have become a foundational business requirement for any facility to operate effectively in most modern organizations/government agencies. If limitations in State procurement requirements were to preclude DMS/MFN from entering term contracts with carriers, DMS would need to consider maintaining a funding source to support special construction costs as applicable to minimize the capital burden to agencies directly. A method to leverage increased flow down costs to recapture these capital funds to the agency/customer should be employed to ensure the investment

funds are not depleted and are replenished over time. While the need for significant special construction would not be expected during contract transition since all current service sites are already serviceable by a last mile carrier, future changes and/or moves would require the use of such a strategy.

3.1.3 Use of Private versus Commercial Network Resources

The State of Florida has established a communications solution for its agencies and customers under the successful MFN-2 program. By using dedicated backbone Multiprotocol Label Switching (MPLS) infrastructure, DMS has been able to incorporate a high level of enhanced security infrastructure due to the overall architecture of MFN-2 and using dedicated backbone infrastructure. The use of dedicated backbone infrastructure has also permitted MFN-2 to support highly customizable Service Level Agreements (SLA) and Quality of Service (QoS) profiles for its subscriber community. The use of a private backbone also provides DMS with inherent transparency through its selected service provider. With a dedicated solution in place, reporting on backbone capacity and utilization can be obtainable by DMS. Such transparency into the core transport environment in a shared environment is not typically available from commercial providers. Typically, commercial carriers only provide reporting details for the edge connections to subscribers and do not provide insights into the carrier's backbone infrastructure, since that infrastructure supports all their customers.

The carriers operate their backbones autonomously with no direct input or oversight from their customer base. The adherence to performance SLAs, which typically include factors such as drop rate, latency, or jitter, are the governing factors that carriers leverage to determine enhancement and upgrade timelines. Externally, from the viewpoint of the end subscriber, the use of shared vs. private resources is not observable in that both service delivery approaches are expected to operate under the same overall SLAs. Both solutions can also support the same overall MFN architecture as both methods are typically supported over the same technology (MPLS) within the core[9].

The primary differentiators between a private approach, such as the current MFN-2 methodology, versus a shared approach for the State are the security enhancements and overall flexibility afforded to MFN by its use of private dedicated infrastructure. Without that investment, the current MFN provided distributed IDS/IPS (intrusion detection/ intrusion prevention) service offerings would not be possible. Commercial/public carriers are typically not as flexible with shared infrastructure and do not permit the installation of probes and monitoring systems. While it may be possible for MFN-3 to obtain like services from a shared carrier solution, it is likely that such an offering would still require some level of dedicated hardware/infrastructure as well as customization to ordering and fulfillment systems. This would result in costs being close to, if not exceeding, the same offering over a private environment.

The flexibility currently afforded using a private approach has enabled DMS to add additional over-the-top services to MFN-2 such as Private Data Center (PDC) access, Cloud Connect, dedicated/cloud voice, and SIP (voice) services. While such services are possible to offer using shared infrastructure, there are likely to be more obstacles and restrictions to overcome to do so. In a shared model, future service offerings may be restricted to only those offerings made publicly available over the selected

[9] Assumes MFN-2 WAN services only and excluding MAN services.

provider's infrastructure. This results in less flexibility for DMS in terms of what services can be added to the MFN portfolio in the future.

3.1.4 Current Telecommunication Technologies

The following subsections describe current telecommunication market conditions and technology trends related to both MFN-2 and local loop infrastructure. These factors are intended to provide background information on the current market as points of interest for future MFN-3 architecture and service offering discussions. Soliciting strategies on the use of these technologies from potential MFN-3 vendors will help inform the selection process. The subsections provided are:

- Broadband Expansion
- 5G Development
- Internet of Things/Digitization
- Cloud Services
- Virtualization and Software Defined Networking (SDN)
- Cybersecurity
- Artificial Intelligence/Machine Learning (AI/ML)
- Low Earth Orbit Satellite Broadband
- Workforce Hybridization

3.1.4.1 Broadband Expansion

The Infrastructure Investment and Jobs Act (IIJA) is a landmark development towards the expansion of broadband access throughout the country. The Internet has become a necessity to participate in the digital economy, and access to it is considered foundational to economic growth and enablement. The IIJA sets forth a $65 billion investment into broadband, of which $48.2 billion will be administered by the National Telecommunications and Information Administration (NTIA). The NTIA has established the Broadband Equity, Access, & Deployment (BEAD) Program through which it will distribute the funding to deserving broadband expansion projects throughout the country. NTIA has allocated more than $1.16 billion through the federal BEAD program to Florida to facilitate the expansion of broadband Internet and service access across the state[10]. Coupled with the expansion of Cellular 5G

[10] https://www.floridajobs.org/news-center/DEO-Press/2023/11/21/floridacommerce-announces-30-day-public-comment-period-for-florida-s-bead-initial-proposal-volume-ii-to-access-more-than-$1.16-billion-in-broadband-funding#:~:text=In%202023%2C%20the%20state%20of,service%20access%20across%20the%20state, Accessed on 1/11/2024

technologies and millimeter wave, this represents a large potential infrastructure expansion opportunity for Florida.

The expansion in broadband access will require supporting middle and last mile fiber optic infrastructure. The State has a unique, time-sensitive chance to leverage these investments to opportunistically expand infrastructure where appropriate. The State of Florida, through the Department of Commerce, is currently working through the review process with NTIA to obtain BEAD funding[11]. Once funding is secure, it would be advantageous to the State if resource sharing agreements are required with benefiting providers, so that government entities may secure access to the fiber infrastructure assets being implemented assets implemented under the BEAD program. Once in place, these assets can be positioned for future opportunities to establish long term infrastructure connecting Florida's anchor institution facilities (government facilities, libraries, schools, Public Safety Answering Points, prisons, etc.), supporting high-speed communication between facilities while lowering overall telecommunications spend through the reduction in monthly recurring expenses. This effectively lowers future financial-based constraints, allowing the State to deploy applications that provide higher value to the community. Coupling these new investments with existing State fiber optical assets would provide a robust foundation for future iterations of MFN both during and beyond MFN-3, providing additional options for connectivity to the State.

3.1.4.2 5G Deployment

Carriers will have priorities around the deployment of cellular 5G technologies. 5G has the potential to deliver 20Gbps peak bandwidth capacity to mobile and fixed clients alongside a significant reduction in latency and jitter. This increase in access speeds will require corresponding investments in backhaul infrastructure to support them. Traditional wireless point-to-point backhaul communications solutions will struggle to keep pace with the growth in edge bandwidth, which will require investment in optical cabling infrastructure. The increased spectrum available for 5G (2-10 GHz, 24-53 GHz) required to support the higher capacity bandwidth increases will result in large scale deployments of microcell and picocell base stations by service providers to provide ubiquitous coverage. This will result in an increased need for fiber capacity to service each base station. Coupling this private sector initiative with federal programs (NTIA, IIJA, BEAD) to support broadband expansion will result in significant public/private partnership opportunities for government organizations, supported by resource sharing agreements to leverage right of way to support government network expansions.

The high-speed services provided by the adoption and expansion of 5G services will be a catalyst for increases in Internet of Things (IoT) and digital transformation efforts. Use cases and applications that are not possible with currently available communications technologies will become viable as the high-speed infrastructure to support them becomes available. This expansion will increase the ability to deploy monitoring infrastructure to provide near real-time data reporting, which will in turn be available to feed machine learning and artificial intelligent systems that can analyze the data streams and provide insights on actionable situations and events. Agencies in Florida have already sought to deploy use-cases involving sensors placed in both urban and rural areas. Greater bandwidth capacity may further enable real-time use-cases for agency objectives.

[11] https://www.internetforall.gov/bead-initial-proposal-progress-dashboard Accessed on 01/12/2024

High capacity cellular 5G capacity will be a potential solution for last mile connectivity for small to midsized facilities. While current frequency bands are expected to support up to 1 Gbps, fixed-facility enterprise use cases may require higher bandwidth capacities associated with the 5G 24-35 GHz spectrum range. As infrastructure supporting the cellular carriers are upgraded and augmented with the required additional micro/pico-cell solutions, 5G will become a viable alternative to traditional cabled last mile service offerings in areas where 5G has been implemented. The availability of higher cellular bandwidth alongside the technology's ability to support native network "slicing" positions 5G as a potential enterprise-grade last mile network communications access solution. Coupling this technology with SDN based solutions may further add velocity to adoption where available.

3.1.4.3 Internet of Things/Digitization

The growth rates in both compute capabilities as well as communications capacity have resulted in an environment that can now support digital transformation at a scale never before possible. As more information is digitized, Government agencies are impowered to make more informed decisions. This data driven power requires that data not only be collected, but also stored and analyzed at scale.

Digital transformation will have a transformational impact on government operations and services. In a recent study published by Deloitte based on over 1,200 interviews with government officials[12], 76% reported that emerging digital technologies are having a disruptive effect in the public sector, with 73% reporting that their public sector agency's digital maturity is significantly lacking when compared to private industry. As governments strive to embrace emerging technologies, there will be an increase in demand for high-speed resilient infrastructure to accommodate the collection and centralization of these data stores. While technologies like edge computing may reduce the overall data transport load through deduplication and trending analysis, there will remain a need for centralized data archival and processing. Each organization's growth rate towards digital maturity is different due to varying levels of need and available funding for strategic efforts, however the following potential benefits of digital transformation will drive maturity initiatives:

Reduced Costs
Digital services are typically 74% faster for the citizen and 95% cheaper to deliver than traditional in-person services[13].

[12] https://www2.deloitte.com/content/dam/insights/us/articles/digital-transformation-in-government/DUP_1081_Journey-to-govt-digital-future_MASTER.pdf, Accessed on 1/11/2024
[13] https://blogs.iadb.org/ideas-matter/en/how-digital-technology-can-deliver-government-services-more-cost-effectively/#:~:text=Digitalization%20can%20help%20ease%20these,for%20public%20institutions%20to%20deliver, Accessed on 1/11/2024

Improved Transparency
Digitization can make data more accessible to citizens promoting higher levels of accountability and overall subscriber satisfaction with services.

Improved Business Continuity
Digital delivery of services can enable higher levels of resiliency and ease of Continuity of Operations planning.

Improved Equity
Digitization enables more agile development of processes that can evolve to meet changing community needs more effectively. This can result in better levels of equity in terms of service availability.

Gartner predicts that by 2026 75% of all organizations will adopt a digital transformation model predicated on cloud as the fundamental underlying platform[14]. As these strategies are defined and put into motion, the demand for communication capacity to and from these cloud resources will also grow.

3.1.4.4 Cloud Services

Revenue associated with public cloud services is forecasted in 2024 to grow at a rate of 21.3%, resulting in a total spend on services at $725B[15] as organizational adoption of emerging technologies such as generative AI (Artificial Intelligence), Web3, and metaverse continue to drive digitization and innovation in businesses. While all segments of public cloud service offerings were forecasted to see growth in 2023, the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) segments were expected to see higher growth rates at 30% and 22.5%, respectively. Software as a Service (SaaS) spending is still expected to exceed the total revenue for either of these services, continuing to be the highest revenue area for all public cloud service offerings. The State of Florida has also embraced a cloud-first posture, placing the State in-line with this trend in migration to cloud services. This industry trend will translate to increased pressure on communications infrastructure and bandwidth demands, as application service paths transition from private internal datacenters to public cloud offerings.

-

[14] *Gartner, Predicts 2023: The Continuous Rising Tide of Cloud Lifts All Boats, Sid Nag, Yefim Natis, Ed Anderson, David Smith, Dennis Smith, and Jay Heiser, 9 March 2023*

[15] https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023#:~:text=Infrastructure%2Das%2Da%2Dservice,%25%20(see%20Table%201).&text=Note%3A%20Totals%20may%20not%20add%20up%20due%20to%20rounding, Accessed on 1/11/2024

The global SaaS market share is projected to reach $720.44 Billion by 2028[16]. This explosive growth rate can be attributed to cloud-based SaaS solutions that provide organizations with flexibility, scalability, and cost effectiveness that cannot be obtained through internal application development alone. SaaS is steadily becoming the go to method for various business applications for organizations of all sizes. SaaS solutions that incorporate AI capabilities provide organizations with insights that would otherwise be unattainable. SaaS providers are in a unique position to access datasets from multiple organizations within the same vertical market space, as well as across market segments. These datasets can be leveraged to support enhanced AI driven decision capabilities. While the governance of such practices will need to be defined to ensure privacy and security are maintained, the potential benefits of these macro layer data driven capabilities are immense.

The adoption of SaaS applications will drive adaptations to IT network designs, increasing the need and reliance of Internet services. SaaS services have made supporting hybrid workforces more achievable. The appeal of SaaS delivery models has also resulted in more vertically targeted service providers for traditional niche markets like health care and government services. SaaS solutions such as "Office 365" have already been widely adopted by many governmental organizations and are gaining in popularity. This has resulted in a sub-trend within the SaaS provider world known as microSaaS, which are specifically targeted application services for niche market segments, offering potential solutions for what were traditionally only custom developed offerings.

3.1.4.5 Virtualization and Software Defined Networking (SDN)

The software defined networking (SDN) solutions now available to industry lessen the operational barriers that plagued traditional encrypted virtual private overlay network deployments. SDN solutions leverage a central controller system where governance policies are defined, and which are then translated to distributed device configurations that affect that policy into the production network. This orchestration abstracts the complexities of deployment enabling the following benefits to organizations that leverage this approach:

Agility
With built-in support for zero touch automated deployments as well as orchestrated changes that are defined centrally, but provisioned automatically to edge devices, an SDN implementation can significantly reduce the time to market for new deployments as well as deployments of new services on existing infrastructure. Additionally, the Internet Protocol Security Virtual Private Network overlay nature of many SDN solutions coupled with the ability to virtualize end points that can run natively inside commercial cloud provider services permits a simplified method to facilitate cloud service adoption and expansion.

[16] https://www.globenewswire.com/en/news-release/2023/02/20/2611455/28124/en/Global-SAAS-Market-report-2022-to-2028-Featuring-Microsoft-Salesforce-Oracle-and-IBM-Among-Others.html, Accessed on 1/11/2024

Ease of Management
SDN technology offers the promise of centralized control and the single-pane-of-glass interface that network operators have been working to create within the industry.

Reduced Costs
Through its inherent orchestration and automation principles, SDN exponentially increases the throughput of network engineering resources while simultaneously reducing errors in deployments through structured templatized deployments. The inherent constructs used within the platforms to abstract the technical device level configurations combine to enforce a rigorous approach to operational deployments. Coupled with the ability to leverage multiple commodity internet transport services can also significantly reduce leased telecommunications costs while maintaining required application performance SLAs through enhanced monitoring and dynamic traffic routing controls.

Network Security
The orchestrated solution provided by SDN infrastructures can also result in enhanced overall security. By automating device level configurations, the solution can more readily ensure adherence to standard configuration requirements, including security related aspects. The automated solution also permits the deployment of complex IPsec overlays using more secure authentication mechanisms, increasing the overall security. The orchestrated functions also make tasks such as encryption tunnel rekeying that were traditionally administratively burdensome now trivial in comparison. Coupling this with some solutions ability to invoke next generation flow-based security features further enhance the security capabilities of organizations that deploy the technology.

The deployment of SDN technologies in the wide area network (WAN) has resulted in an increased demand for high-capacity, low latency commodity broadband Internet Service Provider (ISP) services and a corresponding decrease in VPN services provided directly by the carriers. To support more stringent applications such as voice and video services deployments often also requires multiple ISP service connections where available, or a combination of ISP and traditional VPN services operating at reduced bandwidth levels. This trend is likely to continue resulting in higher levels of Internet service competition and increased costs associated with the direct SLA-governed carrier VPN service offerings. This trend combined with the overall broadband expansion programs is likely to increase capacity within carrier network infrastructures.

The use of SDN (Software Defined Networking), in the form of SD-WAN (Software Defined Wide Area Networking), combined with Secure Access Service Edge (SASE), will increase. Gartner has an SDWAN market forecast of $5.3 billion for 2023, growing to more than $8 billion by 2026. Dell'Oro Group expects SDWAN to double from 2022 to 2027, hitting $6 billion[17]. MFN-3 will need to develop a

[17] https://www.sdxcentral.com/articles/analysis/sd-wan-by-the-numbers-market-size-growth-adoption/2023/08/, Accessed on 1/11/2024

solution that allows integration between SDWAN based service delivery and its current more traditional private MPLS infrastructure.

MPLS will remain the de facto standard for supporting virtualized service delivery over a common shared backbone infrastructure. Enhancements to MPLS such as SR (segment routing) as a new control plane for MPLS point to the continued development of MPLS technologies as carriers work to build upon their investments in their packet-based infrastructures. With wide industry adoption and continued development, MPLS will continue to remain the most cost-effective method for servicing the larger MFN facilities.

SDWAN will become a cost effective and operationally attractive option for edge service extension/last mile solutions. With its built-in support for multi-pathing and intelligent load sharing based on specific application flow requirements and real-time awareness of transport layer performance, SDWAN is an attractive option for MFN network service delivery. Coupling the benefits of SDWAN technology with the expected expansion of 5G, Low Earth Orbit (LEO) Satellite, and traditional wireline broadband service due to federal BEAD programs, SD-WAN is set to have a large impact on the future of MFN-3 services. SDWAN has not matured from a standards perspective sufficiently to support interoperability between vendor solutions, and as such it will be important to the overall cost effectiveness of MFN to define a single supported solution/vendor partnership to support MFN-3 that can provide multi-tenancy and virtualization.

3.1.4.6 Cybersecurity

The security of information technology assets, systems, users, and applications will continue to play a critical role in technology trends. Digital transformation efforts will bring a corresponding increase in the overall threat landscape. As transformational new systems and services are developed, the societal reliance on the infrastructures supporting them will also increase. This necessitates increased diligence in designing and implementing effective security mitigation and controls within every system. As systems become more integral in delivering public services, the potential impacts associated with malicious exploits become more mission critical. Digital transformation, remote work force enablement, virtual citizen service offerings, and cloud-based service adoption all increase the potential threat domain of cyber-attacks. Attackers will leverage these same innovations in Artificial Intelligence/Machine Learning (AI/ML) to enhance their tactics.

A centralized point of control, or security boundary, will no longer remain feasible as both users and applications are distributed through SaaS and virtual/hybrid workplace solutions are brought into organizational norms. As with SDN, strategies will require a centralized policy definition coupled with distributed execution to keep pace with the ever-changing IT landscape. The traditional line between security and transport infrastructure will continue to be blurred as network operators recognize the importance of end-to-end security and realize their defense-in-depth strategies. Identity management and multi-factor authentication services will become increasingly critical foundational solutions that underpin the entire organizational and cross-organizational IT service landscape.

3.1.4.7 AI/ML

The growth of Artificial Intelligence (AI) and Machine Learning (ML) applications will impact MFN-3 requirements. AI and ML are innovative technologies that aim to simulate human intelligence, enabling machines to learn and make decisions without explicit programming.

Artificial Intelligence (AI):

- AI refers to the development of computer systems that can perform tasks that typically require human intelligence, such as problem-solving, understanding natural language, and recognizing patterns.
- It encompasses a broad range of techniques and approaches, including rule-based systems, expert systems, and machine learning.

Machine Learning (ML):

- ML is a domain of AI that focuses on developing algorithms and statistical models enabling computers to improve their performance on a task over time without being explicitly programmed.
- ML relies on data to identify patterns and make predictions or decisions. ML use-cases are typically categorized into supervised learning, unsupervised learning, and reinforcement learning.

Key Components:

- Data: Both AI and ML heavily depend on data for training and improving models.
- Algorithms: These are mathematical models and statistical techniques that enable machines to learn patterns from data.
- Computing Power: AI and ML often require substantial computing resources for processing large datasets and complex algorithms.
- Feedback Mechanism: Machine learning systems learn from feedback, adjusting their models based on the outcomes of previous predictions.

Applications:

- AI and ML have a wide range of applications across industries, including healthcare, finance, marketing, and manufacturing.
- Examples include image and speech recognition, natural language processing, recommendation systems, and autonomous vehicles.

Benefits:

- Increased Efficiency: AI and ML can automate repetitive tasks and optimize processes, leading to increased efficiency and productivity.
- Data-Driven Insights: These technologies enable organizations to extract valuable insights from large datasets, facilitating informed decision-making.
- Personalization: AI can tailor experiences based on individual preferences, improving user satisfaction.

Challenges:

- Ethical Concerns: Issues such as bias in algorithms, privacy concerns, and the impact on jobs raise ethical questions.
- Data Quality: The success of AI and ML depends on the quality and relevance of the data used for training models.
- Interpretability: Understanding and explaining the decisions made by AI systems can be challenging.

In summary, AI and ML are transformative technologies with the potential to revolutionize industries, streamline processes, and enhance decision-making through the application of advanced algorithms and learning from data.

AI systems rely on large datasets to learn and make predictions. These datasets can come from various sources, such as online databases, public records, research institutions, and organizations that collect and curate data. The rapid availability of data will be the key resource defining successful AI driven projects and innovations. These future systems will require and consume increasingly large datasets, spawning growth in digitization/monitoring service requirements. These groundbreaking technologies will require distributed data collection for analysis and processing. While supporting technologies such as edge computing will help to alleviate the need for wholesale edge communications bandwidth, the trends will continue to push communications capacity requirements higher and are likely to result in higher edge demands where the datasets are generated and initially collected.

Organizations are expected to begin to adopt AI technologies into real world applications. It is expected that adoption will be more centered around tailored AI deployments with more strategic dataset models designed to provide specific insights into business trends. Organizations will build out their own portfolio of specialized models and datasets, each fine-tuned for a specific function and minimally sized to reduce costs and boost performance. This shift will lead to a greater number of smaller, focused models being used in production deployments. This trend will have direct impacts on growth in public cloud service consumption as organizations work to find suitable methods for obtaining the required supporting compute and storage services in a cost-effective manner while these new technologies are explored.

The current maturity of the industry and lack of baseline models for performance and predictive requirement specifications will drive organizations to leverage expandable/consumption-based services to support application development. Expanding AI adoption will also lead organizations to mature their current data quality, security, privacy, and trustworthiness. As the power of AI capable applications are realized there will be renewed emphasis on ensuring the baseline data collected to drive these innovations is accurate and dependable to ensure the results of the AI enhanced decisions are as accurate as possible. This will drive increased pressure and requirements on securing the telecommunications infrastructure and associated datastores. As the benefits of these emerging technologies are realized in government applications, supporting infrastructure will be required to keep pace.

3.1.4.8 Low Earth Orbit Satellite Broadband

SpaceX, Amazon Kuiper, Iridium Certus, Facebook Athena, & Google Alphabet Loon are all organizations that are developing and implementing broadband communications infrastructures based on Low Earth Orbit (LEO) satellite technologies. While satellite-based communication services have been around for decades, these new low orbit-based offerings offer significantly lower latency capability as compared to the more traditional geostationary orbit solutions. Traditional satellite-based communications services offered fixed latency rates as high as 477 milliseconds (ms) while LEO-based solutions using orbits (between 100 to 1,000 miles) offer latency levels less than 27ms[18]. This significantly increases the effectiveness of LEO-based solutions to support modern applications and services. For example, two-way voice communications require total delay to be less than 120ms.

LEO-based solutions are not "new," as companies attempted to build out LEO-based infrastructure networks as early as 1990. For example, Microsoft funded Teledesic, Globalstar, and Iridium. However, the costs associated with launching the thousands of required LEO satellites prevented the emergence of a viable business model to support full deployments. With private companies now able to more cost effectively deliver payloads into space, the viability and interest in implementing this technology has had a notable resurgence. LEO broadband services have the potential to deliver broadband communication services at a much higher level of flexibility and lower time to market.

Coupling these new communication service offerings with SDN/SD-WAN presents an opportunity for organizations to leverage these technologies in exciting and innovative ways. LEO-based implementations can now be leveraged to provide communication fault-tolerance (path diversity) to terrestrial facilities and are also now viable options for primary communications, particularly in locations where terrestrial service infrastructure is unavailable or cost prohibitive. The challenge for widespread organizational adoption will be related to the maturity of the service offerings and business processes around their ordering and support. LEO companies such as SpaceX are technically capable and ready to provide service in many areas, however, their relatively short experience delivering services may result in varying levels of maturity in business-grade procurement and operational aspects. Additional factors such as cosmic radiation (solar flares) as well as space debris fields within the target areas where LEO satellite orbits are established, coupled with the time delays

-

18 https://www.isoc.org/inet97/proceedings/F5/F5_1.HTM#:~:text=For%20GEO%20satellite%20communications%20systems,as%20high%20as%20400%20milliseconds), Accessed on 1/11/2024

associated with the logistical coordination involved with affecting repairs of the space-based solutions, must also be evaluated when considering the use of the services within enterprise organizations.

3.1.4.9 Workforce Hybridization

The COVID-19 pandemic resulted in significant changes in culture and technology. The pandemic forced organizations to rapidly develop or expand remote access solutions to support workforce virtualization, Continuity of Operations (COOP) activation, and overall business continuity. The pandemic also increased the need for virtual servicing, where possible, of customers and citizens resulting in enhanced service offerings supported over the Internet. The necessities of operational requirements under the pandemic also resulted in the realization that workforce hybridization was possible and provided intrinsic benefits such as decreased facility costs and infrastructure support.

Mechanisms to support hybridization have been adopted, for example Microsoft Teams and Zoom for internal messaging and teleconferencing. These apps help to foster increased productivity associated with workforce hybridization. At a macro layer, the decrease in commuting associated with workforce hybridization resulted in a tangible improvement in the environment. Employee satisfaction levels have also been increased with hybridization. Workers that could not support traditional work requirements are now afforded employment opportunities that provide more flexible work/life balance capabilities.

Hybridization has caused a fundamental shift in the organizational communications architectures with higher levels of employees relying on remote access solutions. In addition, the evolution has also mandated a need for the deployment of a unified communications platform[19] providing seamless integration of traditional PSTN (Public Switched Telephone Network) and desktop communications services. Coupled with the increased use of video enabled virtual meeting solutions, global Internet bandwidth usage from 2019-2023 expanded at a 4-year compound annual growth rate (CAGR) of 28%[20].

3.1.5 Analysis of Results from MFN-2 User Survey

As part of this Business Case, a survey was conducted of IT professionals responsible for provisioning and supporting MFN services for end-user agencies and organizations. This survey aimed to gauge user satisfaction and gather relevant feedback for the upcoming MFN-3 contract.

The overall sentiment from the survey responses indicates a desire for improvements in order status updates, portal access, procurement strategy, pricing structure, resource dedication, SLA enforcement, and technology upgrades. There is also a need for better support during transitions between MFN contracts. The agencies value security, stability, predictability, and flexibility in their network services.

The survey results reveal a strong desire for improvements across various aspects of network services. Agencies emphasize the need for better order status updates and user-friendly portal access. Real-

[19] https://federalnewsnetwork.com/innovation-in-government/2023/08/the-evolution-of-the-hybrid-work-environment-depends-on-unified-communications/, Accessed on 1/11/2024
[20] https://blog.telegeography.com/total-international-bandwidth-now-stands-at-1217-tbps, Accessed on 1/11/2024

time visibility into order progress is crucial, and accessible interfaces are valued. Regarding procurement strategy, opinions are divided: some prefer the current simplicity of a single vendor, while others advocate for an unbundled approach to enhance flexibility and competition. The current flat rate and month-to-month pricing structure is generally favored for its predictability, but periodic reviews are suggested. A private, dedicated, secure network is a priority. SLAs are deemed extremely important, and agencies seek rigorous enforcement. During transitions between MFN contracts, better support is needed. Technology upgrades, including SDWAN and improved encryption, are desired. Overall security, stability, predictability, and flexibility are key priorities for these agencies as they navigate network services.

Recommendations for MFN-3 contract improvements include:

1. **Clear SLAs and Penalties:** The contract should define specific Service Level Agreements (SLAs) with measurable metrics such as uptime, Mean Time To Repair (MTTR), and performance. Penalties for non-compliance should be outlined to ensure accountability.
2. **Improved Communication Channels:** The contract should mandate regular communication channels between the provider and agencies. This could include monthly status meetings, quarterly reviews, and a dedicated point of contact for each agency.
3. **Enhanced Reporting and Visibility:** The contract should require comprehensive reporting capabilities. Agencies need access to firewall logs, internet traffic logs, and other relevant data. Transparency is crucial for security and troubleshooting.
4. **Multi-Factor Authentication (MFA):** The contract should mandate MFA for VPN access. This strengthens security and prevents unauthorized access.
5. **Flexible Cost Models:** Maintain the flat-rate cost model, but allow for adjustments based on agency-specific needs. Flexibility in budgeting ensures alignment with fiscal cycles.
6. **Transition Support:** The contract should outline a smooth transition process from the existing network to the new one. Dedicated consulting services and NOC support during the transition are essential.
7. **Infrastructure Ownership:** Specify that infrastructure resources are dedicated to Florida agencies. However, explore configurations that leverage public/commercial network resources while ensuring security.
8. **Innovation and Competition:** Consider unbundling core and last-mile services to encourage competition among providers. This can lead to better innovation, reliability, and cost-effectiveness.
9. **Redundancy and Failover:** Ensure redundancy without single points of failure. Agencies rely on continuous service availability, so robust failover mechanisms are critical.
10. **User-Friendly Portal:** The contract should emphasize an intuitive, user-friendly portal for agencies to manage services, track usage, and access information easily.

A list of the questions provided in the MFN-2 User Survey, as well as detailed analysis of each response is included below as Appendix B.

3.2 Evaluation of MFN-3 Contracting Options

The MFN-3 contract could be developed as a multi-award contract. Under such a contract, the State could break the contract into several components (functional areas) with an awarded vendor for each specific functional area. In addition, each functional area could also be itself a multi-award. A multi award contract may provide benefits to the State for the MFN contract services. The MFN-1 and MFN-2 contracts were both single-award, all-encompassing contracts in that a single contractor was awarded the contract to design, build, and operate the MFN infrastructure. The contractor established sub-contract agreements with various partner companies including telecommunications service providers to support the MFN.

There are benefits to such a contract in that the complexities of managing the various components of the MFN solution are offloaded completely to the awarded contractor. A single contract award option provides a direct business relationship between the prime contractor and the subcontracted service providers that contractor chooses to partner with. In exchange for this management function value-add, the contractor typically charges fees in addition to the fees it directly incurs to deliver the service.

In contrast to the current and previous contract models, the MFN-3 contract could be divided into separate functional areas. The MFN architecture could be separated into distinct functional areas within the MFN contract, with separately awarded contractors designated for each. Such an approach may offer DMS benefits such as the potential for overall reduced costs, as the management overhead for these additional functional areas from a single prime contractor could be avoided. Since the MFN will still require an operational lead contractor responsible for end-to-end service support, some overhead for these functions will still be expected as for each functional area added to the contract, management complexity increases.

While it is possible to define clear demarcation points in the MFN architecture for each potential functional area, the MFN must function as a cohesive system to deliver the required services to subscribers. Disruptions and impairments to subscriber services can occur within any of the end-to-end components. As the number of demarcation points in the end-to-end services increase, the operational complexity also increases as each distinct functional area becomes a potential source for the impairment. Disruptions to service are typically easier to diagnose to determine the functional area causing the issue. Impairments, however, can present additional difficulty in isolating root causes and requires cooperation between each of the distinct functional area operational support teams.

A strategic separation of the telecommunication services within the MFN should be considered. Separating the telecommunication services, specifically the last mile services, into a distinct functional area within the MFN contract could provide DMS with increased control on this critical area of the MFN architecture. Separating the MFN last mile services into a distinct functional area would allow DMS to select the best value service option for each facility supported by the MFN.

Due to the diversity of Florida telecommunications services, this functional area would benefit from a multi-award type service contract where DMS could obtain competitive costs directly from multiple vendors for each MFN connected facility. This separated functional area would permit DMS to be the direct customer of record for all procured services, while the multi-award nature would help to ensure Florida obtains the best value solution available for each of the MFN facilities. Allowing multiple

service areas or regions within the telecommunications functional area is also warranted for consideration. A telecommunications functional area could be further segmented into individual services that the MFN could then leverage as required. The following services should be considered for further break out:

- Metropolitan Area Network Ethernet Services (MEF 2.0 compliant)
- Dark Fiber services
- Optical/dedicated transport services (DWDM/OTN)
- Transit Internet Services (ISP)
- Commodity broadband Internet access services (ISP – Cable, xPON (Passive Optical Network), Cellular, Satellite, WiSP (wireless Internet service provider))

Other functional areas that could be considered are as follows:

- Premises Based Security Services (Boundary)
- Cloud Service Provider Transport
- Centralized VPN Services
- Managed CPE/SDWAN

While the above services could be segmented into separate functional areas, they will pose challenges in complexity. If a multi-award model is selected, a more consolidated approach to the contract may be warranted to allow for a single integrated solution to be developed more easily. Separation of the leased telecommunications service components would still be beneficial to include in the contract, as it is likely that any MFN contractor would require associated subcontract agreements for these services under either contract method. Separating the telecommunications services into a separate functional area would ensure that DMS remains the customer of record for any procured services and ensures that the procured services can remain in place during transitioning of any of the other functional aspects of the MFN. Once the baseline infrastructure is established, future contract interactions could further define additional functional areas more easily as the demarcation points between them will become more concrete in nature. This approach could also allow DMS to expand the services provided by the MFN through the addition of new functional areas in the future as needs are identified.

3.2.1 Last-Mile Services

Last mile services are telecommunications services that extend the MFN backbone out to the various subscriber facilities throughout the state. While there are options for how last mile services can be designed for the MFN (see section 3.3.2) the standard method for supporting last mile services is through the leasing of services provided by a ILEC (incumbent local exchange carrier) or CLEC (competitive local exchange carrier). 100% (excluding the Primary Data Center (PDC) facility) of the current MFN-2 facilities are supported through this method.

The current MFN-2 contract combines last mile leased telecommunication circuits with the overall MFN solution as an end-to-end bundled service offering from the provider. The MFN contractor is responsible for providing end-to-end service to each facility serviced by the MFN. The MFN contractor establishes partnerships with ILEC and CLEC providers which are then leveraged by the MFN

contractor to extend services to each required facility. While this has proven to be effective under both MFN-1 and MFN-2, there are benefits to be considered in separating the last mile telecommunications services within the MFN contract.

The primary benefit to separating last mile telecommunications service procurement from the MFN contract is the designation of the State as the customer of record for last mile service contracts. By separating telecommunication service procurement from the MFN contract, DMS will ensure the customer of record for all procured services under that telecommunications contract is DMS directly. This permits the circuits procured to be fiscally separate from the MFN backbone provider. The MFN primary contractor, in coordination with the customer agency, would remain the designated DMS support contractor responsible for the procurement, implementation, monitoring, and day to day operations and maintenance of the end-to-end MFN services. The MFN primary contractor would perform this work as a designated agent of DMS under the MFN contract and would be required to select from vendors that DMS has competitively vetted and awarded. This permits DMS to retain or re-negotiate last mile circuit leases as required independently from the MFN backbone contract in the event of any future migration away from the primary contractor.

Due to the fractured landscape of LEC services within Florida, such a telecommunications contract to support the State of Florida would be suited for a multi-award-based contract. The large geography of Florida results in regions where different LEC service providers have invested heavily in infrastructure, while other providers in the region have not. The investment level varies among carriers, region by region, resulting in a commercial telecommunications landscape that is not consistent throughout Florida. A multi-award contract permits DMS to award the contract to multiple telecommunications service providers that can provide the base services required by MFN.

This contract should include MEF 3.0 EvPL[21] as well as Emulated Local Area Network (E-LAN) based services as a primary option to support the MFN access connectivity. The contract may also be extended to provide broadband ISP services as a separate functional area. Broadband ISP services could be coupled with SDWAN technology to support lower SLA extension services (see below Section 3.3.2.2 on introduction of SDWAN). This establishes a procurement vehicle that allows DMS to procure telecommunications services through small, site specific, competitive procurements under the telecommunications contract for all MFN serviced facilities.

The contract could also include dark fiber and OTN based services as another functional area, allowing the contract vehicle to be used for multiple MFN connectivity requirements. DMS would issue requests for quotes under the specific functional area required for the MFN for each facility serviced by the MFN, then select the best value offer from the providers.

It will be important for the MFN backbone to provide multiple aggregation points of presence from which bidders can select. The MFN backbone points of presence will serve as the aggregation points where the last mile service provider services are integrated into the MFN. DMS will benefit if potential aggregation points are established within each of the FCC-designated LATA boundaries, as ILEC providers may still be bounded by them and could be precluded from direct bidding otherwise.

-

[21] https://wiki.mef.net/display/CESG/EVPL

DMS should develop the contract so that providers are restricted from charging directly for any service elements associated with the aggregation site(s). The providers should factor the costs associated with the aggregation site elements of their solution into the individual remote circuit cost elements.

A direct cost comparison between a diversified last mile contract solution and the current bundled MFN solution cannot be derived under this analysis. The true costs of the last mile solutions provided by the current MFN are unknown to DMS, as the vendor currently provides flat rate pricing for the MFN, in that all sites subscribing to the same bandwidth and service type pay based on the same fee structure. The actual last mile costs are bundled separately from the overall cost, and then aggregated within the current costs structure under the current MFN-2 contract. In addition, current competitive costs for MFN sites cannot be determined until such a contract exists. To demonstrate the potential cost avoidance of a multi-award per site best value method of selection, the results seen by another state are representative.

The State of Maryland leverages a multi-award Data Communications Master Contract[22]. That contact has several defined functional areas including Functional Area III – Last Mile Access Data Services. The State of Maryland Department of Information Technology was contacted about this contract to inquire how it was performing and if there were any measurable cost avoidance data associated with it. The Maryland Department of Information Technology provided a document summarizing a recent set of projects they engaged in to replace T1/copper-based services with modern Ethernet/fiber services. That project leveraged the Maryland Data Communications master contract to obtain costs from potential vendors for 68 facilities.

[22] https://doit.maryland.gov/contracts/Pages/DataTelecommHome.aspx

The data from the project telecommunications proposals was provided by the Department. Analysis of the data showed that selecting the lowest cost service for each individual site had a wide range of cost avoidance, as compared to the results if all sites were awarded to a single vendor. In that project it was also found that 11 sites (16% of all sites) within the scope of the efforts were only serviceable by a single vendor. Across all 68 sites, the median of attainable cost avoidance for the last-mile servicing portion of an individual circuit's cost, if the lowest cost were chosen for each of the circuits was 44% while the average was 39%. The following graph shows the distribution in proposed 10-year cost between the highest cost vendor and the lowest cost vendor across the 68 sites in this representative project:

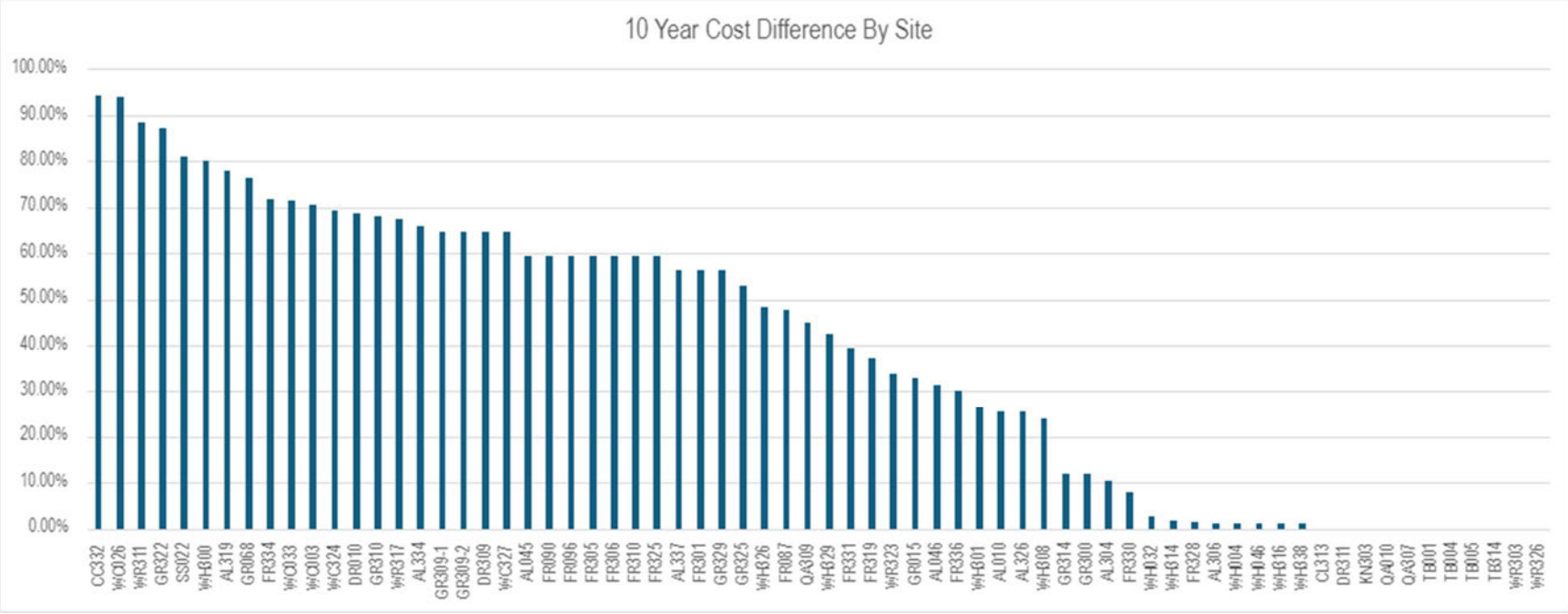


Figure 9: Vendor Bid Differential for networkMaryland Project

The applicability of this data assumes a comparable last-mile environment in Florida. Potential variances in these assumptions may impact the level of cost avoidance achieved by the State, such as:

- The percentage of sites serviceable by a single last-mile vendor may differ in Florida. Based on interviews with the DMS team and an analysis of the geographical distribution of circuits in Florida, the number of sites only serviceable by a single last-mile provider will likely be fewer than Maryland's, which experienced a 16% rate of sites only serviceable by a single vendor.
- In markets serviced by more than one last-mile vendor, the number of available vendors across Florida may be greater than in Maryland leading to increased competition. For example, Florida's business-friendly environment has contributed to the emergence of local consumer-grade fiber ISPs in Florida, such as MetroNet in Tallahassee, IQ Fiber in Jacksonville and Gainesville, and Frontier in Tampa. The Orlando and Miami markets are each currently serviced by at least 6 ISPs offering Fiber in addition to the traditional cable, DSL, and Satellite-based ISPs. This broader emergence of new local ISPs has not been experienced throughout Maryland, which may lead to greater competition in Florida than seen in Maryland.
- The core vendor may impose a service charge for the management of each circuit that would reduce the amount of cost avoidance achieved per circuit. This service charge would likely not approach the cost of the circuit itself and should be negotiated by DMS with a maximum allowable percentage based on the actual circuit cost. As long as the actual percentage of cost avoidance achieved through competitive procurement exceeds the percentage service charge imposed by the core vendor for the management of the last mile circuits, measurable cost avoidance should be achieved.

These factors are summarized below:

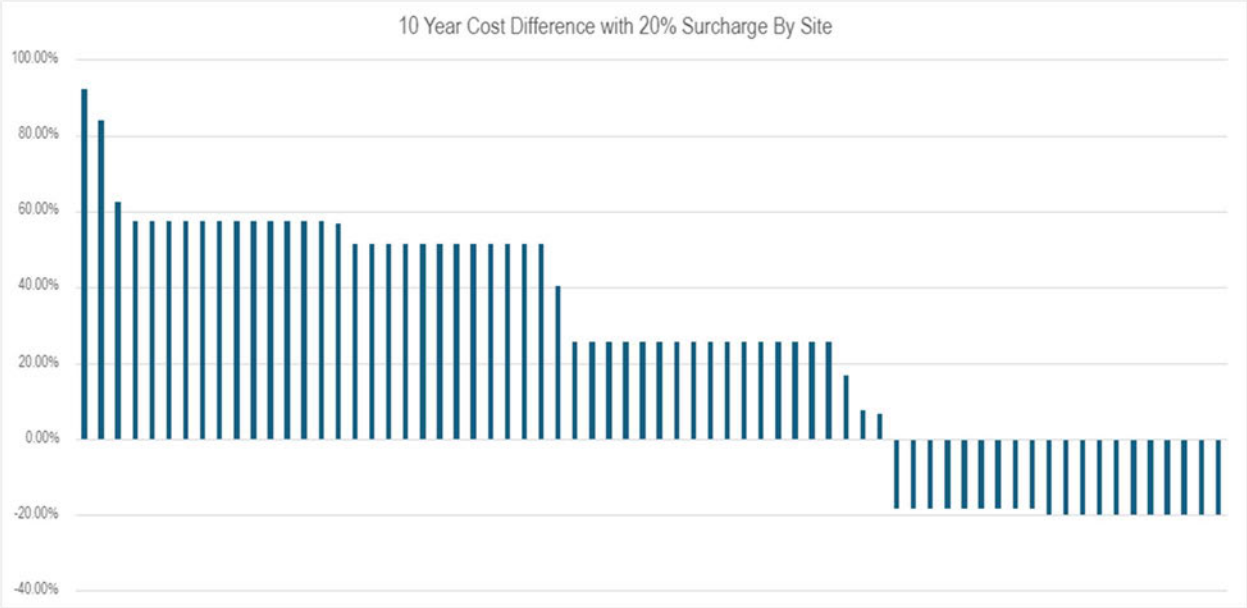


While each state and set of circumstances will always have variance and cannot be assumed to be equivalent, this representative example offers guidance on the potential cost avoidance that may be achieved through adoption of a competitively bid, multi-vendor last mile solution. Applying the average cost avoidance percentages achieved by Maryland through their contract to the current MFN

wholesale rates for the existing MFN services would result in a potential average cost avoidance for MFN and FIRN Services of 39% over 10 years.

There is a potential that if the core service provider must work with a greater number of last-mile service providers, they could add a per-circuit maintenance surcharge that would offset some of the savings that could be seen through multi-vendor competition. To account for this, a scenario was worked through to estimate the impact.

The average monthly recurring cost of each circuit in the reference Maryland project was $512/month. Based on this number, a potential 20% service fee imposed by the core vendor would be priced at an average of $102.40/month. Applying this 20% service fee to the lowest monthly recurring cost of each Maryland circuit decreases the average savings per circuit from 39% to 25%.



Of the 68 circuits measured in Maryland, 20 circuits had a cost differential small enough to result in a higher cost with a service fee charged than the initial savings that would have been realized. This includes a 20% service fee applied to the 11 circuits where there was only a single vendor available. The figure below summarizes the application of this surcharge to the original data provided above.

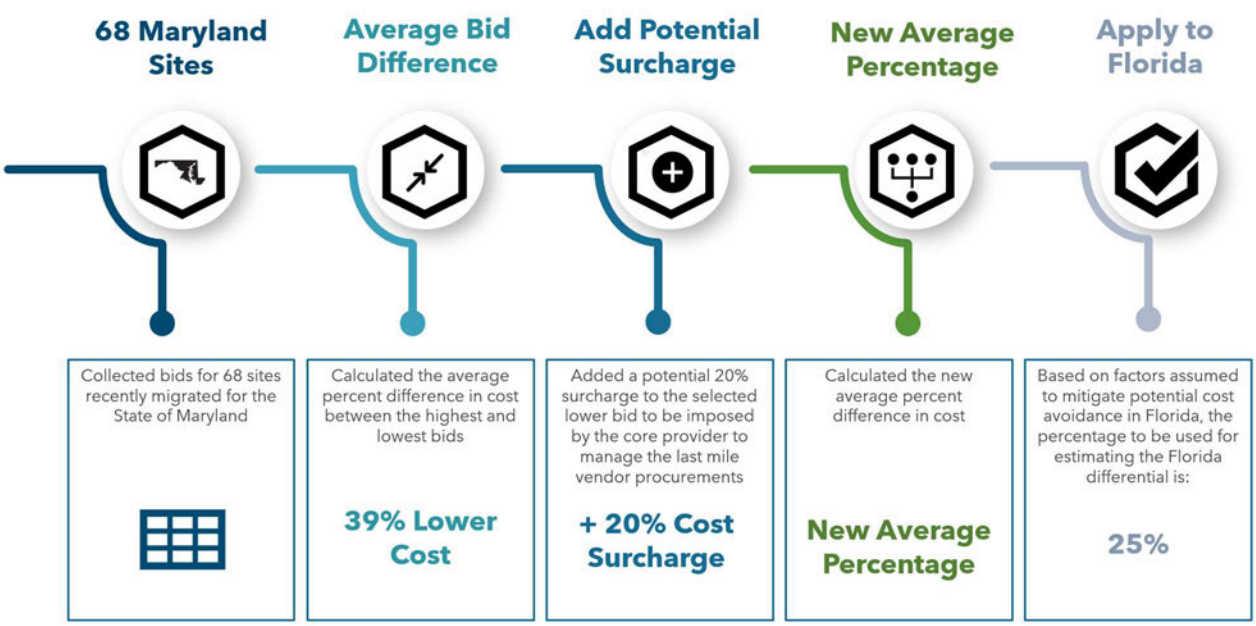


Figure 10: Basis of Estimated Cost Avoidance with Multi-Vendor Last-Mile Services Model

To maximize cost avoidance, DMS should work to negotiate the lowest possible service fee per-circuit or consider negotiating a flat rate for management of circuits that would result in a favorable average percentage when compared to anticipated last-mile services cost.

With the implementation of a multi-award last mile option, DMS would procure the last mile services directly from the awarded vendors and provide the resulting services to the MFN backbone contractor to support last mile extension from the backbone to the MFN subscriber facilities. Under such a model, DMS would either need to specify where the backbone PoPs must be located in the contract (state facilities) or require that the backbone provider designate a specific "meet me" point facility in each defined LATA to ensure a competitive landscape for the last mile vendors is maintained. In addition, the MFN contractor may also need to provide letters of authorization to DMS to permit them to order and deliver circuits to the MFN backbone contractors point of presence within each of the designated facilities if those facilities are commercial datacenters.

Under such a contract scenario DMS would be the customer of record for all last mile circuit/services and DMS would retain vendor selection approvals for each required service. While this will permit last mile services to remain in place under a backbone provider transition, there are additional complexities under such a contract scenario that must be considered. If the backbone vendor is permitted to select their own backbone facilities, it is very likely that the core circuits (integration point for leased services into the backbone) would not be able to be retained during a contract transition as the backbone facilities could change. While the remote physical circuits could remain in place (MFN facilities), new core UNI services (considered aggregation interfaces with the backbone) as well as supporting logical circuits would be required resulting in some level of transitional activities still required. The overall costs for transition under this scenario would still be lower than the current-state single-vendor model since most of the physical circuits could remain in place.

If the State chooses to retain the current single-award as-a-service contract model without a multi-vendor last-mile contract separation, consideration should be given to increasing DMS influence over the vendors' last mile partner selections for MFN sites. Under the current model, the MFN vendor has the ultimate authority in selecting last mile providers for each of the MFN sites. Since the MFN vendor is required to offer fixed rate services to all MFN facilities, the ability for the vendor to select the most cost-effective provider/partner service is critical to their ability to control costs. It may be beneficial under such a contract agreement for DMS to permit a per site cost model from its MFN vendor and perform the conversion of those costs to a fixed model to the MFN subscribers internally with DMS. If DMS were to permit the MFN vendor to provide per site pricing, the service solution for each facility could be more flexible in that the vendor could offer several options to DMS for each facility and permit DMS to select the best value option which may be a higher cost option for a more reliable last mile offering. The MFN subscribers are very supportive of a fixed fee-based service, however, and therefore DMS would need to develop a rate structure for the services provided by the MFN for the subscriber community to standardize the per-facility costs to DMS. While this would increase complexity/involvement by DMS in developing the rate structure, it would also permit DMS to leverage the rate structure to establish a funding pool (excess charged rates vs. costs to DMS) that could be used by DMS to offset special construction and or other service/investment costs.

3.2.2 Single-Award and Multi-Award Approach for Last Mile Services Comparison

Section 287.0571 (4)(f), F.S. - An analysis of the advantages and disadvantages of each option, including, at a minimum, potential performance improvements and risks.

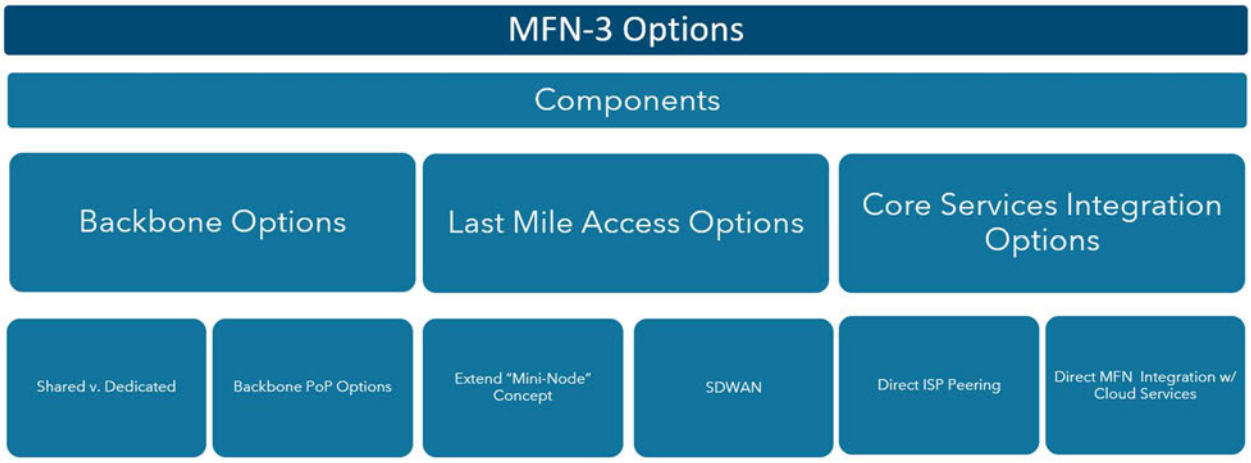
The advantages and disadvantages of each contracting approach for last mile and ancillary services are provided below:

	Single-Award Last Mile and Ancillary Services	Multi-Award Last-Mile and Ancillary Services
Last Mile Component Implementation Influence		
Advantages	• Increased influence of DMS on the single-vendor to implement Mini-Nodes	
	• Increased influence of DMS on the single-vendor contract to implement SDWAN	
Disadvantages		• Potentially varied (inconsistent) levels of compliance with DMS-preferred Mini Nodes design and implementation requirements
		• Potentially varied (inconsistent) levels of influence of DMS on SDWAN implementations

	Single-Award Last Mile and Ancillary Services	Multi-Award Last-Mile and Ancillary Services
Cost Avoidance		
Advantages		• Competitive bidding of last mile access service extension circuits can lead to lower costs for DMS and subscribers on a per site basis
		• Ability to allow multiple functional areas can allow best-value selection of providers for each functional area
Disadvantages	• Potential cost avoidance from last mile access service extension circuits through subcontractors are unlikely to be passed on to the State by the prime contractor	• Potential increase in staffing
	• Subcontracting is only between the prime and the last mile service providers – no DMS influence on contracting structures or functional areas	

	Single-Award Last Mile and Ancillary Services	Multi-Award Last-Mile and Ancillary Services
Transition		
Advantages		• No change of ownership on every transition to a new prime vendor
		• Ability to dictate the contract term for last mile service contracts, independent from the MFN contract term
Disadvantages	• Every change of ownership on every transition to a new prime vendor will require a complete migration of MFN	
	• Subcontracting is only between the prime and the last mile service providers – no DMS influence in renegotiating outside of contract terms	

3.3 Evaluation of MFN-3 Component Level Options



This section outlines options architectural component level options that should be considered for MFN-3. The options identified provide options that DMS should consider when determining how the MFN-3 infrastructure solution is designed by the primary vendor. The options presented are organized into three (3) sections based on the component of the MFN architecture that they relate to.

The figure below provides a high-level architectural overview of the MFN detailing the primary components of the infrastructure. The components of the MFN are not directly observable by the subscribers. Subscriber facilities (sites) are physically connected to the MFN and various logical services are exposed to them through this connection (UNI – user to network interface). There are underlying complexities and additional services not directly depicted (i.e., Remote Access/VPN and Ancillary Services, distributed security monitoring) as the diagram is designed to detail only the primary services leveraged by the MFN community.

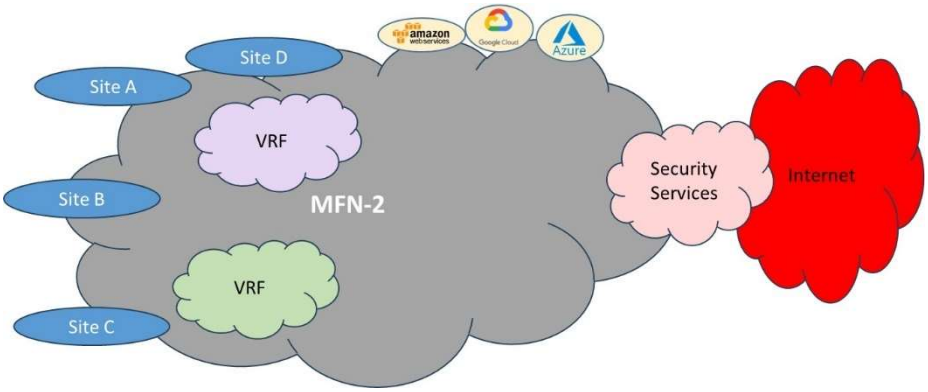


Figure 11 – MFN High Level Diagram

Figure 11 provides an abstracted view of what is observable from the viewpoint of a subscriber. There are complexities within the MFN infrastructure that support the delivery of the various services available through the solution. Figure 12 provides a view of the MFN infrastructure with a layer of abstraction removed to show the underlying architectural components.

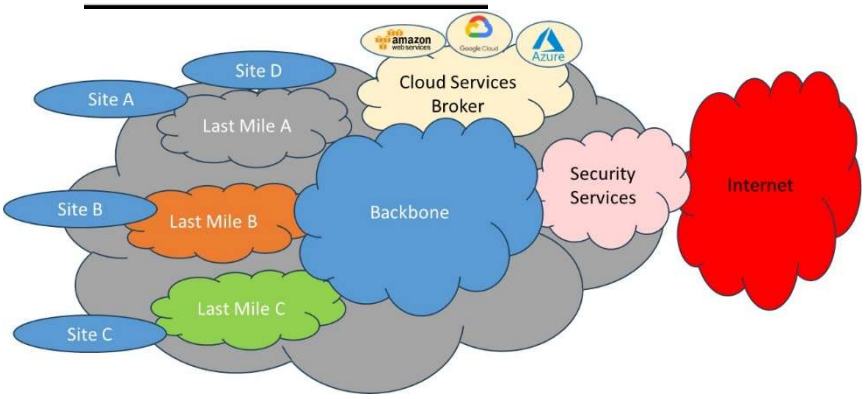
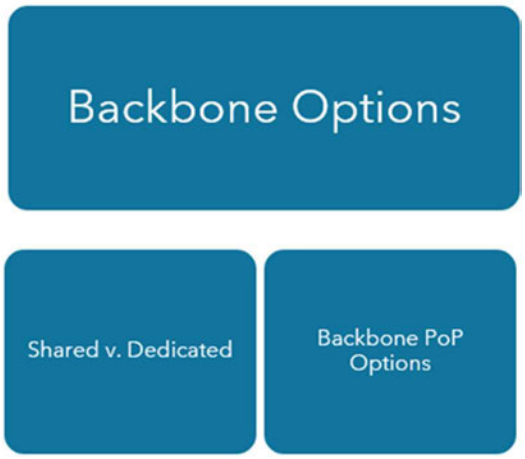


Figure 12 – MFN Level 2 Functional Diagram[23]

As pictured in Figure 12 above, the MFN is made of several distinct functional elements. The backbone element is considered the central component of the architecture, integrating all other elements into a single cohesive service delivery solution for the subscribers. The backbone element consists of the physical facilities, network equipment, and fiber optic assets leveraged to establish the interconnected core for the MFN. Core services are then extended out to subscriber facilities (sites) through last mile services. Internet, security, and cloud services are also integrated into the core at select locations to permit communication between the MFN and these services. The various options presented in the following sections relate specifically to these functional elements.

In considering incremental improvements to a vendor-owned and vendor-managed MFN-3 model, DMS should develop requirements that encourage the provider to consider these component options and the potential impact they could have on cost and MFN performance to the state.

3.3.1 MFN-3 – Backbone Options



This section provides details on several options that relate to the backbone of the MFN. An evaluation of shared vs. dedicated infrastructure is provided as well as various options for consideration on how DMS could establish a backbone infrastructure.

[23] Note – Current MFN-2 architecture extends security services to the boundary between the last mile and backbone. This diagram only depicts the centralized services such as boundary and remote access services.

3.3.1.1 MFN-3 Shared vs. Dedicated Infrastructure

Under the MFN-1 and MFN-2 contracts, the State required the contracted vendor to establish a dedicated backbone infrastructure that was only leveraged by the MFN subscriber community. This requirement for dedicated infrastructure as opposed to leveraging shared (public) infrastructure is an option for MFN-3 that warrants evaluation.

A dedicated MPLS backbone consisting of six (6) core nodes was established under the MFN-2 contract. Fiber optic resources were then leveraged to provide interconnects between the core nodes in a redundant manner. The nodes leverage MPLS and supporting control plane protocols to then establish end to end provisioned services. The design and technology leveraged to create the MFN-2 backbone are consistent with the backbone solutions deployed by commercial carriers to deliver similar services to their customers.

Functionally, there is no difference between the dedicated MFN-2 design versus leveraging the commercial backbone of a single service provider, as both solutions leverage the same equipment types and protocols to provide the same basic services. The service architecture supporting Florida, as detailed in Figure 12, can be supported using either a dedicated backbone infrastructure or the shared backbones within existing large commercial carrier infrastructures. Leveraging the investment made by commercial carriers to support their customers can yield a more cost-effective solution for the State as the costs for engineering and managing the infrastructure can be amortized by the provider across a larger customer base. This can result in lower costs to deliver services to each. The RFI (Request for Information) conducted between the MFN-1 and MFN-2 contracts, however, found that this cost avoidance potential was minimal at the service scale associated with DMS/MFN requirements.

There are several benefits to establishing and leveraging a dedicated backbone infrastructure for the MFN versus leveraging a shared commercial solution:

- Meeting the State's unique requirements using the public network presents its own set of issues. As technical requirements, laws, and regulations governing data at rest and in transport continue to be refined and evolve, the use of dedicated infrastructure provides increased flexibility to support them.
- A dedicated network approach has allowed upgrades to keep MFN "state of the art," elastic in nature, and allowed addition of network technologies and services as the need has arisen.
- A dedicated network approach provides the ability to more rapidly deploy new technologies such as Bi-Directional Forwarding Detection (BFD) for emergency services, Get VPN, and customized solutions within the MFN as compared to the ability to do so over commercially shared public infrastructure.
- A dedicated network approach provides the ability to consider, test, and adopt customer requested solutions that integrate elements of both core and CPE.
- Dedicated infrastructure allows a support staffing model that ensures familiarity with network elements both from the provider and from the customer.
    - Facilitates lines of communication by providing direct access to tier 3/tier 4 support to customers
    - Dedicated personnel allow much easier compliance with Criminal Justice Information System (CJIS)[24] and other security requirements.

[24] https://www.fbi.gov/services/cjis

  - Institutional knowledge over many years of experience with the State's networks, administrators, and requirements
- A dedicated network approach provides increased flexibility in solution design.
  - Ability to introduce and support tightly integrated solutions and technologies that overlay the dedicated core, such as emergency services voice networks, Session Initiation Protocol trunks, and hosted voice solutions.
  - Read-only control plane statistics access to customers on all dedicated equipment.
  - Ability to fully integrate new initiatives such as Next Generation 911 (NG 911) projects into the dedicated core/local loop/CPE providing elements otherwise unavailable such as the "emergency voice" QoS profile that differentiates emergency service traffic from that of other users
  - More flexible QoS model customizations permitting DMS to tailor the operational aspects of the shared backbone capacity to align with the State's requirements.
- The use of dedicated infrastructure lessens the potential risks of performance impacts associated with cyber threats against non-MFN subscribers.
- The use of dedicated infrastructure permits MFN/DMS to define and manage over-subscription ratios directly ensuring capacity to support critical state government business functionality.

There are aspects of the existing MFN service solution that would not easily be replicable under an MFN that leverages a shared public backbone. The current distributed IDS security monitoring solution that permits monitoring of all MFN transported traffic would not be possible under a shared infrastructure-based solution. The distributed traffic flow monitoring solution requires that "tap" devices be installed at strategic integration points within the physical infrastructure. Commercial carriers are unlikely to permit such devices to be implemented within their commercial public infrastructures as doing so could expose traffic not associated with the MFN.

DMS should continue to build on the successful attributes of MFN-1 and MFN-2. The centralization of buying power under the MFN programs has proven successful for the State of Florida. The architecture established under MFN-1 and evolved under MFN-2, consisting of the network core based on MPLS technologies, integrated with last mile ILEC and CLEC provider infrastructures, has provided MFN and its subscriber community with consistent reliable performance. This architecture also supports the flexibility required to further the evolution of the program through the introduction of advanced security and other over-the-top value-add services. The standardization on ethernet for last mile access that occurred under MFN-2 has also aided Florida in reducing complexities and costs associated with specialized CPE hardware while allowing MFN to keep pace with similar commercial offerings. Integration with cloud service providers has further extended the usability of the MFN infrastructure and permitted the subscriber community to adopt cloud strategies more easily. The flexibility of the MFN dedicated core backbone has permitted DMS to implement managed security offerings, including distributed traffic monitoring solutions that allow subscribers to operate at a higher level of security monitoring than would be achievable on their own at similar cost.

3.3.1.2 MFN-3 Backbone PoP Facility Options

Site selection for the MFN-3 vendor's core backbone facilities is an important component of the evaluation that DMS will perform as part of the procurement and should consider several factors. The current MFN-2 backbone has been established in commercial collocation datacenters provided by

LUMEN[25]. The current MFN-2 contractor has partnered with LUMEN to obtain datacenter rack space at the core pop facilities where the MFN backbone has been established. The use of a commercial datacenter to support these critical infrastructure components allows the MFN to leverage the investments made by the datacenter owner(s) in redundant power, HVAC services, as well as physical security without requiring direct management of that infrastructure. A notable nuance to the current MFN-2 solution is that the owner of record for the collocation agreements is the MFN-2 contractor, not DMS. This requires that any change in contract holder from MFN-2 to MFN-3 results in the establishment of new core infrastructure, even if that infrastructure were to be installed within the same designated facilities. The leasing agreements for rack space within these facilities are not typically transferable. There are alternative options for DMS to support MFN backbone facilities that warrant evaluation for MFN-3.

There are several factors that DMS should consider when evaluating the site facilities selected by the MFN-3 vendor to support the MFN-3 backbone requirements. DMS should ensure the vendor establishes backbone points of presence that permit the most open access to LEC service provider infrastructures. Where possible, it is recommended that the backbone facilities supporting MFN-3 be established in a manner that can provide two (2) physical aggregation points within the core POP facilities for each potential LEC providing last mile services. This ensures the MFN can support the redundancy services currently available under MFN-2 for non-FIRN subscribers. This provides the ability for MFN to support site level redundancy for these critical integration points where required. In addition, DMS should consider the following factors when evaluating the PoP facilities envisioned by the prospective MFN-3 vendor:

- **Physical Site Access**: The core PoPs will exist within the highest levels of the MFN-3 service hierarchy. These facilities will serve as aggregation points for LEC integration as well as transit points for interconnections between the various PoP facilities that will establish the MFN-3 backbone. It is, therefore, critical that DMS evaluate site access as a factor in reviewing vendor PoP facility selection. A preference for direct 24x7x365 physical access should be adopted. "Direct Access" is defined as the ability for DMS as well as the contracted vendor to access the site and specific room/location where the MFN-3 equipment is located without requiring any other party involvement. Direct Access for background-checked contractors is often facilitated through a combination of biometric, badge, and other two-factor authentication methods to allow 24x7x365 access. This is in contrast to "Facilitated Access" where DMS would be required to arrange access through a third party/site tenant that would be required to meet the DMS team on site to permit access or otherwise arrange access for the DMS staff. While it is feasible to leverage facilities with only facilitated access available, it should not be the preferred option as quick access to sites during operational events is a critical factor to ensuring overall network uptime and availability.
- **Power Services**: MFN core sites should be established in facilities where augmented power services are available. Such facilities should, at a minimum have a facility power generator that is regularly serviced and has a method of ensuring fuel is supplied during natural disasters and/or other such events. A facility/room UPS system is also preferred but is not considered critical as rack mount UPS solutions can also be leveraged if required to provide appropriate hold over power for transition events between commercial and facility backup power services.

[25] MFN-2's colocation datacenters were originally provided by a combination of Level3 and CenturyLink. Over the duration of the MFN-2 contract, Level3 was purchased by CenturyLink in 2017, and the company rebranded as LUMEN in 2020.

- **HVAC Services**: The equipment that will be leveraged to support MFN-3 backbone services will generate heat that must be factored into site selection. It is important that the facilities selected to support these critical backbone facilities are augmented with sufficient HVAC to ensure the room(s) supporting the MFN maintain proper operating temperatures and humidity levels to properly support the expected thermal loads. Where possible, solutions should be redundant to protect against systems failures that could result in nodal failures.
- **Connectivity**: Each of the core PoPs supporting the MFN backbone will support the aggregation and transit services for a larger number of subscriber services. It is therefore important to ensure that each backbone facility has connectivity options that can provide as much diversity as possible. Where possible, there should exist at least two (2) completely diverse communication paths that have sufficient capacity to support the expected MFN communication requirements. Typically, this will be fiber optic-based communication services. A preference for facilities with diverse building penetration and conduit systems should be selected, where available. Shared building penetrations can be supported but the amount of shared conduit should be reduced, where possible to limit risks of full-service disruption to the PoP due to single events. Access to multiple potential dark fiber providers including state/local/municipality assets should also be evaluated and preferred as site selection criteria. If sites are not already connected to fiber resources, geographic proximity to such resources should be evaluated as fiber construction requirements can add significant costs to the solution.
- **LEC Infrastructure Availability**: DMS should also take into consideration LEC infrastructure availability to/from potential facilities as a factor in site selection for the MFN-3 backbone PoPs. A primary role for each MFN-3 backbone PoP will be to aggregate MFN subscriber services in the corresponding region to provide access to the other regions and supported services. It is, therefore, important that these sites have existing direct integration or the capacity for direct integration with as many LEC service providers as possible within the PoPs' expected service region. The evaluation should also include considerations for access to potential state/local fiber asset access in addition to commercial infrastructures.
- **Proximity to Transport Resources**: Another factor that should be considered during vendor backbone site evaluation is the site's proximity to available backbone transport resources. Construction costs to extend fiber resources to facilities can be a large factor in the overall costs for establishing the backbone.

3.3.2 MFN-3 Last-Mile Access Options



Another area of consideration for component level options to support the MFN focuses on the last mile service extension elements. The last mile component of the MFN architecture extends the services provided by the MFN backbone to the subscriber's facilities. There are two options presented in the sections below for consideration for inclusion into MFN-3. For each option, information on the potential costs is provided.

3.3.2.1 Mini-Node Deployments for Multi-tenant Facilities

MFN-2 provides a reliable, high-speed connection to the State's PDC, also known as the SSRC. The PDC service in Tallahassee enables MFN-2 backbone traffic and Tallahassee MAN traffic to flow into the PDC. MFN-2 has implemented a mini-node at this facility where the MFN-2 service provider provides physically diverse backbone fiber routes from the PDC implemented on the Tallahassee MAN. The service has the same SLA guarantees as provided to the MFN-2 core. Traffic is monitored for malware by the IDS located at each core node. This mini-node approach permits MFN-2 to aggregate connectivity requirements for the subscribers at the facility over a shared solution.

There are other sites within the MFN-2 service environment that could benefit from extending the mini-node architecture to additional sites. Currently, 16% (394/2506) of the MFN-2 services facilities have more than one (1) MFN subscriber service delivered. The current MFN-2 model for service delivery extends a separate last mile service (circuit) to the facility for each required subscriber. This results in a one-to-one mapping of leased circuit costs per subscriber within the MFN-2 facilities. Extending the MFN to these facilities, like the mini-node approach currently used for PDC, would permit DMS to perform the same service aggregation achieved in the PDC model for each of these multi-subscriber facilities.

Figure 13 provides an overview of the current method for servicing sites with multiple subscribers within MFN-2. In the current method, each subscriber receives a dedicated UNI (user to network interface) connection from the last mile service provider (LEC). A separate virtual circuit is provided by the LEC for each subscriber MFN service. While logical services can be multiplexed over the same physical connection, a distinct UNI is implemented to support each distinct subscriber serviced by the MFN.

Circuit charges by vendors are typically charged based on physical UNI (access port) coupled with separate charges for each logical service delivered (virtual circuit) based on the bandwidth subscribed. Port charges are typically fixed based on the type of interface (100M, 1G, 10G, etc.) while virtual circuit charges vary based on subscribed bandwidth. As subscription rates increase, the cost per megabit per second (Mbps) decreases. For example, in the current MFN-2 pricing structure, a 10Mbps has a $48/Mbps monthly rate (wholesale local loop - $480 total) applied while a 1000Mbps service has a $1.95/Mbps monthly rate applied (wholesale local loop - $1950 total). As the subscribed bandwidth rate increases, the cost per Mbps decreases substantially. For this reason, it is beneficial to aggregate bandwidth at a facility to a single logical service to obtain the lowest cost per Mbps rates.



Figure 14 provides an overview of a consolidated approach to providing the same MFN services to a facility using a mini-node approach. As detailed in Figure 14, an MFN device is installed at the facility between the subscriber CPE devices and the last mile provider. This MFN node aggregates all the subscriber services together at the facility. Only a single UNI port and circuit is requested from the last mile provider to connect this MFN extension node (mini-node) to the MFN backbone. The bandwidth requirements for the facility are then consolidated into that a single leased service, permitting DMS to obtain the lowest cost/Mbps possible by leveraging the consolidated purchasing power.



Separate subscriber UNI connections are maintained but delivered directly on the MFN node installed within the facility. The MFN node maintains logical service separation between subscribers using similar methods as supported by the core nodes. There are several viable technical options available for the MFN to support a mini-node solution at remote multi-subscriber facilities. This would permit the MFN to procure bandwidth at the reduced cost per Mbps rates associated with the higher capacity services resulting in a lower overall service cost for delivering the same subscriber services. The MFN would incur additional costs for the mini-node hardware as well as maintenance and support costs

which would offset the cost avoidance to some degree. A positive ROI is still likely depending on the level of consolidation achieved and the MFN-3 vendors' willingness to adopt the required architecture.

In addition to the cost avoidance associated directly with the aggregation of service bandwidth, the MFN could also realize additional cost avoidance through deploying oversubscription of bandwidth at these facilities. Modern applications are bursty in nature, characterized by short periods of high utilization of bandwidth resources, followed by longer periods of little to no utilization while the data is consumed and analyzed by the users. While the addition of real time applications such as video conferencing and voice services change this general behavior, today's general business application-use networks still follow this general trend.

Modern networks are packetized and leverage statistical multiplexing methodologies to distribute available bandwidth resources among competing application flows. As currently deployed in MFN-2, quality of service mechanisms further enhance the ability of packetized networks to leverage network resources more efficiently, while simultaneously ensuring that critical and/or real time flows are provided specialized treatment to maintain user experience. In such networks, it is standard to deploy a subscribed ratio of bandwidth that is not equal to the full downstream capacity of clients. This concept is known as the oversubscription of bandwidth where the total downstream capacity of a network can exceed the uplink capacity. MFN could employ over-subscription of bandwidth policies on the mini-nodes, further resulting in overall cost avoidance through more efficient use of bandwidth resources.

Experienced operating government networks similar to MFN has yielded successful results leveraging 4:1 and higher subscription ratios. Within these networks, internal studies conducted found that ratios of up to 4:1 can be deployed on aggregation wide area network links and the resulting average bandwidth resource utilization remains less than 50% during peak periods, with associated peak utilization rates remaining below 80%. Packet loss rates for all transported traffic remains less than .001% even within the lowest class queues, with 0% rates for the higher guaranteed traffic classes. Subscription policies must also ensure that upstream bandwidth capacity always exceeds the highest capacity supported subscriber service by 20% to ensure no single customer/service utilization event can result in a direct impact to all other customer traffic. In evaluating MFN-3 core and backbone vendors, over-subscription ratios to enable aggregated service bandwidth cost avoidance should be evaluated, as over-subscriptions can have a significant beneficial impact on associated MFN service costs.

An evaluation was conducted as a part of this business case leveraging the mini-node approach, to provide a cost avoidance potential for utilization of this concept within the MFN. The current services were then analyzed to determine how many existing facilities have more than a single subscriber service provisioned, to understand which would be able to take advantage of the mini-node solution. Three hundred ninety-four (394) total sites with 2 or more MFN services were identified. An oversubscription ratio can be applied based on the sites' total subscribed services count. For sites with 2 or 3 services (337 sites), a subscription ratio of 2:1 should be applied while for sites with more than 3 services (57 sites), a 4:1 ratio should be applied for a potential reduction of annual costs.

3.3.2.2 SDWAN

Software defined wide area network (SDWAN) technologies have become widely deployed solutions to support the wide area communications requirements for many organizations. At a fundamental level, SDWAN solutions are based on the same core technology supporting the current MFN-2 "Remote Access Virtual Private Network" (VPN) service offerings. SDWAN solutions leverage IPSEC and other tunnel protocols to establish a private routed network solution that leverages commodity internet and/or leased MPLS services at the transport layer between nodes. SDWAN solutions often offer macro segmentation within the provided SDWAN communications fabric solution permitting the users of the technology to support multiple virtual network environments over a common SDWAN foundational communications fabric. SDWAN also provides the ability for nodes within the fabric to leverage multiple transport connections and services to provide enhanced diversity for the tunneled traffic fabric. SDWAN nodes can leverage multiple underlay transport services, concurrently balancing traffic flows across the available transport connectivity based on application-aware methodologies. SDWAN nodes continuously measure the performance of the underlay network environments and can apply business logic to route specific application traffic flows only over transport services that can meet the specific application SLA requirements to ensure favorable user experiences. SDWAN solutions also offer advanced functions such as selective packet duplication and deduplication over transport networks that are experiencing packet loss to help ensure the user traffic flows for critical applications remain intact dynamically based on underlay transport network conditions.

The complexities of SDWAN are underpinned by a controller-based solution where business and policy logic (intent) are expressed by the operators. The end nodes then automatically program their operational states to affect the given policies defined. This abstracts the complexities of direct configuration allowing network staff to be more efficient. These solutions are typically considered CPE (customer premise equipment) functions and are designed to replace the standard CPE routing devices that integrate the LAN with the WAN services. Some SDWAN vendors have developed solutions targeted at the Managed Service Provider (MSP) market by incorporating multi-tenant features into their solution offering. This allows a single SDWAN fabric to be designed and implemented by a central provider, while allowing the administrative functions to be exposed to tenant organizations in a manner where each tenant only sees and manages the nodes that have been centrally associated with their tenant account. In this way, a common SDWAN fabric and support infrastructure can be established and then shared by multiple tenant organizations. This is known as a managed services approach for SDWAN deployment. A central organization, such as MFN, would deploy the nodes and fabric solutions while permitting the subscribers to self-manage their services by defining their own tenant-specific policies and application rule sets.

SDWAN technologies are considered transport network agnostic as any transport network that can provide direct IP communication between nodes in the fabric can be leveraged by the solution. This permits the technology to use ISP services as well as private services as a transport. This enables incredible flexibility for the SDWAN user as any available transport at a facility is able to be leveraged, including:

- DIA (direct internet access) circuits
- Commodity Broadband ISP services
    - Hybrid Fiber Coaxial (HFC/Cable Modem)
    - Packet Optic Network solutions (GpoN, 10GpoN, XGPon, FioS)

    - Cellular
    - Satellite (Low Earth Orbit and Geospatial)
- L3VPN (Layer 3 Virtual Private Network)/VRF MPLS services

These services can also be leveraged together, in either fault tolerant or application aware load balanced methodologies.

DMS should consider adding SDWAN services to its portfolio of required services provided by the MFN-3 vendor either in place of, or in addition to, the existing Remote Access Virtual Private Network offering. SDWAN could also be provided as an optional managed CPE solution similar in nature to the current MFN-2 offering. SDWAN vendors have begun to add client layer virtual solutions that provide an SDWAN virtual appliance inside a compute node, allowing that client to virtually connect as part of the SDWAN fabric. This provides SASE (Secure Access Service Edge) functionality that can replace traditional IPSec VPN Client solutions, allowing centralized policy definition and monitoring with distributed processing. There is still a need for traditional IPSec site to site VPN services to support business to business intranet services, as SDWAN is typically proprietary and requires a like vendor node at each location. This is in contrast to standards based on IPSec solutions that are designed to allow multi-vendor integration.

Since SDWAN is designed as a CPE replacement, it will not negate the need for an MFN backbone infrastructure. SDWAN should be designed into the MFN permitting seamless integration between SDWAN services and the MFN VRF services. This allows the MFN to seamlessly service subscribers over ether traditional or SDWAN methods.

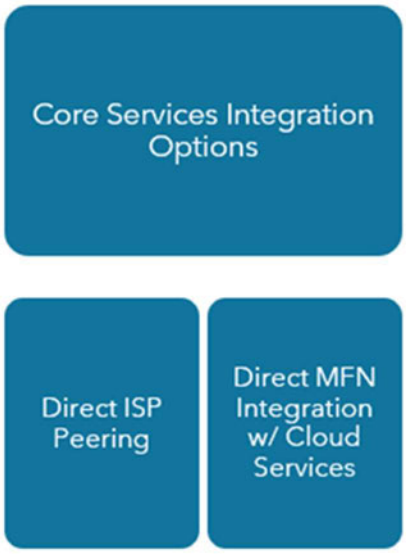
An issue with SDWAN as a component option is that SLAs cannot be guaranteed unless the underlay transport network can provide SLA guarantees to the overlay. While SDWAN nodes can leverage multiple Internet services for transport and transfer packet flows between them as needed to ensure application traffic meets the required SLAs, a simultaneous impairment to both Internet transports cannot be overcome by the technology. For this reason, multiple connections are typically required to enable SLA adherence, with one of the services recommended to be an MPLS based service if the facility is required to support real time voice and video applications.

The requirement for multiple circuits to support SLAs typically results in a cost close to that of a traditional MPLS based solution. Some business facilities, however, may be able to function at an acceptable level using a best effort solution. There are some business cases where a site does not require stringent SLA adherence and could be supported using SDWAN with a single commodity ISP service. In these cases, SDWAN provides a cost-effective method for MFN service deployment. It would be important for both the MFN and the subscriber to understand and agree to the best effort nature of these deployed MFN services.

DMS should consider adding SDWAN as an offering to MFN-3 in two (2) distinct ways. First, a SDWAN solution should be offered as a CPE option available for lease by subscribers, similar to the current leased/managed CPE offering under MFN-2. This would allow subscribers to leverage the macro segmentation and advanced application layer capabilities of such a solution. This will require that supporting services such as automatic interface IP configuration via Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) be supported on the MFN services in order to permit the zero-touch provisioning (ZTP) functions of the SDWAN solutions to work properly.

Secondly, DMS should consider leveraging SDWAN technologies as a method for delivering MFN services to sites willing to accept best effort SLAs for reduced costs. An SDWAN fabric solution could be implemented and integrated to the MFN core permitting any VRF to be extended to remote sites using the SDWAN fabric. This would permit MFN to leverage Starlink™ or Cellular services for sites where traditional telecommunications services are unavailable.

3.3.3 Core Services Integration Options



MFN requirements necessitate its backbone communications infrastructure have points of presence throughout the geography of Florida. A review of the current MFN-2 serviced facilities reveals that the public service nature of the MFN subscriber community results in a service delivery landscape that extends throughout Florida. While there are concentrations of facilities near population centers, the overall physical topology of sites is distributed over the Florida landscape. The distributed nature of governmental networks can be leveraged to provide additional benefits to the network that are not directly applicable to more traditionally centralized communication architectures. Establishing a core facility in a strategic public commercial peering facility would permit the MFN to leverage the available direct peering options inherently provided through physical collocation, allowing for direct connectivity between partner network infrastructures.

Direct peering has the potential to both reduce the overall costs for MFN service delivery by avoiding costly leased services, while also enhancing overall performance for applications and services that utilize the peering connections. The sections below detail two (2) options by which MFN-3 could benefit from core site selection decisions that incorporate access to public peering services as a criterion. Currently, the Equinix Miami collocation facility[26] is one of the most popular facilities in the Florida telecommunications market and has a high concentration of collocated networks and associated peering opportunities.

3.3.3.1 Direct ISP Peering with MFN Subscriber SaaS/Content Service Networks

Internet Peer Exchanges, often abbreviated as IPX or IX, represent a decentralized network infrastructure where multiple Internet service providers (ISPs), content providers, and networks connect and exchange traffic directly with one another. Unlike traditional hierarchical network structures, IPX's operate on a peer-to-peer basis, facilitating direct data exchange between participating entities. At the core of an IPX is the concept of peering, wherein ISPs and other network operators establish direct interconnections with one another to exchange data traffic. These connections are typically facilitated through Internet Exchange Points (IXPs) or private peering arrangements. Instead of routing traffic through multiple intermediary networks, an IPX enables a more

[26] https://www.equinix.com/data-centers/americas-colocation/united-states-colocation/miami-data-centers

efficient and direct exchange of data, resulting in reduced latency, improved network performance, and potentially lower operational costs for both participating network operators.

By leveraging Internet Peer Exchanges, organizations can improve the performance and reliability of their online services and applications. Direct data exchange between networks minimizes latency and packet loss, ensuring smoother user experiences and higher levels of user satisfaction. Traditional methods of routing traffic through transit providers can incur significant costs for organizations, especially those with high data transfer requirements. Leveraging an IPX offers a cost-effective alternative by eliminating the need for intermediary providers such as transit network services, reducing transit data expenses. As organizations cater to growing user demands, scalability becomes paramount. Internet Peer Exchanges provide a scalable infrastructure that can accommodate increasing traffic volumes without compromising performance or incurring substantial infrastructure investments. IPX's can also enhance network resilience by enabling redundant connectivity options. By establishing direct interconnections with multiple peers, businesses can mitigate the risk of network outages and disruptions, ensuring continuous availability of their online services.

While Internet Peer Exchanges offer compelling benefits to customers, several considerations should guide their implementation:

Network Security: Maintaining robust security measures is paramount when participating in Internet Peer Exchanges. The benefit of the exchange in terms of security is that the physical proximity and direct peering permits both parties participating to have a higher level of confidence in the connection. Additionally, typically peering fabrics are non-transit in that the fabric itself is not directly accessible from the Internet and is only available to the directly connected organizations.

Peering Strategy: Developing a comprehensive peering strategy is essential for maximizing the benefits of an IPX. MFN will need to develop a standardized approach to determining which available networks warrant direct peering. Typically, these decisions are best made with data from the current flow patterns on the production network to identify what remote networks the MFN subscribers communicate most with and then determining if those networks are available on the fabric. MFN should also evaluate business criticality of the service provided as another factor in the policy as bandwidth alone may not justify the peering but the performance reliability for critical applications may justify peering.

Performance Monitoring and Optimization: Continuous monitoring of network performance metrics is essential for identifying and addressing potential bottlenecks or inefficiencies within the IPX infrastructure. The MFN should leverage monitoring tools and analytics to optimize traffic routing and enhance overall network performance. Where possible this should also include simulated application transaction monitoring to services available over the fabric to help proactively identify service degradation. This is important as multiple physical network components administratively controlled by the facility provider are typically involved in the service that neither the MFN nor its peering partners can monitor directly.

Internet Peer Exchanges represent a paradigm shift in network connectivity, offering organizations significant opportunities to enhance performance, optimize costs, and expand their reach. By

embracing an IPX as a part of the network strategy and adopting a strategic approach to peering, the State will further position itself for improved customer experiences.

The MFN-3 has a unique opportunity to establish direct integration with the larger IXPs available within Florida that its subscribers would likely not be able to justify within their own networks. The demonstrated successes of the MFN programs underscore the benefits of the aggregation of the state's service requirements. Similar organizations to MFN such as networkMaryland™[27] have leveraged IXPs in their network strategies and regard them as highly successful additions.

There are several IXPs operating in Florida[28], one of the largest is the Equinix MI1 datacenter in Miami located at 50 NE 9th Street. This datacenter facility houses two (2) separate public exchange services, the Equinix IXP (EQIX-MI)[29], and the Community IX (Tel)[30]. A review of these exchange services shows a robust list of existing exchange members including SaaS providers like Amazon Web Services, Google, Microsoft, as well as content providers such as Akamai, Fastly, and Cloudflare. The collocation of an MFN-3 backbone in a facility with these resources would provide significant benefit to the overall MFN-3 solution by enabling more direct connections between MFN customers and these services.

DMS would benefit from requesting information on prospective vendors' peering strategy as part of the solicitation and evaluation for the MFN-3 contract.

3.3.3.2 Direct MFN Integration with Cloud Services

The State of Florida has developed a cloud first strategy towards data processing services defined in Section 282.206 F. S.[31]. The MFN supports all governmental communication services, and as such MFN-3 is expected to expand its ability to integrate the infrastructure with commercial cloud providers to lessen technical and financial impediments for the subscriber community as each agency works to comply with the statute. While the current MFN-2 solution provides integration with commercial cloud services, it does so through partnership with AT&T netbond[32] and other third-party partner services. While this partner/outsourcing solution provides the required extension of MFN services to cloud providers, there is a more cost-effective alternative of which MFN-3 may take advantage.

Placing the next generation MFN points of presence within commercial datacenters that have cloud services available would permit the MFN to remove the need for third party involvement, and instead directly connect the MFN backbone with cloud service providers and/or cloud fabric services. This is possible because many of the public cloud services already establish collocated points of presence in popular commercial datacenters to be able to support direct integration with their customers.

[27] https://doit.maryland.gov/support/Pages/networkMaryland.aspx
[28] https://www.internetexchangemap.com/#/building/8186
[29] https://www.peeringdb.com/ix/17
[30] https://www.peeringdb.com/ix/954
[31] http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.206.html
[32] https://www.business.att.com/products/netbond.html

Amazon Web Services (AWS), Microsoft, as well as Google[33], list the Equinix MI1 facility in Miami as an available facility for direct connect services[34]. The next closest available peering point listed is QTS ALT1 in Atlanta GA. The availability of a facility within Florida that can support direct integration with such a broad range of potential cloud service providers is very beneficial to the MFN. If MFN-3 were to establish a backbone point of presence within the Miami Equinix facility, direct connectivity between MFN-3 and these cloud service providers could be established. This would permit direct integration between MFN and the upstream service providers, effectively eliminating the need for any third-party transit services or broker organizations and their associated costs.

Due to the expected prevalence and reliance on cloud services in the future for MFN subscribers, it will also be important that MFN-3 establish an alternative peering facility for cloud service integration to support redundancy. The next geographically closest facility for direct cloud service integration by the larger cloud providers is Atlanta. There are other options offered by datacenter providers for cloud service extensions such as the "Equinix Fabric™"[35] and the Coresite "Open Cloud Exchange"[36]. MFN-3 could leverage these services to extend MFN for cloud integration as an alternative to the Miami facility, but care will be needed to ensure the services obtained are not dependent or delivered out of the Equinix Miami facility to ensure resiliency. MFN-3 will need to consider cloud service connectivity as a variable in the selection criteria for core PoP facilities. There should be at least two (2) MFN-3 core PoP facilities that offer direct cloud integration or fabric services to facilitate cloud provider integration/extension.

[33] https://cloud.google.com/network-connectivity/docs/interconnect/concepts/choosing-colocation-facilities#north-america
[34] https://aws.amazon.com/directconnect/locations/
[35] https://www.equinix.com/products/digital-infrastructure-services/equinix-fabric
[36] https://www.coresite.com/cloud-networking/open-cloud-exchange

3.4 Option Groupings for Cost Benefit Analysis Examples

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.

This section is designed to provide a cost example for potential MFN-3 solutions that leverage the options detailed above. This section provides details on which of the component level options are considered applicable to each contract approach.

Example 1 outlines an MFN-3 based on the current outsourced model with the MFN provided by a single vendor. Example 1 is detailed in Section 3.4.1.

Example 2 augments the current outsourced MFN scenario through a multi-award-based MFN contract approach, where the last mile telecommunications services are separated out into a distinct functional area. Example 2 is detailed in Section 3.4.2.

These examples are meant to provide a model of potential costs for operation under each provided scenario. The models are based on detailed assumptions which may vary when each model is implemented. Table 4 provides a summary of the resulting two cost models over a ten-year period (see below sections for details on how each model was created). The lowest cost option is the Vendor-Owned/Vendor-Managed multi-award option at ~$61.1M/year. This conservative estimate represents an annual ~$7.6M cost avoidance as compared to the Vendor-Owned/Vendor-Managed single-award model (~$68.7M).

Table 4 – 10 Year MFN-3 Cost Model Comparison Summary

MFN-3 Contract Cost Model Comparison										
Year	1	2	3	4	5	6	7	8	9	10
SA VO/VM MFN Costs	68,658,300	137,316,600	205,974,900	274,633,200	343,291,500	411,949,800	480,608,100	549,266,400	617,924,700	686,583,000
MA VO/VM MFN Costs	61,064,913	122,129,826	183,194,739	244,259,652	305,324,565	366,389,478	427,454,391	488,519,304	549,584,217	610,649,130

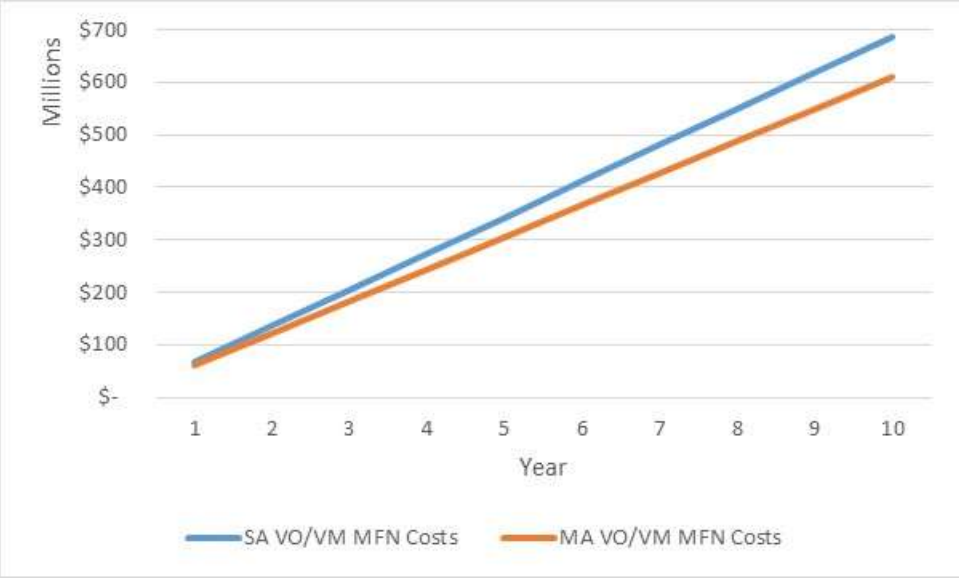


Figure 15 - 10 Year MFN-3 Cost Model Comparison

3.4.1 Single-Award Vendor-Owned Core and Backbone Infrastructure (Example 1)

The first contract model evaluated is the current outsourced contract model leveraged by the existing MFN-2 contract. Under this model the MFN is provided as a service to Florida in that the infrastructure and all associated services required to deliver the MFN services to the subscribers are owned by the contractor.

3.4.1.1 Component-Level Options

This section of the document describes how the component level options defined in section 3.3 may apply to the vendor-owned/vendor-managed single-award model of contract for MFN-3.

3.4.1.1.1 MFN-3 Backbone Options

This section details the applicable MFN backbone infrastructure component options for Florida under a vendor-owned/vendor-managed single-award MFN contract. This model is the model leveraged under the current MFN-2 contract.

3.4.1.1.1.1 Shared vs. Dedicated Infrastructure

The previous findings detailed under the MFN-2 business case continue to be relevant for MFN-3. While the cost avoidance potential associated with a shared infrastructure solution should be evaluated by DMS during the MFN-3 procurement, the restrictions such a model will place on the MFN-3 solution are expected to remain a major deterrence to such an implementation. DMS should permit respondents to MFN-3 to propose both options if desired so that DMS can compare the costs associated with the shared versus dedicated infrastructure proposals to help determine if the choice is financially attractive.

A restriction associated with a shared infrastructure solution will be the ability for DMS to implement IDS/IPS and other monitoring/security solutions at the Core/Access integration layers of the network as a bundled part of the service offerings. It is feasible for DMS to instead re-architect these functions to be performed by the CPE equipment at the edge in a more distributed model. Modern CPE equipment can support native and third-party applications based on micro-services architecture that permit functions to run as embedded services on the hardware. This currently includes services such as IDS/IPS as well as application monitoring solutions as a distributed service running on the CPE hardware. Coupling these capabilities with a centralized control/reporting service running within the MFN Common Services VRF could provide a suitable alternative to the current centralized architecture for the service under MFN-2.

Such a distributed solution can provide congruent functionality for DMS. However, it is expected that the costs would be higher than the current centralized model deployed under MFN-2 as DMS would incur additional licensing fees and integration requirements. Any cost avoidance associated with the use of shared infrastructure would need to be compared to these cost increases to determine the true

value of such a decision. The ability for this analysis to evaluate the cost impact of this option in a generalized fashion is limited, as costs proposed would be highly variable based on existing vendor network architectures.

3.4.1.1.1.2 MFN-3 Backbone PoP Facility Options

The ability to dictate the backbone PoP facility locations in the fully outsourced model may be significantly limited. An outsourced solution typically limits the influence that the contracting entity can have over how the contracted services will be delivered. While it may be possible for the MFN-3 contract to be written in a manner that requires the backbone PoPs to be established in DMS determined facilities, this often results in a significant increase in cost. Network operators such as the current MFN-2 incumbent would typically select existing facilities where they already have operational points of presence as backbone locations for an MFN solution proposal. By leveraging their existing investments in staffing, standard processes, and facility leases, the providers can offer a lower cost to MFN. A requirement to locate equipment in new facilities, where such relationships are not already established, is very likely to result in negating the potential for cost avoidance to MFN by avoiding last mile service fees for the local facility subscribers. Access to potential state resources such as fiber infrastructure as well as general facility access to a commercial company is likely to also be restricted, or in some cases prohibited completely. It is for these reasons that site selection for backbone PoP establishment is likely to only be partially applicable to a model that reflects the MFN current-state. It would be beneficial for DMS to impose requirements in the MFN-3 contract to have an MFN backbone PoP established in the Equinix Miami datacenter so that the benefits detailed in the Core Services Integration Options section below are available to MFN. A secondary PoP in a suitable alternative open access carrier facility is also warranted to provide redundancy.

3.4.1.1.2 MFN-3 Last Mile Options

3.4.1.1.2.1 Mini-Node Deployments for Multi-tenant facilities

The selected contractor for MFN-3 may choose to deploy the mini-nodes in multi-tenant facilities. This should lower costs to DMS where servicing is provided to a site or facility with multiple subscribers. While the cost avoidance may not be apparent if circuit pricing is bundled, inquiring about each vendor's approach to mini-node deployment should encourage the vendor to consider mini-nodes in their architectural approach, resulting in cost efficiency to the State.

3.4.1.1.2.2 SDWAN

SDWAN devices could be added as a CPE option for subscribers to lease from the MFN alongside the existing CPE options. SDWAN infrastructures typically require a control system solution to be implemented that provides the control plane orchestration for the fabric. The control plane is often available as a SaaS (software as a service) offering from the vendors, or in a private offering where the customer stands up the required servers/services either in a private or public cloud environment. In both methods, there are considerable costs for the solution associated with the implementation and maintenance of these control plane elements. The MFN should consider partnering with an SDWAN vendor solution that is designed for operation by a Managed Service Provider. In this manner, MFN could centralize the control plane functions while permitting multiple subscribers to leverage the investment. Such a solution would negate each subscriber from having to purchase and pay the associated fees for the control plane elements, resulting in significant cost efficiency to the State.

DMS could require such an SDWAN service offering with centralized multi-tenant support to be implemented as part of the MFN-3 contract under an outsourced model. If required, DMS should consider stipulating that current client-based VPN solutions be replaced by a SASE offering. This would provide higher value to the MFN subscribers by being able to support advanced security functionality and end point control functions in addition to the basic client VPN access services.

3.4.1.1.3 Core Services Integration Options

It is possible, and beneficial, to mandate that the MFN contractor establish at least 1 backbone PoP in the Equinix Miami facility to ensure the MFN has access to the associated IX and cloud services. However, in an as-a-service model the contractor is in control of how the network is designed and implemented.

While DMS can mandate as a part of the contract that the MFN-3 solution have a presence on the Equinix IX and Cloud Exchange Fabric, the cost efficiency for these services may not be directly passed on to the State as the cost efficiency for these services are highly dependent on traffic and application make up, as well as subscriber usage which can vary over time. Due to this variability, the potential cost avoidance is likely to be normalized within the static cost structure provided under the MFN outsource contract and as such is not likely to be directly exposed to DMS. Mandating these connections from the MFN, however, will enhance the overall performance of the services leveraged by the MFN community over these connections. As such, it would still be considered beneficial for direct peering to be required under the MFN-3 contract even if the cost efficiency is not directly passed through to the State.

3.4.1.2 Contract Transitions

The transition of MFN-1 to MFN-2 imposed a high cost from both a financial and business impact perspective to the State of Florida. To facilitate the contract transition, a completely new MFN infrastructure was established while operation of the MFN-1 service continued concurrently during implementation of MFN-2. The two infrastructures were then integrated to permit communication between the two environments, which then allowed for services to be transitioned in a phased manner. The transition required that new last mile access services be installed, then subscribers physically and logically transitioned their CPE connectivity from the MFN-1 to the MFN-2 services on a site-by-site basis.

As the State experienced previously during the MFN-1 to MFN-2 migration, transition costs between MFN contracts using an outsourced model are high while requiring two years or more to complete the transition. During the transition period, the State is supporting the financial burden of two concurrent MFN contracts. The transition efforts produce little overall value to the business operations of the state beyond those competitively associated with the vendor's offer.

In addition to the direct contract costs, transitioning between contracts with a change in service provider requires staff labor to support the service transitioning at each facility for each circuit/service. A replacement circuit was provisioned and delivered for each production service under MFN-1 to facilitate the MFN-2 transition. While the costs for this provisioning may not have been directly charged to DMS/Florida, they were incurred by the provider and their last mile partners under the MFN-2 contract and as such they were incorporated as part of the overall MFN-2 proposed fee structure which

ultimately was paid for by the MFN subscribers. Additional labor effort was required to perform the actual transition of service at each site for each MFN circuit as new physical circuits were required to be delivered to support the transition.

Impacts to State's business were also incurred to support the transition between MFN-1 and MFN-2. Agency business operations were required to be suspended during site level transitions. Scheduling outages outside of normal business hours are an effective mitigation strategy, however, there are still impacts to offline processing and similar services. Agency personnel were required to coordinate and plan transition activities with DMS/MFN-2 which required staff involvement and time.

3.4.1.3 Prime-Managed Last-Mile Awards

Under the vendor-owned/vendor-managed single-award contract type the MFN contractor would be responsible for the end-to-end MFN service delivery in that the contractor would directly procure all required components. This would include the procurement and management of leased telecommunication services. Under this contract model, the MFN contractor would establish sub-contract agreements with various LEC (local exchange carrier) services organizations where the vendor would negotiate recurring and non-recurring service costs directly. The prime contractor is responsible for the procurement processes and operational management of the sub-contractor services.

3.4.1.4 Prime-Managed Additional Services

Under the vendor-owned/vendor-managed single-award contract type the MFN contractor would be responsible for the end-to-end MFN service delivery in that the contractor would directly procure all required components. This would include the procurement, integration, and management of any MFN required services. Under this contract model, the MFN contractor would establish sub-contract agreements with services organizations where the vendor would negotiate recurring and non-recurring service costs directly. The prime contractor is responsible for the procurement processes and operational management of the sub-contractor services. This is how the current MFN-2 model operates. While some services are provided directly by the MFN-2 contractor others such as cloud integration services are provided through sub-contract agreements with various vendors. The end-to-end services are managed by the prime contractor; however, the vendor determines which components they own/provide directly and which they procure from sub-contractors. The complexities associated with the management of the multiple component services and their integration with the MFN backbone are still present within the MFN solution as the MFN prime contractor must still manage these service agreements to ensure the end-to-end MFN subscriber service viability.

3.4.1.5 Return on Investment Period Horizon

The ROI (return on investment) period for a vendor owned solution is equal to the term length of the contract. MFN contractors must ensure a positive ROI is achievable for any investment they make in the provided MFN solution within the contract period. Often this is specifically limited to the guaranteed period of the contract as extending ROI periods into optional years represents risk to the contractor organization. As for-profit organizations, commercial entities need to further constrain the ROI period for evaluating MFN augmentations or design options to a significantly lower time frame than the contract period, to ensure sufficient profit is achievable to offset the overall risks to their investment.

3.4.1.6 Enhanced Strategic Alignment with MFN Contractor

Due to the ROI period constraints described in 4.3.1.5, strategic alignment between DMS and the MFN contractor can be difficult to achieve. The MFN contractor must ensure a positive return and profit on the services provided under the MFN. This can lead to situations where the longer-term needs of the State are not consistent with the relatively shorter term (contract period) horizons for the MFN contractor. DMS will want to consider providing provisions in the MFN-3 contract to alleviate some of the factors that can lead to this misalignment. For example, permitting a cost-plus model for last mile services would allow the risks for last mile services to be shared between Florida and its MFN contractor.

Under the current MFN-2 contract the MFN vendor provides flat rate pricing to DMS for all MFN services. It is relatively low risk for the contractor to support this model for the initial MFN implementation as the MFN facilities are known and service quotes for them can be obtained from partners allowing the contractor to set pricing accordingly. Future service moves/adds/changes, particularly around new facilities, represent a greater risk to this model for the contractor.

Costs for leased telecommunication services can vary wildly from region to region within the state. Since the MFN contractor is required to provide flat rate pricing for all MFN services, this represents a large potential risk to the MFN contractor that must be mitigated. The MFN contractor either mitigates this risk through higher service fees or in some cases may choose to not deliver services and instead pay SLA violation restitution because the costs associated with not delivering the requested services are lower than the costs to deliver them.

Under a cost-plus model, the vendor would negotiate a specific service fee percentage that would be added to the costs incurred to deliver the service, which would be the final costs associated with the service delivery to DMS. DMS could continue to offer MFN subscribers flat rate pricing, as separate billing service fees could be levied by DMS. In this manner, DMS and the MFN contractor become more aligned as risks are shared. This would also allow DMS to influence the MFN contractor more readily with respect to last mile servicing vendors for specific sites. With the cost model between DMS and the MFN contractor being dynamic, while fixed at a specific percentage over costs, DMS could request that LEC partners that perform poorly within specific regions or sites are not leveraged and instead agree to pay higher costs for better services.

3.4.1.7 Cost-Benefit Analysis for Vendor-Owned/Vendor-Managed Single-Award Model

This section provides a cost model using the current MFN-2 outsourced based contract as a basis of estimate for the Vendor-Owned/Vendor-Managed single-award contract model. The primary purpose is to provide a cost basis to compare this single-award model to the multi-vendor model to permit a better understanding of the potential cost avoidance of the alternative contract option. A baseline using the existing MFN-2 current costs (as of the time of this analysis) was leveraged. This cost model was also based on the current MFN costs so the comparison between the examples provides an accurate representation of what Florida could experience in terms of percentage differentials between

models through the application of the presented options. Similar to the other cost model below, this cost model includes the following components from the current MFN-2 contract[37]:

1. Remote site costs
    a. Sum of all access costs from each active MFN-2 service.
    b. Sum of all port costs from each active MFN-2 service.
    c. Sum of all CPE costs from each active applicable MFN-2 service.
    d. Sum of all Internet costs from each active applicable MFN-2 service.
2. Ancillary service costs
    a. Sum of all C2L service costs.
    b. Sum of all L2L Main costs.
    c. Sum of all L2L additional costs.
3. FIRN costs
    a. Sum of all active FIRN Access costs from current MFN-2 contract.
    b. Sum of all active FIRN Port costs from current MFN-2 contract.
    c. Sum of all active FIRN CPE costs from current MFN-2 contract.
    d. Sum of all active FIRN Internet costs from current MFN-2 contract.

[37] Costs derived from DMS-provided dataset

Table 5 - Example 1 Vendor-Owned/Vendor-Managed Single-Award Cost Model Detail[38]

Vendor Owned/Vendor Managed Single-Award MFN-3 Cost Model										
Year	1	2	3	4	5	6	7	8	9	10
MFN Services	54,361,644	108,723,288	163,084,932	217,446,576	271,808,220	326,169,864	380,531,508	434,893,152	489,254,796	543,616,440
MFN Internet Costs	684,216	1,368,432	2,052,648	2,736,864	3,421,080	4,105,296	4,789,512	5,473,728	6,157,944	6,842,160
MFN Managed CPE	3,632,820	7,265,640	10,898,460	14,531,280	18,164,100	21,796,920	25,429,740	29,062,560	32,695,380	36,328,200
MFN Ancilary Costs	695,904	1,391,808	2,087,712	2,783,616	3,479,520	4,175,424	4,871,328	5,567,232	6,263,136	6,959,040
FIRN Access Costs	4,644,480	9,288,960	13,933,440	18,577,920	23,222,400	27,866,880	32,511,360	37,155,840	41,800,320	46,444,800
FIRN Port Costs	1,931,604	3,863,208	5,794,812	7,726,416	9,658,020	11,589,624	13,521,228	15,452,832	17,384,436	19,316,040
FIRN CPE Costs	1,029,264	2,058,528	3,087,792	4,117,056	5,146,320	6,175,584	7,204,848	8,234,112	9,263,376	10,292,640
FIRN Internet Costs	1,678,368	3,356,736	5,035,104	6,713,472	8,391,840	10,070,208	11,748,576	13,426,944	15,105,312	16,783,680
SA VO/VM MFN Costs	**68,658,300**	**137,316,600**	**205,974,900**	**274,633,200**	**343,291,500**	**411,949,800**	**480,608,100**	**549,266,400**	**617,924,700**	**686,583,000**

As detailed in Table 5, the cost model for the MFN under a single-award vendor-owned/vendor-managed contract is a linear cost model of $68.6M annual cost to Florida with a 10-year total cost of $687M. Excluded from this model are contract transition costs that would occur during the initial 2-to-3-year period. Since transition costs would be expected to be the same for all of the models if a new primary vendor is selected, exclusion of these costs does not affect the validity of the comparison of the models as they have been excluded for all models. Also, as subscribers tend to require higher bandwidth services over time, costs incurred due to elective increases in total bandwidth on a per-circuit basis are not included in this model.

DMS has set out to evaluate the MFN-3 solutions and contracting options with the intent to procure at a lower overall cost. To this end, DMS includes for consideration the other option of the use of multiple contract award for last mile services, described in the following section, 3.4.2.

[38] Costs derived from DMS provided dataset

3.4.2 Single-Award Vendor-Owned Core and Backbone, Multi-Award Last-Mile Services (Example 2)

The second contract model evaluated is similar to the current outsourced contract model leveraged by the existing MFN-2 contract for the core MFN backbone and services. This model separates the last mile telecommunication services as a distinct functional area with multi-award within the overall contract. Under this model the MFN backbone and core services are provided as a service to Florida, with the infrastructure and all associated services required to deliver the MFN services to the subscribers owned by the contractor. The last mile services used to extend the core to the MFN subscriber facilities would be procured by the prime contractor from a set of vendors approved on the MFN-3 telecommunications contract category for last-mile services. Vendors on this category would go through a periodic competitive evaluation conducted by DMS, similar to other state contracts that enable multiple vendors to work with the State of Florida.

This functional area would be a multi-award procurement model permitting the primary core services contractor to request quotes on behalf of DMS from all contract vendors for each specific required last mile service. The primary contractor would then select the appropriate vendor quote based on best value determination, with DMS able to override decisions if necessary and appropriate. The awarded vendor would then install their proposed service between the designated MFN core meet me facility and the MFN subscriber remote facility. Latitude could be provided to each responding telecommunications vendor permitting them to designate which of the designated core "meet me" facilities they will leverage for the proposed services. Once installed the primary MFN contractor would then integrate the service into the backbone and provide the end-to-end subscriber service. Operational support for troubleshooting would be provided by the primary MFN contractor who would serve as DMS's designated agent for any required support services engagement by the various vendors under the last mile contract.

3.4.2.1 Component-Level Options

This section describes how the component level options defined in section 3.3 could apply to the vendor-owned/vendor-managed multi-award model of contract for MFN-3.

3.4.2.1.1 MFN-3 Backbone Options

This section details the applicable MFN backbone infrastructure component options for Florida under a vendor-owned/vendor-managed multi-award MFN contract. This model is effectively the model leveraged under the MFN-1 and MFN-2 contracts with the separation of last mile telecommunication services as a distinct functional area within the MFN contract.

3.4.2.1.1.1 Shared vs. Dedicated Infrastructure

The shared vs. dedicated infrastructure option (see 3.3.1.1) is directly applicable to an outsourced contract model for MFN-3 with respect to the backbone network infrastructure. The description given in Section 3.4.1.1.1.1 under MFN-3 Backbone Options also applies to this section under this option grouping.

3.4.2.1.1.2 MFN-3 Backbone PoP Facility Options

The ability to dictate the backbone PoP facility locations in an outsourced model may be significantly limited. The description given in Section 3.4.1.1.1.2 under MFN-3 Backbone Options also applies to this section under this option grouping.

Under a multi-award contract, it will become important to the State that the backbone is designed in a manner that ensures the highest level of competition within the last mile services contract functional area. Under such a contract DMS must ensure that the backbone provider is required to establish a "meet me" facility within each of the defined FCC LATA regions that permits open access to LEC service providers so that no ILEC/CLEC is excluded from being able to integrate with the MFN. Primary MFN contract respondents should be required to detail the physical facilities in their proposals where they will support LEC/Last mile service integration. Evaluation of the solutions should include a review of the proposed integration facilities with a weighted preference on facilities located in higher population density regions as these are likely to be associated with lower costs for the LEC service providers to establish connectivity to.

3.4.2.1.2 MFN-3 Last Mile Options

3.4.2.1.2.1 Mini-Node Deployments for Multi-tenant facilities

Mini-node deployments are applicable to this model. The description given in Section 3.4.1.1.2.1 under MFN-3 Last Mile Options also applies to this section under this option grouping.

3.4.2.1.2.2 SDWAN

SDWAN is applicable to this model. The description given in Section 3.4.1.1.2.2 under MFN-3 Last Mile Options also applies to this section under this option grouping.

3.4.2.1.3 Core Services Integration Options

Direct peering is considered to have limited applicability under an outsourced model for the MFN. The description given in Section 3.4.1.1.3, Core Services Integration Options also applies to this section under this option grouping.

3.4.2.2 Contract Transitions

Contract transition will still require replacement of the MFN core network under a vendor-owned/vendor managed multi-award contract. Since the MFN is owned by the contractor, a new MFN contract will require a transition period where MFN subscribers are migrated from the incumbent vendor infrastructure to the new. Under the multi-award model DMS would be directly involved in onboarding last-mile vendors to a State contract, adding some level of additional complexity in coordination to the overall transition processes. Once vendors have been added to the last-mile contract, the primary MFN-3 contractor would work as an agent of DMS to competitively issue RFQs to procure circuits from last mile service providers.

A multi-award contract where last mile telecommunication services are a separate functional area offers an advantage to Florida as compared to the single-award contract, in that DMS is the customer of record for last mile services. The physical circuits leased under the MFN contract are more likely to

be able to transition between contracts since the customer of record remains consistent. This is not a guarantee, as since the telecommunication services were procured under the older contract, individual providers may require new replacement circuits to be installed that are associated with the new contract.

Retention of existing circuits during contract transition would be a beneficial requirement for future MFN contracts after the expiration of MFN-3, as it would reduce transitional costs/complexities. Since the MFN backbone must transition between contracts in this model, the core integration circuits between the LEC providers and the MFN contractor must be changed. New physical circuits for each LEC will need to be established to the new MFN contractor provided backbone/core, and then each remote site will be required to be logically migrated from the incumbent MFN core to the new core. While this represents lower cost and complexity to the subscribers since the remote site circuits can remain in place, the transitional costs for these logical rehoming efforts will still be significant to DMS. The actual impacts and required support from subscribers will be reduced but will still be present, and coordination for the transitional activities will still require subscriber support as changes to their CPE configurations will be required.

It is also important to consider that any leased CPE equipment will also be required to be transitioned to new hardware provided by the new MFN provider, which will require outages and support from the subscriber community. Given the high take rate associated with the current MFN-2 managed CPE, offering the lower complexities associated with transitioning leased circuits may result in no appreciable benefit due to the added complexities and interdependence between these last mile circuits and managed CPE services.

3.4.2.3 Procurement Vehicle for Last-Mile Awards

Under the vendor-owned/vendor-managed multi-award contract model, procurement of last mile services would be performed by the primary MFN contractor as an agent of DMS. Under this model, the primary MFN contractor would provide DMS with designated LEC integration facilities and LOA's (letter of authorization) to DMS to facilitate the installation of circuits within them. In most cases, when new requests for services are submitted by MFN subscribers, the primary MFN contractor would issue a request for quote under the MFN telecommunications functional area to obtain proposals from the awarded vendors servicing the region that encompasses the target facility. The prime MFN contractor would review the quotes and evaluate based on criteria provided by DMS, and award based on best overall value. The awarded provider would install the physical circuits and logical services requested to connect the facility to the MFN backbone. In some cases, DMS may elect to perform the procurement of a circuit on their own. The letters of authorization provided by the primary MFN contractor will enable this. It is not anticipated that DMS-led procurement of individual circuits would occur frequently, if at all.

The MFN core contractor will integrate the service into the backbone and provision the subscriber requested service, ensuring to update the CMDB (configuration management database) for the MFN service record and associated operational last mile circuit and vendor. DMS would be the official customer of record for the services procured, as the MFN contract is directly between the vendor(s) (multi-award) and DMS. The MFN core contractor would be the DMS designated management agent

and as such would be able to open support tickets with the vendor as required to address any operational issues.

3.4.2.4 Return on Investment Period Horizon

The description given in Section 3.4.1.5, Return on Investment Period Horizon also applies to this section under this option grouping.

3.4.2.5 Enhanced Strategic Alignment with MFN Contractor

Due to the ROI period constraints detailed in the previous section, additional strategic alignment between DMS and the MFN contractor can be difficult to achieve. The MFN contractor must ensure a positive return and profit on the services provided under the MFN. This can lead to situations where the longer-term needs of Florida are not consistent with the contract period time horizons for the MFN contract.

3.4.2.6 Cost-Benefit Analysis for Vendor-Owned/Vendor-Managed Multi-Award Model

This section provides a cost model using the current MFN-2 outsourced based contract as a basis of estimate for the Vendor-Owned/Vendor-Managed multi award contract model. Some of the component options can be applied to the outsourced model, however, it is unclear what portion of the overall cost avoidance the State would achieve under an outsourced contract since the contractor would control those components. For this reason, a baseline using the existing MFN-2 current costs as of the time of this business case has been leveraged and detailed in section 3.4.1.7.

The separation of last mile services as a distinct functional area within the MFN is included in this provided cost model. A multi-award telecommunication contract has the potential to result in an approximately 25% reduction to MFN based on results achieved by the State of Maryland using a similar model/approach. It can be assumed that the current MFN contractor (MFN-2) employs a similar approach in sub-contracted service selection, however, the partnership nature of the current MFN contract vs. the directly competitive nature of a direct state contract is likely to result in less competition per facility than what would be achieved by the state through direct procurement. This is due to the nature of the contract where the MFN contractor must identify subcontractor partners as part of the procurement process. This can result in more limited last mile partner options as compared to an open procurement model.

While it is possible for the other component level options to be deployed by an MFN contractor under a vendor-owned model, it is not clear what percentage of the resulting costs avoidance would be directly observable by DMS as the vendor has full control over its pricing model. Further, if a flat rate service pricing structure is negotiated as part of the MFN contract, it is unlikely that deviation would occur as cost avoidance options are exercised. Due to these reasons, estimation of potential costs

avoidance to Florida for these other component options have not been included in the provided model[39]:

1. Remote site costs
    a. Sum of all access costs from each active MFN-2 service reduced by 25% to account for multi-award increased competition.
        i. The 25% reduction is derived from the cost avoidance discussed in section 3.2.1. The 25% was chosen as a conservative estimate based on calculating potential service fees that may be imposed by the core service provider.
    b. Sum of all port costs from each active MFN-2 service.
    c. Sum of all CPE costs from each active applicable MFN-2 service.
    d. Sum of all Internet costs from each active applicable MFN-2 service.
2. Ancillary service costs
    a. Sum of all C2L service costs.
    b. Sum of all L2L Main costs.
    c. Sum of all L2L additional costs.
3. FIRN costs
    a. Sum of all active FIRN Access costs from current MFN-2 contract.
    b. Sum of all active FIRN Port costs from current MFN-2 contract.
    c. Sum of all active FIRN CPE costs from current MFN-2 contract.
    d. Sum of all active FIRN Internet costs from current MFN-2 contract.

[39] Costs derived from DMS-provided dataset"

Table 6 - Example 2 Vendor-Owned/Vendor-Managed Multi-Award Cost Model Detail[40]

Vendor Owned/Vendor Managed Multi-Award MFN-3 Cost Model										
Year	1	2	3	4	5	6	7	8	9	10
MFN Services	47,929,377	95,858,754	143,788,131	191,717,508	239,646,885	287,576,262	335,505,639	383,435,016	431,364,393	479,293,770
MFN Internet Costs	684,216	1,368,432	2,052,648	2,736,864	3,421,080	4,105,296	4,789,512	5,473,728	6,157,944	6,842,160
MFN Managed CPE	3,632,820	7,265,640	10,898,460	14,531,280	18,164,100	21,796,920	25,429,740	29,062,560	32,695,380	36,328,200
MFN Ancilary Costs	695,904	1,391,808	2,087,712	2,783,616	3,479,520	4,175,424	4,871,328	5,567,232	6,263,136	6,959,040
FIRN Access Costs	3,483,360	6,966,720	10,450,080	13,933,440	17,416,800	20,900,160	24,383,520	27,866,880	31,350,240	34,833,600
FIRN Port Costs	1,931,604	3,863,208	5,794,812	7,726,416	9,658,020	11,589,624	13,521,228	15,452,832	17,384,436	19,316,040
FIRN CPE Costs	1,029,264	2,058,528	3,087,792	4,117,056	5,146,320	6,175,584	7,204,848	8,234,112	9,263,376	10,292,640
FIRN Internet Costs	1,678,368	3,356,736	5,035,104	6,713,472	8,391,840	10,070,208	11,748,576	13,426,944	15,105,312	16,783,680
MA VO/VM MFN Costs	**61,064,913**	**122,129,826**	**183,194,739**	**244,259,652**	**305,324,565**	**366,389,478**	**427,454,391**	**488,519,304**	**549,584,217**	**610,649,130**

As detailed in Table 6, the cost model for the MFN under a multi-award vendor-owned/vendor-managed contract is a linear cost model of $61.1M annual cost to Florida with a 10-year total cost of $611M. Excluded from this model are contract transition costs that would occur during the initial 2-to-3-year period. Since transition costs would be expected to be the same for all the models if a new primary vendor is selected, exclusion of these costs does not affect the validity of the comparison of the models as they have been excluded for all models. The State would be expected to incur higher actual costs than depicted in this model since these transition costs have been excluded. Also, as subscribers tend to require higher bandwidth services over time, costs incurred due to elective increases in total bandwidth on a per-circuit basis are not included in this model.

NOTE: The cost avoidance associated with a Florida multi-award data telecommunications contract cannot be fully validated without response submissions from a formal RFI. To obtain a cost basis for this business case, DMS's consulting partner has leveraged the results of prior experience with similar statewide contracts, the State of Maryland project described in section 3.2.1. The applied cost avoidance was calculated by applying the estimated 25% average reduction resulting from releasing a competitive bidding of services to more than one vendor for each circuit, with the core vendor-imposed processing fee. The actual cost avoidance the State would experience may vary significantly from the provided estimates.

[40] Costs derived from DMS-provided dataset.

4 FIRN Sourcing Options

On the current MFN-2 contract, the Florida Information Resources Network 2 (FIRN-2) is coupled with MFN-2 allowing E-rate eligible customers such as K-12 entities to avail themselves of the reduced volume pricing that MFN-2 customers receive on the current contract. FIRN services are logically separated to ensure the applicability of E-rate[41] funding for its subscribers. The services provided include:

- FIRN-2 SIB Service: Provides enterprise infrastructure for Florida's educational institutions.
- FIRN-2 DAN Service: District Area Network internet services.
- FIRN-2 Broadband Service: Offers high-speed connectivity.
- FIRN-2 Ancillary Services: Additional support services.
- FIRN-2 Direct Internet Access: Provides internet connectivity.

The main goal of FIRN-2 is to enhance the connectivity, security, and efficiency of Florida's education institutions, ensuring a reliable communications infrastructure for learning and collaboration.

Currently, there are 206 E-rate eligible services being utilized on the MFN-2 contract. The currently provided services consist of:

- 1 FIRN Broadband connection
- 150 FIRN DAN connections
- 12 FIRN Direct Internet connections
- 43 FIRN Internet Bundled connections

Of those connections, 147 leverage leased CPE and 144 of them are currently being managed under the MFN-2 contract.

Under MFN-3, it is recommended that FIRN be included in the contract as it is today. It is in the State's best interest to aggregate as much service bandwidth as possible to obtain the lowest overall cost for transit/peering services. FIRN and MFN should share the same logical transit peering services.

It is important to note that school systems are more frequent targets for DDOS events, and as such precautions should be taken to ensure a robust DDOS mitigation solution is in place to protect the MFN/FIRN subscriber community. While such a solution is currently in place within the MFN-2 solution, it may be advantageous to the State for such a solution to be outsourced to an upstream vendor that can mitigate at higher capacities. Modern DDOS events can easily exceed 100Gbps in overall traffic volume which may overwhelm the MFN infrastructure. A dynamic solution where the mitigation can occur upstream from the MFN that can mitigate very high-volume loads may be warranted especially when the MFN and FIRN communities share a common infrastructure.

It is important for the FIRN subscriber community that the services maintain E-rate eligibility. This continued eligibility will depend on which of the component options described in the outsourced

[41] https://www.fcc.gov/consumers/guides/universal-service-program-schools-and-libraries-e-rate

sections of this analysis are implemented. Those details will need to be further explored based on the final direction that the MFN-3 contract takes.

5 State Business Processes and 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.

The continuation of the single award contract method for MFN-3 presents no anticipated impact to existing DMS processes or policies that are not effectively managed under the current MFN-2 contract. A transition to a new provider will require some adjustments to specific work instructions and systems to ensure requests are submitted to the proper intake systems on the vendor side but these would be considered minor adjustments to existing processes and work instructions. The existing processes have been developed and refined over time supporting the MFN-1 and MFN-2 contracts and have supported the successful delivery and maintenance of the MFN services to the subscriber community.

Consideration for including the defined mini-node concept is warranted. While the inclusion of this requirement in the MFN-3 contract will not directly change current DMS business practices since the selected core vendor will have the responsibility to support the deployment architecture, the consolidated service delivery method will have impacts to contract costs and may require billing augmentations. Additionally, the deployment method will also require new SLA's to be defined and monitored.

If the State elects to transition to a multi-award contract method with the separation of last mile telecommunication services from a bundled service offering, this will require the adaption of business processes leveraged to support other telecommunications contracts to meet the increased management requirements, as well as adjustments to existing processes. Under a multi-award contract model, DMS would support but not directly manage ongoing procurement requirements for the required telecommunication services for the MFN-3 contract. The backbone provider would still manage the individual procurements on a circuit-by-circuit basis, and process service requests to ensure sufficient infrastructure resources are available to support the service. The backbone provider would leverage DMS to manage the State contracts that govern which vendors can be leveraged by the backbone provider, while the backbone provider manages process of obtaining and evaluating proposals from last-mile telecom contract vendors for each circuit. As an agent of DMS, the backbone provider would then place orders for selected vendor proposals and coordinate to deliver the end-to-end service. The MFN backbone vendor would still provide onsite activation and demarcation extension services as in the current MFN-2 contract. The MFN-3 backbone contractor would act as an agent of DMS for the implementation, activation, and maintenance activities associated with the services.

6 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 MFN-2 contract contains 35 performance metric service level agreements (SLAs) organized into seven (7) categories as detailed in Table 7 (below). These metrics should be maintained in the new contract. The SLA should be adjusted to reflect current standards for operations support as follows:

- References to bandwidth services should be increased to reflect the current MFN-2 common bandwidth requirements based on ethernet services.
- References to 64k, T1, and other Digital Subscriber line services (DS) should be removed and replaced with more applicable MEF3.0 standards[42].
- Penalty caps should be evaluated for increase and/or removal to ensure that requested services are delivered to all required MFN subscriber locations. Considerations of special circumstances where last mile services are not available to support the required service requests should also be considered.
- SLAs for Cloud Services should be incorporated into the next contract as the use of cloud services is expected to increase based on Florida governmental statutes requiring increased cloud-based services consumption.
- Considerations for expanding "Internet Access Availability and Performance Degradation" SLA governance to include specific SaaS service environments such as Microsoft O365, Amazon, Google, and like providers should be considered for inclusion to ensure performance to critical services leveraged by the subscriber community is maintained at acceptable levels.
- SaaS services are becoming increasingly important to daily operations of agency workloads. Specific performance measurements to popular provider infrastructures should be considered for inclusion in SLAs to ensure the services provided meet the business needs of the MFN subscribers.

If a multi-award contract is selected, the SLAs should be applied to all contract areas as applicable. For example, performance metrics such as latency, jitter, and packet loss would be applicable to last mile services as well as core/backbone, however, specific measurement points for each provider would need to be incorporated. SLAs governing bandwidth subscription rates on the MFN integration circuits will also be required to ensure all vendors maintain a fair competitive environment.

Additional governance SLA's may also be required to support the defined mini-node expansion concept if selected. Governance on permitted bandwidth oversubscription will need to be defined and validated on production service deployments.

[42] https://www.mef.net/service-standards/underlay-services/carrier-ethernet/

Table 7 - MFN-2 Service Level Agreements

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Core Network Availability and Performance Degradation				
Core Network Availability: the amount of time the core network is accessible to the customers.	Outage restored within 60 seconds, with time increments of 1 hour	Credit of $250 per impacted customer end-site if outage is greater than 60 seconds. Credit is capped at 100% of customer end-site Monthly Recurring Charge (MRC) invoice per month. Credit of $100 per impacted customer end-site for each 1-hour increment. Credit is capped at 100%	A full mesh of availability measurement tests will be performed. The intention of a meshed testing configuration is to require a monitoring implementation with measurement "paths" to be effective at monitoring all necessary performance characteristics. The mesh of devices to be monitored is dependent on the Contractor's network design. Availability tests will be performed every 15 seconds. Each test will consist of five (5) 64-byte packets. Within each test, the loss of all five packets would indicate a test failure. Four (4) consecutive failed tests will trigger an alert in the alert monitoring system indicating an outage, which start the SLA clock. An SLA violation occurs when the	**All services in the MFN-2 Contract**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
		of customer end-site MRC invoice per month.	outage of any impacted customer site/connection/service is not restored or converged to an alternate infrastructure within the applicable performance target. The outage can be caused by any component within the core network which includes but is not limited to: • Failure of a network module (hardware or software) in the core which interconnects the access network (layer 2 infrastructure) • Misconfiguration of BGP peering or any other configuration error • Poor engineering or design • Line card failures • Core transport facility (interconnection) • Control plane The SLA clock stops once the impacted customer end-site is no longer impacted. The SLA clock start and stop times shall be validated part of the scrubbing	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			process using a combination of tools such as the Contractor's NOC ticket and the logs from the alert monitoring system. For example, logs from the alert monitoring system will be reviewed part of the scrubbing process to validate the accurate start timestamps are noted in the Contractor's NOC ticket. Core Performance Degradation and Core Network Availability SLAs are stacked (assessed separately) with the exception of: If a specific entire core node location is subjected to the Core Network Availability SLA, then the financial consequences for Core Performance Degradation SLA for that specific core node location shall not be assessed as well. However, other core node locations will be subjected to the Core Performance Degradation SLA requirement and financial consequences.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Latency (performance degradation): the round-trip delay between the core devices	Latency will be less than or equal to 45 ms round trip between core devices.	Credit of $10,000 if performance degradation continues beyond 2 hours. Credit applies for each 2-hour increment. Credit is capped at $40,000 per month.	A full mesh of latency, jitter, and packet loss measurement tests will be performed. The intention of a meshed testing configuration is to require a monitoring implementation with measurement "paths" to be effective at monitoring all necessary performance characteristics. The mesh of devices to be monitored is dependent on the Contractor's network design. Performance degradation tests will be repeated every 5 minutes. Each test will consist of two hundred (200) 1,400-byte packets. Within each test, any packet outside the performance target range would indicate a test failure. Three (3) consecutive failed tests will trigger an alert in the alert monitoring system indicating performance degradation, which starts the SLA clock. The performance target between core devices is the same regardless of the number of hops. For example, the performance target for latency applies regardless of if there are two, three, or	
Jitter (performance degradation): the delay variation in the time between packet arrivals between core devices	Jitter will be less than or equal to 20 ms round trip between core devices.			
Packet Loss (performance degradation): the percentage of packets lost as data is traveling between the core devices	Packet loss will be less than or equal to 0.5% between core devices.			

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			four hops between core devices. An SLA violation occurs when the performance degradation is not corrected within the applicable performance target. The SLA clock stops once the impacted customer end-site is no longer impacted. The SLA clock start and stop times shall be validated part of the scrubbing process using a combination of tools such as the Contractor's NOC ticket and the logs from the alert monitoring system. For example, logs from the alert monitoring system will be reviewed part of the scrubbing process to validate the accurate start timestamps are noted in the Contractor's NOC ticket. Core Performance Degradation and Core Network Availability SLAs are stacked (assessed separately) with the exception of: If a specific entire core	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			node location is subjected to the Core Network Availability SLA, then the financial consequences for Core Performance Degradation SLA for that specific core node location shall not be assessed as well. However, other core node locations will be subjected to the Core Performance Degradation SLA requirement and financial consequences.	
Internet Access Availability and Performance Degradation				
Internet Access Availability: the amount of time Internet Access is accessible to the customers.	Outage restored within 60 seconds with time increments of 1 hour	Credit of $5,000 if outage is greater than 60 seconds. Credit of $50,000 if outage is greater than one hour. Credit of $50,000 applies for each 1-hour increment.	Core Devise to Internet gateway: Availability tests shall be performed from the Core to Internet gateway. Availability tests will be performed every 15 seconds. Each test will consist of five (5) 64- byte packets. Within each test, the loss of all five packets would indicate a test failure. Four (4) consecutive failed tests will trigger an alert in the alert monitoring system indicating an outage, which starts the SLA clock.	All services in the MFN-2 Contract

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			Internet gateway to destinations on the Internet: Each Internet gateway probe in each Internet gateway complex will poll six (6) Internet Hosts once every sixty (60) seconds. The intention is to measure the Internet gateway's ability to access the Internet. A poll is defined as "HTTP GET." Loss of connectivity to all six (6) Internet Hosts from all Internet gateways specific to each VRF type would indicate a test failure. This test failure will trigger an alert in the alert monitoring system indicating an outage, which starts the SLA clock. An SLA violation occurs when Internet access ("Core device to Internet gateway" or "Internet gateway to destinations on the Internet") is not restored or converged to an alternate infrastructure within the applicable performance target. The outage can be caused by any component between the core device and the Internet gateway facility, or any device in the critical path to the Internet. This	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			includes but is not limited to: • Failure of any component between the core and the Internet gateway facility • Configuration errors • Poor engineering or design • Line card failures • Firewall devices and services • Virus/Malware Signatures not updated • Intrusion Detection System devices • Domain Name Servers (DNS) failure • Content filtering services • Lack of default route The SLA clock stops once the impacted customer end-site is no longer impacted. The SLA clock start and stop times shall be validated part of the scrubbing process using a combination of tools such as the Contractor's NOC ticket and the logs from the alert monitoring system. For example, logs from the alert monitoring system will be	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			reviewed part of the scrubbing process to validate the accurate start timestamps are noted in the Contractor's NOC ticket. Internet Performance Degradation and Internet Access Availability SLAs are stacked (assessed separately) with the exception of: If the Internet Access Availability SLA is invoked then the Internet Access Performance SLA shall not apply to the same elements of the network that are down. In addition, this SLA does not apply in the event that the loss of internet access availability is determined, via the mitigation process, to be the result of a DDoS attack. In this event, the "Initiate Mitigation of DDoS Attack" SLA would apply.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Latency (performance degradation): the round-trip delay between the core device and the Internet gateway device.	Between the core device and the Internet gateway device, latency will be less than or equal to 45 ms round trip.	Credit of $10,000 if performance degradation continues beyond 2 hours. Credit applies for each 2-hour increment of time. Credit is capped at $40,000 per month.	A full mesh of latency, jitter and packet loss measurement tests will be performed. The intention of a meshed testing configuration is to require a monitoring implementation with measurement "paths" to be effective at monitoring all necessary performance characteristics. Performance degradation will be measured from a mesh of core probes to Internet gateway probes. Performance degradation tests will be repeated every 5 minutes. Each test will consist of two hundred (200) 1400-byte packets. Within each test, any packet outside the performance target range would indicate a test failure. Three (3) consecutive failed tests will trigger an alert in the alert monitoring system indicating performance degradation, which starts the SLA clock. The performance target between the core devices and the Internet gateway devices is independent of the number of hops. For example, the performance	
Jitter (performance degradation): the delay variation in the time between packet arrivals between the core device and the Internet gateway device.	Between the core device and the Internet gateway device, jitter will be less than or equal to 20 ms round trip.			
Packet Loss (performance degradation): the percentage of packets lost as data is traveling between the core device and the Internet gateway device.	Between the core device and the Internet gateway device, packet loss will be less than or equal to 0.5%.			

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			target for latency will apply even if there are two, three or four hops between the core devices and the Internet gateway devices. An SLA violation occurs when the performance degradation is not corrected within the applicable performance target. The SLA clock stops once the impacted customer end-site is no longer impacted. The SLA clock start and stop times shall be validated part of the scrubbing process using a combination of tools such as the Contractor's NOC ticket and the logs from the alert monitoring system. For example, logs from the alert monitoring system will be reviewed part of the scrubbing process to validate the accurate start timestamps are noted in the Contractor's NOC ticket. Internet Performance Degradation and	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			Internet Access Availability SLAs are stacked (assessed separately) with the exception of: If the Internet Access Availability SLA is invoked then the Internet Access Performance SLA shall not apply to the same elements of the network that are down.	
Local Loop Access and CPE Availability and Performance Degradation				
Local Loop Access and CPE availability: the amount of time the local loop access and/or CPE is accessible to the customer.	Outage restored within 4 hours, with time increments of 4 hours	Credit of $150 per impacted customer end-site if outage continues beyond 4 hours. Credit applies for each 4-hour increment. Credit is capped at 200% of customer end-site MRC invoice per month.	CPE and local loop access availability measurement test will be performed. The CPE will be polled every 5 minutes from the Contractor's network management system. One missed poll will indicate a test failure. One failure will trigger an alert in the alert monitoring system indicating an outage, which starts the SLA clock. An SLA violation occurs when outage is not restored within the applicable performance target. The SLA clock stops once the impacted customer end-site is no longer	**All services in the MFN-2 Contract**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			impacted. The SLA clock start and stop times shall be validated part of the scrubbing process using a combination of tools such as the Contractor's NOC ticket and the logs from the alert monitoring system. For example, logs from the alert monitoring system will be reviewed part of the scrubbing process to validate the accurate start timestamps are noted in the Contractor's NOC ticket.	
Latency (performance degradation): the round-trip delay from the CPE to the core device.	For bandwidth speeds 256kbps and greater, latency will be less than or equal to 75 ms round trip. For bandwidth speeds less than 256kbps, latency will be less than or equal to 100 ms round trip.	Credit of $150 per impacted customer end-site if performance degradation continues beyond 4 hours. Credit applies for each 4-hour increment. Credit is capped at 200% of customer end-site MRC	CPE latency, jitter and packet loss measurement tests will be performed. Measurements are between the loopback 0 interface on the CPE to the core device. Performance degradation will not trigger an SLA violation if the local loop access utilization is greater than or equal to 75%. Performance degradation tests will be repeated every 5 minutes. Each test will consist of one hundred (100) 40-byte packets.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Jitter (performance degradation): the delay variation in the time between packet arrivals between the CPE and the core device.	Jitter will be less than or equal to 30 ms round trip.	invoice per month. Latency, jitter, and packet loss SLAs are stacked (assessed separately) if it can be accurately determined they are based on unrelated causes. If there are separate assessments, the cap remains at 200% of the MRC.	Within each test, any packet outside the performance target range would indicate a test failure. Three (3) consecutive failed tests will trigger an alert in the alert monitoring system indicating performance degradation, which starts the SLA clock. An SLA violation occurs when the performance degradation is not corrected within the applicable performance target. The SLA clock stops once the impacted customer end-site is no longer impacted. The SLA clock start and stop times shall be validated part of the scrubbing process using a combination of tools such as the Contractor's NOC ticket and the logs from the alert monitoring system. For example, logs from the alert monitoring system will be reviewed part of the scrubbing process to validate the accurate start	
Packet Loss (performance degradation): the percentage of packets lost as data is traveling from the CPE to the core device.	Packet Loss will be less than or equal to 1%.			

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			timestamps are noted in the Contractor's NOC ticket.	
Operational				
Service Availability Check (Service Inquiry) - Check availability of fiber facilities from Contractor's facility (e.g., Central Office) to customer's premises	Complete within 10 calendar days	Credit of $100 per calendar day, for each customer end-site request not completed within the performance target. Credit is capped at 100% of customer end-site MRC invoice per month.	This SLA is only applicable to new sites/connections/services installed under the MFN2 contract, not those sites/connections/services that are migrating from the current Contracts to MFN-2. Service availability check for fiber local loop facilities will be completed by Contractor; this process takes place before DMS submits a service order to the Contractor. An SLA violation occurs when the service availability check results are not completed and provided to DMS within	All services in the MFN-2 Contract

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			the applicable performance target. The SLA clock starts with the official statement to the Contractor either through an email or the CSAB system. The SLA clock stops when the service availability check results have been completed and provided to DMS. The Contractor shall provide the results of the service availability check to DMS either through an email or the CSAB system. DMS, at its sole discretion, will select the method of delivery; either through email or CSAB system.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Facility Installation Date for orders that require Special Construction if bandwidth speed is greater than 12Mbps (Based on the Service Availability Check results)	Provide the number of calendar days to complete the service order with facility installation within 7 calendar days of the Service Availability Check results.	Credit of $100 per calendar day, for each request not completed within the performance target. Credit is capped at 200% of customer end-site MRC invoice per month.	This SLA is only applicable to new sites/connections/services installed under the MFN2 contract, not those sites/connections/services that are migrating from the current Contracts to MFN-2. The Contractor shall provide the number of calendar days to complete installation of the facility. This SLA will only apply if the "Service Availability Check" SLA results indicate that special construction is required to build-out facilities. In addition, this SLA will only apply for bandwidth speeds greater than 12Mbps if special construction is required to build-out facilities. For bandwidth speeds 12Mbps and lower orders that require special construction, the Operational IMAC SLA (Type 1) will apply. An SLA violation occurs when the Facility Installation Date is not provided by the Contractor to DMS within the applicable performance target.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			The SLA clock starts once the results of the Service Availability Check are complete and provided to DMS. The SLA clock stops when the Facility Installation Date is provided to DMS. The Contractor shall provide the Facility Installation Date to DMS either through an email or the CSAB system. DMS, at its sole discretion, will select the method of delivery; either through email or the CSAB system.	
Operational Installation, Move, Add, Change (IMAC) - Type 1 (Service Order)	Complete 64kbps to T1 service within 30 calendar days	Credit of $100 per calendar day, for each customer end-site service order not completed within the applicable performance target. Credit is capped at 200% of customer end-site MRC invoice per month.	This Operational IMAC SLA is only applicable to new sites/connections/services installed under the MFN2 contract, not those sites/connections/services that are migrating from the current Contracts to MFN-2. Disconnect of services is not considered an IMAC. This Operational IMAC SLA (Type 1) will	
	Complete greater than T1 to 45Mbps service within 45 calendar days			

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
	Complete greater than 45Mbps service within 90 calendar days		apply to all service orders with the exception of where special construction is required to build-out facilities for bandwidth speeds greater than 12Mbps. This Operational IMAC SLA (Type 1) will also apply if special construction is required to build-out facilities for bandwidth speeds 12Mbps and lower. If no special construction is required to build-out facilities, this Operational IMAC (Type 1) will apply to all bandwidth speeds. An SLA violation occurs when the Operational IMAC is not completed within the applicable performance target. The performance target timeframe includes the Contractor's responsibility to survey the site. As part of the site survey, the Contractor will evaluate the condition of the site in order for the site to be ready for services. The Contractor shall provide the results of the site survey to the customer and DMS including a list of corrective actions if	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			any. The SLA clock starts when the Contractor receives a complete and accurate service order from DMS. The SLA clock will not restart for any reason once the service order is submitted to the Contractor. However, the SLA clock will be suspended for any of the approved SLA hold time reasons listed in the "Performance Measures" section of the Statement of Work, section 3. The SLA clock start and stop timestamps will be reported in CSAB. CSAB system will be the book of record for timestamps and order issuance to the Contractor. The SLA clock stops when all criteria have been met in the "Criteria for IMAC signoff and billing start" subsection of the "Miscellaneous Conditions" section of the Statement of Work, 2.21.24	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Operational Installation, Move, Add, Change (IMAC) - Type 2 (Service Order)	- CPE upgrade on existing local loop access - CPE module upgrade on existing CPE Complete within 30 calendar days for bandwidth up to 10Mbps Complete within 45 calendar days for bandwidth greater than 10Mbps	Credit of $100 per calendar day, for each customer end-site service order not completed within the applicable performance target. Credit is capped at 200% of customer end-site MRC invoice per month.	This Operational IMAC SLA is only applicable to new sites/connections/services installed under the MFN2 contract, not those sites/connections/services that are migrating from the current Contracts to MFN-2. Disconnect of services is not considered an IMAC. This group of simple Operational IMACs are initiated through the CSAB system, not the Contractor's NOC ticketing system. An ongoing list of Simple Operational Changes will be	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
	- Extension of the Demarcation on existing service within the same building - Bandwidth upgrade/downgrade on existing local loop access. For example, if a customer has a 12 Mbps local loop access provisioned on a DS3 and a DS3 upgrade is needed to accomplish the upgrade - Establishing optional features such QoS, Multicast, and Encryption on existing service that requires DMS service order.		developed during the standing monthly operational meetings based on a historical sample of service order requests. However, below is an approved list of Simple Operational Changes that the Contractor will comply with: 1. CPE upgrade on existing local loop access 2. CPE module upgrade on existing CPE 3. Extension of the Demarcation on existing service within the same building 4. Bandwidth upgrade/downgrade on existing local loop access. For example, if a customer has a 12 Mbps local loop access provisioned on a DS3 and a DS3 upgrade is needed to accomplish the upgrade 5. Establishing optional features such QoS, Multicast, and Encryption on existing service that requires DMS service order. An SLA violation occurs when a Simple	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
	Complete within 15 calendar days		Operational Change is not completed within the applicable performance target. The SLA clock will start when the Contractor receives a complete and accurate service order from DMS. The SLA clock will not restart for any reason once the service order is submitted to the Contractor. However, the SLA clock will be suspended for any of the approved SLA hold time reasons listed in the "Performance Measures" section of the Statement of Work, section 3. The SLA clock start and stop timestamps will be reported in CSAB. CSAB system will be the book of record for timestamps and order issuance to the Contractor. The SLA clock stops when all criteria have been met in the "Criteria for IMAC signoff and billing start" subsection of the "Miscellaneous Conditions" section of the Statement of Work 2.21.24.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Operational Installation, Move, Add, Change (IMAC) - Type 3: CPE Configuration Changes (Request via Contractor's NOC Ticketing System)	Complete simple changes in less than or equal to 2 hours (at the rate of up to 6 devices in a 2-hour window)	Credit of $50 per hour per request up to six devices beyond the performance target. Credit applies for each 1-hour increment. Credit is capped at 200% of customer end-site MRC invoice per month.	An SLA violation occurs when the simple CPE configuration change is not completed within the performance target. Simple CPE configuration changes will be reported in the Contractor's trouble ticketing system with the SLA clock start and stop time stamps. The SLA clock will start when the trouble ticket is created within the Contractor's trouble ticketing system. The SLA clock will stop when the changes are complete and the Contractor's NOC ticket is closed.	**All services in the MFN-2 Contract**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Operational Installation, Move, Add, Change (IMAC) - Type 4: VPN Appliance (Service Order)	Complete within 30 calendar days	Credit of $25 per calendar day, for each customer end-site service order not completed within the performance target. Credit is capped at 100% of customer end-site MRC invoice per month.	This Operational IMAC SLA is only applicable to new sites/connections/services installed under the MFN2 contract, not those sites/connections/services that are migrating from the current Contracts to MFN-2. Disconnect of services is not considered an IMAC. An SLA violation occurs when this Operational IMAC is not completed within the performance target. The SLA clock starts when the Contractor receives a complete and accurate service work from DMS. The SLA clock will not restart if the Contractor rejects the service order. However, the SLA clock can be suspended for any of the approved SLA hold time reasons listed in the "Performance Measures" section of the Statement of Work, section 3.	
Operational Installation, Move, Add, Change (IMAC) - Type 5: Firewall (Service Order)	Complete within 30 calendar days	Credit of $25 per calendar day, for each customer end-site service order not completed within the performance target. Credit is capped at 100% of customer end-site MRC invoice per month.		

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			The SLA clock start and stop timestamps will be reported in CSAB. CSAB system will be the book of record for timestamps and order issuance to the Contractor. The SLA clock stops when all criteria have been met in the "Criteria for IMAC signoff and billing start" subsection of the "Miscellaneous Conditions" section of the Statement of Work 2.21.24. IMAC Type 4: Applies to contractor-provided VPN appliances. In addition, SLA applies to customer-Provided VPN appliance with contractor installation. IMAC Type 5: Applies to only contractor-provided firewall equipment.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Operational Installation, Move, Add, Change (IMAC) – Type 6 (Service orders that require Special Construction for bandwidth speeds greater than 12Mbps.)	Complete the service order within the number of calendar days specified in the results provided by the Contractor in response to the Facility Installation Date SLA requirement.	Credit of $100 per calendar day, for each customer end-site service order not completed within the applicable performance target. Credit is capped at 200% of customer end-site MRC invoice per month.	This Operational IMAC SLA is only applicable to new sites/connections/services installed under the MFN2 contract, not those sites/connections/services that are migrating from the current Contracts to MFN-2. Disconnect of services is not considered an IMAC. This Operational IMAC SLA (Type 6) will apply for bandwidth speeds greater than 12Mbps if special construction is required to build-out facilities. For bandwidth speeds 12Mbps and lower that require special construction, the Operational IMAC SLA (Type 1) will apply. An SLA violation occurs when this Operational IMAC is not completed within the performance target. The SLA clock starts when the Contractor receives a complete and accurate service order from DMS. The	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			SLA clock will not restart if the Contractor rejects the service order. However, the SLA clock can be suspended for any of the approved SLA hold time reasons listed in the Statement of Work, Section 3, Performance Measures. The SLA clock start and stop timestamps will be reported in CSAB. CSAB system will be the book of record for timestamps and order issuance to the Contractor. The SLA clock stops when all criteria have been met in the Statement of Work, Section 2.21, Criteria for IMAC signoff and billing start" subsection 2.21.24.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Service Order Status Updates	Provide status updates for all pending service orders at a minimum of bi-weekly (every other week) on Wednesday (by 5:00 PM ET.).	Credit of $50 per calendar day beyond the performance target. Credit is not capped.	Status updates will be emailed to DMS using an email distribution list. The Contractor will provide detail status updates including the following: 1) Contractor will provide DMS the milestones associated with each service with milestones shown throughout the installation and service order process. Examples include but not limited to: a) Order assigned to a group or moved between groups, b) Local loop access facilities assigned, c) Site visit made, d) Local loop facilities available, e) Special Construction needs assessment, f) CPE orders g) CPE configurations 2) If applicable, an explanation as to why the order cannot be fulfilled by the agreed upon due date or an acknowledgment that the order is on target meeting the due date An SLA violation occurs if DMS does not receive sufficient status updates within the performance target. Furthermore,	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			an SLA violation occurs if the status update is provided with insufficient details.	
Equipment End-of-Life (EOL) Support: - CPE such as routers, VPN appliances and firewalls. - Core equipment such as Core routers, Internet gateway, firewalls, DNS, SCR, and probes.	Upgrade and refresh CPE by EOL support date declared by the equipment manufacturer	Credit of $50 per calendar day, for each CPE, not upgraded or refreshed before the performance target. Credit is not capped.	The Contractor is responsible to upgrade (refresh) equipment declared End-of-Life by the equipment manufacturer. This includes both the hardware and software EOL support. An SLA violation occurs if the Contractor does not upgrade (refresh) the equipment by the performance target. The SLA requirement and financial consequences for hardware and software EOL support are distinct and will apply on a per incident basis for each customer end-site.	
	Upgrade and refresh core equipment by EOL support date declared by the equipment manufacturer	Credit of $100 per calendar day, for each core equipment, not upgraded or refreshed before the performance target.		

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
		Credit is not capped.		
Service notifications	Within 15 minutes for an outage notification Within 30 minutes for a degradation notification	Credit of $50 per impacted customer end-site Credit is capped at 100% of customer end-site MRC invoice per month.	Service notifications will be provided through Contractor's alert monitoring system. Customers must enroll a single email address (distribution list) in the Contractor's alert monitoring system in order to qualify for this SLA. If customer approves, customer may opt-out from receiving degradation notification if the local loop access utilization is greater than or equal to 75%. The SLA clock starts when the applicable tool detects the outage or degradation. An SLA violation occurs when notifications are delayed beyond the applicable performance target.	**All services in the MFN-2 Contract**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			The SLA clock start and stop times are based on timestamps in the alert monitoring system.	
SLA Scrubbing and Validation report - Contractors Submission and DMS approval	Complete within two (2) calendar months	Credit of $50 per calendar day for each day beyond the performance target Credit is not capped.	The Contractor will present to DMS a complete SLA report detailing all the raw data for the specific SLA month. This report will detail all categories of the SLAs listed in this Exhibit. The SLA report will provide SLA compliance and violation details needed for a proper reconciliation. SLA scrubbing and validation process will occur monthly. The data collection ends on the last day of the month and the scrubbing and validation process begins the following day (on the first day of each month), lasting two calendar months. The two-calendar	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			month scrubbing process includes the Contractor compiling a complete SLA report detailing all raw data for the specific SLA month. DMS and the Contractor are responsible to analyze the data. The goal of the process is to cull the raw data down to an accurate list of SLA violations. Once there is an agreement on the violations, the Contractor will finalize the related SLA credits. To finalize the SLA credits, the Contractor will provide DMS with the detail SLA credits ready for final approval. The Contractor's two calendar month window must allow 10 calendar days for DMS to perform its final review & approval. An SLA violation occurs if DMS is not able to provide final approval of SLA violations within the SLA window. Final approval will be withheld when an accurate list of SLA violations has not been obtained due to inaccurate or incomplete detailed reporting. DMS will work in good faith and be reasonable in cases where final	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			approval is withheld. However, DMS requires the Contractor will apply an appropriately staffed team and make available other necessary resources to complete the Scrubbing and Validation process on time. The SLA clock starts the day the scrubbing process begins. The SLA clock stops when DMS receives and approves the final list (report) of SLA violations and related SLA credits.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Application of Credits from the Scrubbing and Validation process	After the scrubbing and validation process, SLA credits are applied to the appropriate customer account by the next billing cycle. The "next billing cycle" is illustrated with examples in the SLA details of this SLA requirement.	Credit of $50 per calendar day for each day beyond the performance target until all SLA credits are applied to the appropriate customer account Credit is not capped.	An SLA violation occurs if the Contractor has not applied the agreed upon SLA credits due from the SLA Scrubbing and Validation process within the applicable performance target. The performance target for applying SLA credits will not be delayed if there is a delay completing the Scrubbing and Validation process. Example 1: 1. The SLA Scrubbing and Validation Process for the January 2014 SLA report lasts two (2) calendar months ending 3/31/2014. 2. SLA Credits must be posted to "5/1/2014 to 5/31/2014" billing cycle also known as the 5/1/2014 "Bill Date" Example 2: 1. The SLA Scrubbing and Validation Process for the February 2014 SLA report lasts two (2) calendar months ending 04/30/2014.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			2. SLA Credits must be posted to "6/1/2014 to 6/30/2014" billing cycle also known as the 6/1/2014 "Bill Date" Example 3: 1. The SLA Scrubbing and Validation Process for the March 2014 SLA report lasts two (2) calendar months ending 05/31/2014. 2. SLA Credits must be posted to "7/1/2014 to 7/31/2014" billing cycle also known as the 7/1/2014 "Bill Date"	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Timely Invoicing	All invoices will be electronically posted to DMS within 10 calendar days of the bill date	Credit of $250 per calendar day until all invoices are posted Credit is not capped.	An SLA violation occurs if the Contractor has not submitted all invoices within the applicable performance target. The Contractor's billing cycle ends on the last day of the calendar month. The billing cycle starts on the first day of each calendar month and ends the last day of the same calendar month. For example, a billing cycle of 2/1/2014 through 2/28/2014 or a billing cycle of 5/1/2014 through 5/31/2014. The SLA violation will start on the 11th of the calendar month of billing cycle and stop when all invoices have been electronically posted to DMS. To ensure coordination, the Contractor will provide an email notification of the posting and DMS will immediately provide an official statement of the receipt of the billing invoices. Example 1: For the 1/1/2014 through 1/31/2014	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			billing cycle, an SLA violation occurs if all invoices are submitted on the 15th of January 2014. In this case, the invoice is late 5 days with a total credit amount of $1,250. Example 2: For the 2/1/2014 through 2/28/2014 billing cycle, an SLA violation will not occur if all invoices are submitted by the 10th of February 2014. In this case, the SLA requirement has been met. Example 3: For the 3/1/2014 through 3/31/2014 billing cycle, an SLA violation occurs if all invoices are submitted by the 12th of February 2014. In this case, the invoice is 2 days late with a total credit amount of $500.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Timely Correction of Billing Issues and Adjustments	Resolve billing issues and post invoice adjustments by the next billing cycle. The "next billing cycle" is illustrated with examples in the SLA details of this SLA requirement.	Credit of $5,000 per billing cycle beyond the performance target Credit is not capped.	An SLA violation occurs if the Contractor has not resolved all billing issues and provided all billing adjustments within the applicable performance target. The Contractor will apply all billing adjustments on its next invoice as illustrated by the example below. The Contractor's billing cycle ends on the last day of the calendar month. The billing cycle starts on the first day of each calendar month and ends the last day of the same calendar month. For example, a billing cycle of 2/1/2014 through 2/28/2014 or a billing cycle of 5/1/2014 through 5/31/2014. Within 15 days of receiving an invoice, DMS will provide the Contractor with a written statement detailing all billing issues. The Contractor then works to post invoice adjustments. This SLA shall not be waived if there is a delay in providing a timely invoice.	**All services in the MFN-2 Contract**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			For example: 1. For the 01/01/2014 through 01/31/2014 billing cycle, the Contractor delivers a timely invoice to DMS by 01/10/2014. 2. By 01/25/2014 DMS provides the Contractor with an official written statement detailing all billing issues. 3. The Contractor must resolve all billing issues and post adjustments to the 3/1/2014 through 3/31/2014 billing cycle also known as the 03/01/2014 bill date.	

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Functionality of Network Management Systems	Outage or Functionality restored within 4 hours.	Credit of $100 per hour that any of the NMS tools are not functional Credit is not capped.	The Contractor will be responsible for credits if there are performance issues with the functionality of Network Management Systems. An SLA violation occurs when functionality or outage of any NMS component is not restored to normal operation within the applicable performance target. All NMS tools must be monitored for proper functionality including up and down status and reported to DMS. The SLA clock start and stop times are based on timestamps in the alert monitoring system and validated in the scrubbing process. The SLA clock will stop once the functionality or outage of the NMS tool has been restored.	
Remote Access VPN Service				

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Centralized VPN Appliance	Outage restored within 1 hour, with time increments of 1 hour	Credit of $25 per impacted customer end-site per hour if outage is greater than 1 hour Credit is capped at 200% of customer end-site MRC invoice per month.	The SLA violation measurement tool shall log all SLA violations and automatically send an electronic notification(s) for all service issues. The SLA clock start and stop time are based on timestamps in the alert monitoring system. An SLA violation occurs if any transport circuit fails in the VPN IP connectivity path managed by the Contractor. The SLA violation measurement timer shall start five minutes after the Centralized (or Distributed) VPN service is interrupted and continue five minutes after the service restoration. The SLA monitoring solution must verify that all VPN service components are functional; supporting VPN connectivity as configured for both the stateside and	**All services in the MFN-2 Contract**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Remote site VPN Appliance	Outage restored within one calendar day for in-state and two calendar days for out-of-state with both (in-state and out-of-state) time increments of 1 day.	Credit of $25 per impacted customer end-site per calendar day if outage is greater than one calendar day for in-state. Credit of $25 per impacted customer end-site per calendar day if outage is greater than two calendar days for out-of-state. Credit for both is capped at 200% of customer end-site MRC invoice per month.	the remote side if the remote site is a Contractor provided VPN appliance. IP connectivity to the remote site VPN appliance must be monitored for all possible service anomalies. CPU and RAM Memory 70% Utilization: During normal operation over any five (5) minute period a system element reaches seventy percent (70%) of CPU capacity or RAM memory utilization, the Service Provider shall upgrade that element (or cluster addition devices) within 60-days. Transport Circuit 80% Utilization : The bandwidth capacity, of that connected, to the Centralized VPN solution shall be increased within 60-days, if over any five (5) minute period of normal operation, circuit utilization exceeds eighty-percent (80%) of total circuit throughput capacity.	
Centralized VPN Service Hardware Components	CPU and RAM Memory 70% Utilization	Credit of $25 per day starting on the 61-day and each day thereafter until the system element has been upgraded Credit is not capped		

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Centralized VPN IP Transport Circuits	Transport Circuit 80% Utilization	Credit of $25 per day starting on the 61-day and each day thereafter until the transport circuit has been upgraded Credit is not capped.		
Security				
Security Incident Notification	Notification within 15 minutes	Credit applies as follows: >15 to 30 Minutes $1,500 credit >30 to 120 Minutes $2,500 credit >120 Minutes $5,000 credit Credit is capped at $20,000 per month.	The Contractor shall notify DMS and the Customer via email to authorized users when a critical security event that represents a security incident or threat to the Customer, within the performance target timeframe. Upon receipt of an alert from equipment, and active verification by SOC personnel of a security incident, an incident ticket is opened to track the event through the mitigation process.	Any service impacted by security incidents

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			The SLA clock starts when a security incident ticket is opened. An SLA violation occurs when the amount of time between opening a security incident ticket and the notification of DMS and the Customer exceeds the performance target.	
Initiate Mitigation of DDoS Attack	Redirect traffic to DDoS Mitigation Service within 45 minutes	Credit applies as follows: >45 to 60 Minutes $2,500 credit >60 to 120 Minutes $5,000 credit >120 Minutes $7,500 credit Credit is capped at $35,000 per month.	Upon receipt of an alert from equipment, and active verification by SOC personnel of a DDoS attack affecting customer internet access, a DDoS attack ticket is opened to track the event through the mitigation process. An SLA violation occurs when the amount of time between opening a DDoS attack ticket and the initiation of the mitigation (redirecting traffic to DDoS mitigation service) exceeds the performance target.	Any service impacted by DDoS Attack

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
Migration				
MFN-2 Services Infrastructure and Migration of Sites/Connections/Services from Current Contracts (MFN and FIRN Contracts)	Complete within 20 months of Award Date	Credit of $25,000 per calendar day until migration of all sites/connections/services are completed and accepted by DMS. Credit is not capped.	The migration window includes the completion of the MFN2 Service Infrastructure checklist (refer to the final checklist attached by DMS with the BAFO request and section on performance measure in the statement of work) and migration of all sites/connections/services off of the current contracts (MFN and FIRN contracts). The SLA clock will start on the Award Date. The official Award Date will be posted on the Vendor Bid System (VBS) which starts the SLA clock. The Award Date is not the Contract Execution Date. The Contract is executed after the Award. An SLA violation occurs if any MFN sites/connections/services remain on the current contracts (MFN and FIRN Contracts) beyond the performance target.	**Migration**

MyFloridaNet-2				
SLA Requirements	**Performance Target**	**Financial Consequence for non-performance**	**SLA Details, Measurement and Performance Criteria**	**Service Applicability**
			The Contractor is cautioned that these migration responsibilities are in addition to the typical Operational IMAC that take place in the day-to-day environment of the production network. To be accurate, the Contractor's project plan must take into account the typical day-to-day environment and estimate the impact of typical Operational IMAC in forecasting the resources required to avoid providing service credits for failure to migrate sites/connections/services within the performance target.	

7 Projected Timeline

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 MFN-2 contract model had an initial 7-year contract period with up to seven 1-year renewal options thereafter. This model allowed the core and backbone vendor to recoup their initial investment, while allowing DMS flexibility to explore options after the initial period. The MFN-3 contract period of performance for core and backbone services is projected to follow this same timeline, with an initial contract period of seven years, followed by up to seven one-year renewal options. The renewal period negotiations will permit DMS and the awarded vendor to renegotiate the current terms and financial costs for the associated program efforts to reflect the current reality of the market and investments made into the MFN-3 solution. This will also permit DMS and the MFN-3 vendor(s) to add additional service offerings that have benefit to the MFN subscriber communities.

Alongside the core and backbone "7 and 7" model, if a multi-award approach for last-mile services is leveraged, a shorter period of performance may allow the State to take advantage of the full competitive market for last-mile services. During the re-procurement of last mile service categories, previous and new vendors may be qualified and included in the new contract with updated pricing. . As sites are awarded on a per-site, best-value competitive basis, this allows for competitive pricing over the core category's extended period of performance. Following this model is intended to enable cost avoidance for last-mile services while promoting competition in local regions where circuits are serviced.

It is estimated that a similar timeline to the MFN-1 to MFN-2 transition will be required if selections are made that result in a new core and backbone services vendor, as well as replacement of each circuit serviced by MFN-2. This includes a six-to-nine-month review and selection process for the MFN-3 contract once DMS receives the ITN (Invitation to Negotiate) responses. An additional 24-month transition period to the new core and backbone, as well as last-mile providers will then be required.

Key Events:

- Obtain legislative approval and finalize ITN
- Complete ITN solicitation
- Release ITN to public
- Receive ITN responses
- Review ITN responses, conduct negotiations, and develop recommendations to award
- Prepare and execute contract
- MFN-3 migration efforts completed over 20-month period

- 4-month period for MFN-3 infrastructure preparation
- MFN-3 migration completion
- Process contract renewal options
- End of contract period

This space intentionally left blank

8 Public Records Law 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.

This space intentionally left blank

9 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.

The procurement of MFN-3 should include language drafted in consultation with DMS legal counsel and DMS procurement staff. The contract should outline a plan, subject to negotiation process, to address contractor non-performance.

The procurement 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.

The Department of Management Services should include provisions in the new contract for financial consequences in the event the service provider does not meet established and measured performance expectations. The provisions should provide incentive for a contractor to cure any problems with performance before an event of default occurs.

Suggested remedies for DMS for default and obligations upon termination include:

- 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 contractor 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; and
- Upon prior notice to the Service Provider, after the expiration of any cure periods, perform any term, condition, or covenant that has been breached by the Service Provider at the reasonable expense of the Service Provider.

General suggested termination rights include:

- The ability to terminate individual service areas to allow the Agency to insource components when they are able to perform those duties in the best interest of the state; and
- Service Provider must provide termination assistance services, detailed below.

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, established in writing.

Financial consequences suggestion:

- Financial consequences language including amounts should be included in the ITN and awarded contract. This language should be developed in consultation with DMS legal counsel and DMS Purchasing staff.

Two specific areas to address:

- Should the Service Provider fail to achieve service operation as defined by a mutually negotiated and acceptable implementation plan through the ITN process; as a result of activities/tasks directly within the Service Provider's control, then the Service Provider shall pay an appropriate amount based upon the contractually agreed upon service level agreement until service operation is deemed acceptable by measured contract stipulations per the agreed upon plan; and
- Should the Service Provider fail to achieve the performance metrics prescribed in the contract, as a result of activities/tasks directly within Service Provider's control, then the Service Provider shall pay DMS liquidated damages for each performance metric not met.

10 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.

Section 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. If, at the completion of the current MFN contract, DMS decides to contract with a new vendor, the following steps are advised to ensure a smooth transition of service. In the event that the current contractor is awarded, and if no contractual requirements are changed, the transition plan would only require publishing the new MFN service model with pricing. It is assumed this is an administrative process that is routinely performed given the current MFN contract has gone through numerous amendments with this type of activity already being performed, so there is no impact to the existing process.

10.1 Transition Plan Overview

The Transition Plan suggestions below outline key activities that must be completed while working with DMS and the incumbent vendor, should a transition be required. To ensure a complete and successful ramp up of a team that can provide implementation, engineering, and support services for MFN, the new service provider should be required to provide a detailed migration plan that takes the following into consideration:

- Resources
- Knowledge Transfer
- Communications Plan
- Engineering Review
- MFN Services Transition Plan
    - Network Communications Services
    - Internet Services
    - Cloud Integration Services
    - Security Services
    - Remote Access/VPN

- Ancillary Services

- Provisioning Planning
- Network Operations Center
- Administrative Services

10.2 Resources

The new service provider will confirm the resources needed to provide the support services based upon the technical specifications agreed upon in the ITN. The level of resourcing required from DMS as well as the service provider will depend on the contract type selected. Under any of the contracting models, it is advisable that DMS review and approve proposed resources by vendors to ensure a sufficient level of technical expertise is being provided. Under any of the contract models, the new service provider should be committed to identifying the best resources to fulfill the needs of the project plan.

It is anticipated that due to the large number of DMS customer sites, the service provider should be prepared to assign the appropriate level of dedicated technical project managers and engineering teams. The DMS project team should work with the service provider to define a "Staffing Plan" that outlines (per resource role) the required skill set and desired on-boarding date that meets the expectations of the overall MFN Transition Plan. The staffing plan should be documented and accepted by DMS prior to execution. The on-boarding date for the resources will correspond with the needs of the Knowledge Transfer activities to ensure that resources are on-boarded to fully participate in the activities with incumbent resources as appropriate.

In addition to technical considerations, if the model including a multi-vendor approach to last mile services is selected, DMS will have an increase in responsibility related to Contract Management, Customer Service, Finance, Engineering, and CSAB development offices.

10.3 Knowledge Transfer

Knowledge transfer activities are critical to the success of any transition plan. The MFN-3 service provider, assisted by Department of Management Services, must provide resources to lead and facilitate the knowledge transfer work activities. During the knowledge transfer work effort, the MFN-2 incumbent contractor should be the sole party responsible for support and maintenance of the MFN service layers that are operational through the migration period.

The activities to be completed for each service layer within MFN should be documented in a Knowledge Transfer Plan. The incumbent and new service providers should monitor the Knowledge Transfer Plan on a weekly basis to confirm that resources are completing their knowledge transfer activities in a timely manner. MFN subscriber specific documentation such as site access procedures, subscriber contact/notification standards, and other such information, should be made available and shared in an agreed upon format between the incumbent and new vendors. This should include a full list of the current MFN services and their corresponding service details. This should also include a full

list of each L3 VRF (Virtual Routing and Forwarding) service provisioned on the MFN and the list of attachment circuits for each. Circuit details should include all relevant technical details, such as:

- Bandwidth
- Logical channel ID (vlan, etc.)
- Logical integration details
    - Carrier and CPE IP addressing/subnet mask
- L3 routing details
    - Dynamic vs. static routing and associated policies
- Associated QoS (Quality of Service) profile

10.3.1 Communication Plan

The Department of Management Services, along with both the incumbent and new service provider, should implement a Communication Plan that identifies and addresses the concerns of all key stakeholders during the transition period and the life of the contract. The Communication Plan outlines the following:

- Communication Event(s)
- Communication Vehicle(s)
- Stakeholders list
- Communication Plan Start Date
- Communication Plan End Date
- Frequency of Communication
- Owner of the Communication

The purpose of the Communication Plan is to document identified communication needs and processes that will be used to address the communications objectives:

- Identify key stakeholders
- Provide communications timely and accurately
- Provide feedback mechanisms to ensure feedback is appropriately reviewed
- Adjust the communication plan as necessary to address gaps identified through the process

With a project as large as the MFN that affects a significant aspect of government business in Florida, ensuring subscribers are kept abreast of planned timelines is critical. Sufficient notice of planned events, especially those with a potential impact to services, permits subscribers to plan accordingly to lessen the overall impact to their business. Further, a robust and frequent communications plan fosters a better relationship between DMS and the subscriber communities serviced by the state's investment in the MFN.

10.3.2 Engineering Review

It is critical that a comprehensive technical engineering review take place with DMS as the facilitator between the incumbent contractor and the new service provider. All technical aspects of the physical, logical, and technical definitions for the current MFN network must be documented. The new service provider's project management and engineering teams will leverage this documentation to develop the overall technical transition plan.

Careful consideration should be given to MFN customers whereby critical public services are provided to ensure no impacts and/or risks to the State's public services are mitigated. Adequate planning and production readiness testing are critical steps to ensure that no service interruptions occur.

Since an MFN transition will require changes and integration with CPE devices on the customer premises, it will be important that the transition plan developed by the selected MFN contractor include consulting and support time to aid subscribers in these tasks. While many of the MFN subscribers subscribe to the managed CPE offering, some do not. The migration of managed CPE subscribers, assuming these subscribers continue to avail of the service under the new MFN contract, will be directly supported by the new MFN service provider. The replacement of these managed CPE services will require onsite support from the MFN provider. Coordination with the incumbent MFN provider will also be required to ensure the replaced devices and assets are properly sanitized (from a state information perspective) and returned to the contractor as the current MFN provider owns them. Subscribers that do not subscribe to the managed CPE service may still require support in developing their transition plans to ensure over success of the effort.

If a multi-award contract model is leveraged with diversification of leased telecommunication services as a distinct functional area within the MFN, DMS will also play a critical role in supporting the transition planning. Under this scenario, DMS will support onboarding of vendors to a new contract category and support the winning core and backbone vendor as they manage the process of selecting last-mile vendors for each of the new MFN circuits. Once the transition efforts are completed the volume of work associated with telecommunication service procurement will reduce significantly.

10.3.3 MFN Services Transition Plan

This section provides additional details on critical aspects of the transition plan for the MFN. While the plan development will be the responsibility of the selected MFN-3 service provider, it will be important that DMS partner with the service provider to ensure a successful transition for the MFN subscribers. The selected service provider may not be aware of the existing MFN services and environment to the detailed level of DMS. It will therefore be critical that reviews of the proposed plans associated with the various aspects of the MFN services are conducted by DMS to provide these insights.

The MFN is comprised of several distinct service elements that are integrated to support end to end services to subscribers. A solution as large as the MFN cannot feasibly be transitioned as a single event. The MFN transition will be required to be performed in a phased approach around natural service boundaries. It will be important to the success of the transition efforts that the plan developed by the new service provider addresses these critical solution elements. Since the MFN is a cohesive service delivery platform, the plan will not only need to address the technical aspects of how each component service will be transitioned but will also need to address the order of operation between component transitions as they are interdependent from the perspective of the subscriber. A phased transition plan for each service is recommended to limit the potential impact to business for Florida. Where possible, a plan that permits smaller engineered groups of subscriber services to be transitioned is recommended unless effective risk mitigation strategies are employed inherently within the plan. Additional considerations for these service transitions are provided in the sections below.

10.3.3.1 Network Communications Services

The network communications services provided by the MFN are the foundational services that support all other MFN services. These services are delivered over the MFN backbone infrastructure and then extended to the MFN subscriber through leased "last mile" services. Since these communication services are the foundational element of the MFN, the transition plan associated with them will also drive the other plans as critical milestones will need to be accomplished within the network communication services transition plan before other plans can commence execution.

10.3.3.1.1 MFN Core Services

Under the current MFN contract (MFN-2) the MFN core services are delivered over vendor provided and owned infrastructure. The MFN incumbent, L3Harris, owns the equipment and is the customer of record for the backbone facilities leases, long haul fiber transport infrastructure, and last mile services that support the MFN. A change in MFN service provider (assuming a change in awarded vendor) would therefore require that a completely new MFN communications solution be established, and all subscriber services are transitioned to it.

The MFN exists to support site to site communication services between subscriber facilities and the transition plan must ensure that communication service levels are maintained between transitioned and non-transitioned sites throughout the plan execution. This will require that the new MFN backbone be established in a manner in which high speed integration between the incumbent infrastructure and the new backbone is established in sufficient capacity to support the MFN traffic volume while subscriber services are transitioned to the new infrastructure in the developed phases. The MFN-3 service provider should develop a plan that clearly articulates the timeline associated with the finalized backbone solution and includes details on when this critical interconnectivity will be established. This will require coordination with the incumbent MFN-2 contractor in both the design and execution phases.

If possible, a dynamic solution using direct routing protocol integration is recommended to allow more seamless migration efforts, avoiding the need for manual support of configurations at this integration point. DMS will ensure that the robustness of the proposed integration solution is sufficient to mitigate service disruption risks for the MFN subscribers based on the overall proposed transition

timeline. It is possible for transition activities to begin prior to the full completion of the new MFN backbone implementation, however, this may present risks to Florida which will be evaluated by DMS as the level of resiliency of the MFN-3 backbone may not be fully realized until the full build out is completed. Once a sufficient MFN-3 backbone is established and integration between MFN-3 and MFN-2 infrastructure is implemented and validated, service transitions can begin.

The MFN-2 contractor is currently the named customer of record for the current last mile leased services that are used to extend from the MFN-2 backbone to the subscriber facilities. Replacement services will need to be procured and installed for each subscriber facility under the MFN-3 contract as existing service agreements are non-transferrable.

The service provider may wish to consider leveraging the transition activities to implement MFN component design improvements through activities such as implementing mini-node and/or MAN (Metropolitan Area Network) solutions for applicable facilities. The plan developed by the service provider should outline these activities and how/when each facility will be migrated. This plan should be shared with the affected subscribers along with target timeframes as early as possible, with updates being communicated dynamically.

In addition to backbone and last mile service transition plans, the service provider should also provide details on the proposed transition plan for subscriber transit internet services. Depending on the overall methodology used for MFN-3 transition, internet services transition activities may be a prerequisite for security and remote access service transition activities and may need to occur early in the overall process.

10.3.3.1.2 Vendor-Provided CPE Services

Over 90% of the MFN-2 (91.2%) and over 70% of the FIRN-2 (71%) subscribers also leverage the managed CPE services[43] under the MFN-2 contract. The MFN-2 contractor provides the current MFN managed CPE solution. The incumbent owns the physical equipment providing CPE services at the MFN subscriber facilities. The existing equipment will be required to be replaced during transition, assuming a new service provider is selected for MFN-3. This will require site visits to perform the equipment replacement during transition. The existing physical equipment assets will be returned to the incumbent MFN-2 contractor to perform sanitization processes to ensure Florida specific configuration and data is removed.

10.3.3.2 Cloud Integration Services

The MFN-2 commercial cloud integration services are critical services for the subscribers that leverage them as the application workloads supported are often considered critical to the business operations of the subscriber. The MFN-3 transition plan should therefore include a specific section detailing how and when integration with cloud services will occur. There are potentially several cloud services leveraged by the MFN subscribers under the current MFN-2 service solution and each cloud service

-

[43] 1681 out of 3249 MFN-2 subscribers; 144 out of 206 FIRN-2 subscribers; 3112 out of 3455 total subscribers.

provider may require a specific integration method with the MFN-3 infrastructure depending on the design. Subscribers will need to be coordinated with, to support transitional activities as they control their virtual environments within the various cloud providers directly. The MFN-3 contractor should define a transition plan that effectuates close coordination with subscriber engineering teams.

The Transition Plan must provide the subscribers schedule flexibility so as not to impact regular business. The preferred approach is to make both the old and new virtual interfaces available concurrently so the subscriber can activate the new, test, and transition to, at their preferred schedule. This assumes the subscribers manage/administer their own virtual environments in the cloud services.

10.3.3.3 Security Services

The security services provided to the MFN subscribers under the MFN-2 contract are designed in an as-a-service manner where the equipment supporting them is owned and operated by the incumbent provider. A replacement solution will be required under MFN-3 as the current solution will not transition directly between contracts. Security services, specifically boundary solutions provided at the MFN-2 IAG (Internet Access Gateway) facilities, are critical to the operations of the MFN subscribers.

The MFN-3 replacement solution will need to ensure that congruent services to the current MFN-2 subscribed services are provisioned. This will include translation of all current security and address translation rulesets are ported to the new solution so that transitioning results in no impacts to subscriber services. This may require coordination with systems owners for hosted applications and other such services.

Due to the high risk in potential impacts to subscriber business practices, a phased approach to transitioning is recommended, permitting specific subscribers to be migrated as distinct entities where possible. The transition plan should also include clear fallback activities to ensure business continuity if migrations result in unexpected results. This will require coordination between the incumbent MFN-2 service provider, the new MFN-3 service provider, the affected subscribers, and DMS. The MFN-3 contractor will require existing rule sets and configuration details to properly prepare the transition plan. The MFN-3 security solution should also include DMS required DDOS mitigation as well as IDS/IPS (Intrusion Detection System/Intrusion Prevention System) services so that the packaged offering is capable of delivering the full suite of required services before migration efforts begin.

10.3.3.4 Remote Access/VPN Services

The MFN-3 transition plan will need to account for the transition of remote access and VPN services. With hybrid workforces, remote access solutions are mission critical and are considered a critical solution for subscribers. Solutions that require end point client or authentication changes will require very detailed migration plans as involvement from the subscriber Information Technology departments for desktop management and deployment services will be critical components of the processes. Due to the complexity and potential impacts to the business operations of MFN subscribers, the service provider's transition plan should include a robust plan for the migration of subscribers into the new MFN-3 platforms. Remote access solutions are typically dependent on internet services and also must be integrated into internal subscriber network communication services. In addition, depending on subscriber policy, these services may also require integration into the

security boundary services as well. There are interdependencies with respect to other services for the remote access solutions that must be accounted for in the MFN-3 transition plan.

In addition to the remote access services, VPN services such as traditional site to-site IPSec tunnels as well as "GET VPN"[44] services are also currently supported by services offerings within the MFN-2 contract. The MFN-3 will need to define a solution and transition plan to replace these existing services as the equipment supporting them on the MFN-2 is owned by the incumbent service provider and will not transition between contracts. The transition of IPSec VPN services is complicated by the requirement for coordination between multiple parties. Many IPSec solutions support business to business network communications where one entity communicates security with another, each with its own distinct administrative staff and policies. The migration of IPSec tunnels requires direct coordination among all entities.

10.3.4 Provisioning Planning

During the MFN-3 transition period, it is still likely that subscriber moves, adds, and changes will need to occur. The new service provider must work with DMS and develop a plan to address these requests or prioritize them to align with specific circuit transition schedules. It is assumed that transition will occur in a phased approach. This will result in an environment where some MFN subscriber services may be on the MFN-2 infrastructure while others have been transitioned to the MFN-3. This will require a decision tree to be put into place for service requests submitted by MFN subscribers. While all "new" non-critical service requests should be delayed until they can be supported by the MFN-3 service provider, augmentation requests may be supported during transition. This will require dynamic coordination to determine which vendor (MFN-2 / MFN-3) should be engaged to support the requests. Requests may also influence transition plans as it may be beneficial to move site migration efforts to alternative phases.

10.4 Network Operations Center

The transition of the Network Operations Center (NOC) services is one of the most critical customer-facing tasks in the plan. The Department of Management Services is to ensure that both the incumbent contractor and a new service provider maintain a steady state service availability for all aspects of the NOC service layer as prescribed in the ITN. During the transition period, NOC services will need to be provided by both the incumbent and new service providers. At a specific point in the transition plan, customer facing NOC answer points will need to be transitioned from one NOC provider to the other. Dynamic coordination will be required between the NOC services as subscriber services are migrated from MFN-2 to MFN-3. Where possible, the complexities of which services are migrated versus which are not should be abstracted from the subscriber. A solution where either NOC can distribute support requests between the service NOCs is preferred.

[44] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html

10.5 Administrative Services

The administrative functions required by the service provider will be determined by the MFN-3 ITN. The transition of customer service, account services, and billing services are critical in nature to the overall success of the MFN-3 transition plan. A full definition of the requirements for customer service, and account team interactions should be addressed in the ITN and subsequent transition plan. The billing aspects should be defined such that DMS does not incur significant rework of its billing and reconciliation processes. Where possible, production readiness testing of system integrations should be included as part of the transition planning to avoid unintended process interruptions.

This space intentionally left blank

11 Americans 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 will require that the service provider outline a method to identify and address any ADA concerns.

This space intentionally left blank

12 Contractual Provisions

This business case does not address specifics of the contractual provisions as set forth in section 5 of 287.0571, F.S., as they will be fully defined in the ITN document that is released to the vendor community. The ITN will take into consideration all other sections of the business case to aid in the development of the contextual language as appropriate.

This space intentionally left blank

13 Appendices

13.1 Appendix A – Glossary of Key Networking Concepts

Term	Definition
Physical Ring Topology	A ring topology refers to a network configuration in which each network device is connected to exactly two other devices, forming a closed loop or ring structure. Data travels along the ring in one direction, passing through each device until it reaches its destination. Key characteristics of a ring topology include: 1. **Physical Layout**: In a ring topology, network devices are typically connected in a circular or ring-like configuration. Each device, such as computers, switches, or network nodes, is connected to its adjacent devices using point-to-point links or cables. 2. **Redundancy**: Ring topologies often provide built-in redundancy, as data can travel in both directions around the ring. If one link or device fails, data can still reach its destination by taking an alternate path around the ring. 3. **Token Passing or Token Ring**: In traditional ring topologies, such as Token Ring networks, a special token or control frame is passed sequentially around the ring. Only the device holding the token is allowed to transmit data, ensuring orderly communication, and preventing data collisions. 4. **Performance**: Ring topologies can provide predictable performance, as each device has dedicated access to the network medium without contention. However, the overall performance of the network may be limited by the speed of the slowest link or device in the ring. 5. **Scalability**: Ring topologies can be less scalable than other topologies, such as star or mesh topologies, as adding new devices to the network may require interrupting the ring and reconfiguring the connections. Additionally, ring networks may suffer from degraded performance or reliability if the ring becomes too large or congested. 6. **Fiber Ring**: In modern telecommunication networks, fiber optic ring topologies are commonly used to provide high-speed, reliable connectivity between multiple locations or network nodes. Fiber optic rings offer greater bandwidth and longer transmission distances compared to traditional copper-based ring networks.
Node	A device, network element, or connection point that can send, receive, or route data.

Term	Definition
Backbone	The main central high-speed network connection that links together various smaller networks or segments within an organization or across multiple locations. The backbone serves as the primary pathway for data transmission between different network nodes, such as routers, switches, and servers. Backbones are typically implemented using high-capacity network links, such as fiber optic cables, to accommodate the heavy traffic volume and ensure efficient data transfer. They provide the necessary bandwidth and reliability to support the communication needs of the entire network infrastructure. Backbones can be hierarchical, with multiple layers of interconnected network devices, or they can be flat, consisting of a single high-speed connection. The design and implementation of the backbone network are crucial for ensuring optimal performance, scalability, and resilience of the overall network architecture.
Highly Available (HA)	A network infrastructure design with the ability to remain operational and accessible for an extended period, typically measured in terms of uptime, without experiencing significant downtime or disruptions. A high-availability network is designed to minimize or eliminate single points of failure and ensure continuous service delivery, even in the face of hardware failures, software glitches, or other issues. Key characteristics of a high-availability network include redundancy, fault tolerance, and rapid failover mechanisms. Redundancy involves deploying duplicate or backup components, such as servers, routers, switches, and network links, to ensure that if one component fails, another can seamlessly take over without interrupting service. Fault tolerance involves designing the network in such a way that it can continue to operate properly despite individual component failures.

Term	Definition
Highly Reliable (HR)	High reliability in the context of a computer network refers to the ability of the network infrastructure to consistently perform its intended functions without failures or errors over an extended period. A highly reliable network ensures that data transmission, communication, and access to network resources are consistently available and dependable, meeting the needs and expectations of users and applications. Key characteristics of a high-reliability network include: 1. **Robust Hardware and Software**: Deploying high-quality network equipment, such as routers, switches, and servers, along with reliable operating systems and network protocols, contributes to the overall reliability of the network. 2. **Redundancy**: Implementing redundant components and pathways within the network architecture helps mitigate the impact of hardware failures or network disruptions. Redundant power supplies, network links, and backup systems can provide failover capabilities to maintain uninterrupted service. 3. **Fault Tolerance**: Designing the network to tolerate and recover from faults or failures gracefully is essential for maintaining reliability. Fault-tolerant protocols, mechanisms for automatic rerouting of traffic, and redundant data storage systems contribute to the network's ability to withstand disruptions. 4. **Proactive Monitoring and Maintenance**: Regular monitoring of network performance, health, and security helps identify potential issues before they lead to downtime or service degradation. Proactive maintenance, including software updates, patches, and hardware inspections, can prevent problems and ensure the smooth operation of the network. 5. **Disaster Recovery Planning**: Developing and implementing disaster recovery plans and backup strategies is crucial for mitigating the impact of catastrophic events, such as natural disasters or cyberattacks, on network reliability. Offsite backups, data replication, and contingency plans for restoring network services are essential components of a high-reliability network.

Term	Definition
Out of Band Management Network (OOBMN)	An out-of-band (OOB) management network refers to a separate and dedicated network infrastructure used for managing and monitoring network devices, systems, and components independently of the main production network. The purpose of an out-of-band management network is to provide a secure and reliable means of accessing and controlling network devices, even when the primary network is unavailable or experiencing issues. Key characteristics of an out-of-band management network include: 1. **Separation from Production Traffic**: The OOB management network operates independently of the primary production network, ensuring that management traffic does not interfere with regular data traffic. This separation helps prevent congestion and security risks associated with mixing management and production traffic. 2. **Secure Access**: Access to the out-of-band management network is typically restricted to authorized personnel or systems using secure authentication mechanisms, such as encrypted VPN connections, SSH, or dedicated management interfaces. This helps protect sensitive management data and prevents unauthorized access to network devices. 3. **Remote Management Capabilities**: OOB management networks enable remote monitoring and administration of network devices, allowing administrators to perform tasks such as configuration, troubleshooting, firmware updates, and rebooting devices from a central location. This capability is particularly valuable for managing distributed or geographically dispersed networks. 4. **Redundancy and Resilience**: Out-of-band management networks are often designed with redundant components and failover mechanisms to ensure continuous access to network devices, even in the event of network failures or outages affecting the primary network infrastructure. 5. **Monitoring and Alerting**: OOB management networks typically include monitoring tools and alerting mechanisms to detect and notify administrators of potential issues or anomalies, such as device failures, performance degradation, or security breaches. This proactive monitoring helps administrators quickly identify and resolve problems to minimize downtime and maintain network reliability.

Term	Definition
Intrusion Detection System (IDS)	A security solution designed to detect and alert on suspicious or malicious activities occurring within a computer network or system. Unlike Intrusion Prevention Systems (IPS), which actively block or mitigate threats, IDS operates in a passive mode, primarily focused on monitoring and analyzing network traffic or system events to identify potential security breaches or unauthorized activities. Key features and functions of an Intrusion Detection System include: 1. **Traffic Monitoring**: The IDS continuously monitors network traffic or system events, analyzing packets, logs, or other data sources to detect potential security threats and anomalies. 2. **Signature-based Detection**: IDS uses predefined signatures or patterns of known attacks to identify malicious activities, such as virus signatures, intrusion patterns, or exploit attempts. 3. **Anomaly-based Detection**: In addition to signature-based detection, IDS can also analyze network behavior or system activity to detect deviations from normal patterns, which may indicate a potential security breach or unauthorized activity. 4. **Packet Inspection**: Network-based IDS inspects the contents of network packets, including headers and payload, to identify suspicious or malicious content and behavior. Host-based IDS monitors system logs, file integrity, and other system-level events for signs of compromise or unauthorized access. 5. **Alerting and Logging**: When suspicious or malicious activities are detected, the IDS generates alerts and logs detailing the nature of the threat, the affected system or network segment, and other relevant information to facilitate incident response and forensic analysis. 6. **Integration with Security Information and Event Management (SIEM) Systems**: IDS can integrate with SIEM systems to provide centralized logging, analysis, and correlation of security events across the entire network infrastructure, enabling more comprehensive threat detection and response capabilities. 7. **Forensic Analysis and Reporting**: IDS can assist in forensic analysis by providing detailed information about security incidents, including the timeline of events, affected assets, and potential impact, to support investigation and remediation efforts.
Ethernet Virtual Private Line (EvPL)	Ethernet Virtual Private Line, or EVPL, is a data service defined by the Metro Ethernet Forum (MEF) that provides point-to-point and multiple EVCs between a pair of dedicated UNIs
Internet Access Gateway (IAG)	MFN-2 term used to define the suite of hardware and software solutions that provide the secure integration between the MFN subscribers and the Public Internet.
Common Services	A suite of systems and/or application services that are leveraged by multiple consuming organizations. Services such as DNS (domain name systems) are an example of a common service

Term	Definition
Virtual Routing-and-Forwarding (VRF)	VRF stands for Virtual Routing and Forwarding. It is a technology used to create multiple instances of a routing table within a single physical router or switch. Each VRF instance operates as a separate routing domain, allowing for the segmentation of network traffic and the isolation of routing information between different virtual networks or customer sites. Key characteristics of VRF include: 1. **Isolation**: Each VRF instance maintains its own routing table, forwarding table, and routing protocols, providing logical separation of routing information between different VRFs. This allows for the creation of virtual network segments that are independent of each other. 2. **Multi-Tenancy**: VRF enables service providers to offer virtualized network services to multiple customers or tenants over a shared physical infrastructure. Each customer can have its own VRF instance, ensuring privacy and security of their network traffic. 3. **Traffic Segmentation**: VRF allows for the segmentation of network traffic based on different criteria, such as VLANs, IP addresses, or MPLS labels. This enables efficient handling of traffic between various parts of the network while maintaining logical separation. 4. **VPN Support**: VRF is commonly used in conjunction with Virtual Private Network (VPN) technologies, such as MPLS VPN or Layer 3 VPN, to provide secure communication between geographically dispersed sites or between remote users and corporate networks. 5. **Route Leaking**: VRF instances can share routing information with each other through a process called route leaking, allowing for controlled communication between different VRFs while still maintaining isolation.

Term	Definition
LATA	LATA stands for Local Access and Transport Area. A LATA is a geographic area established by the Federal Communications Commission (FCC) for the purpose of regulating and managing local telephone service provision. Key points about LATAs include: 1. **Geographic Boundaries**: Each LATA is defined by specific geographic boundaries, typically encompassing one or more local calling areas or communities. 2. **Regulatory Framework**: The establishment of LATAs was part of the breakup of the Bell System in the 1980s, as mandated by the Modified Final Judgment (MFJ). The MFJ aimed to promote competition in the telecommunications industry by dividing the Bell operating companies into separate entities and delineating areas where they could provide service. 3. **Service Areas**: Within a LATA, a single local exchange carrier (LEC) or a group of LECs typically provides local telephone services. This includes services such as local calling, access to emergency services, and directory assistance. 4. **Interconnection**: While LATAs are primarily focused on local telephone service regulation, they also play a role in the interconnection of telecommunications networks. Carriers providing long-distance or interexchange services must negotiate agreements with local carriers within each LATA to access local networks and serve customers within those areas. 5. **Competition**: Over time, regulatory changes and technological advancements have led to increased competition in telecommunications services, including local service provision. However, LATAs continue to serve as a regulatory framework for managing local telephone service within specific geographic regions.

Term	Definition
ILEC/CLEC	ILEC stands for Incumbent Local Exchange Carrier. An ILEC is a telecommunications company that was traditionally the primary provider of local telephone services in a specific geographic area, typically defined by a Local Access and Transport Area (LATA). Key points about ILECs include: 1. **Historical Role**: ILECs historically operated as monopolies or near-monopolies in their respective service areas, providing local telephone services, including local calls, access to emergency services, directory assistance, and other basic telecommunication services. 2. **Regulatory Framework**: ILECs were typically established as part of the former Bell System, which was broken up following antitrust actions in the 1980s. As a result, ILECs were subject to regulatory oversight by government agencies such as the Federal Communications Commission (FCC) to ensure fair competition and consumer protection. 3. **Infrastructure Ownership**: ILECs own and maintain the infrastructure required to provide local telephone services, including copper wire networks, fiber optic cables, central office equipment, and other telecommunications infrastructure within their service territories. 4. **Universal Service Obligation**: ILECs are often subject to a universal service obligation, which requires them to provide affordable and reliable telecommunications services to all residents and businesses within their service territories, including rural and underserved areas. 5. **Transition to Competition**: Over time, regulatory changes and technological advancements have led to increased competition in the telecommunications industry, including local service provision. ILECs now face competition from alternative providers, such **as competitive local exchange carriers (CLECs)**, cable companies, and wireless carriers, in offering voice, data, and Internet services. 6. **Continued Importance**: Despite increased competition, ILECs continue to play a significant role in the telecommunications landscape, particularly in providing essential local services and infrastructure. They also often serve as interconnection points for other carriers to access local networks.

Term	Definition
MAN	Metropolitan Area Network. A MAN is a network infrastructure that covers a geographic area larger than a local area network (LAN) but smaller than a wide area network (WAN), typically spanning a city or metropolitan area. Key characteristics of a Metropolitan Area Network include: 1. **Geographic Scope**: A MAN typically covers a geographical area that extends beyond the limits of a single building or campus but is smaller than the coverage area of a WAN. It may encompass multiple buildings, offices, or campuses within a city or metropolitan area. 2. **High-Speed Connectivity**: MANs provide high-speed connectivity and bandwidth to facilitate the efficient exchange of data and communication between various locations within the metropolitan area. This enables organizations to interconnect their local networks and share resources, applications, and services. 3. **Ownership and Management**: MANs may be owned and managed by telecommunications carriers, service providers, or private enterprises. They may also be established through collaborations between multiple organizations or public-private partnerships. 4. **Technologies**: MANs can be implemented using various technologies, including fiber optic cables, Ethernet, SONET/SDH (Synchronous Optical Networking/Synchronous Digital Hierarchy), microwave links, and wireless technologies such as WiMAX (Worldwide Interoperability for Microwave Access). 5. **Applications**: MANs support a wide range of applications and services, including Internet access, voice and data communication, video conferencing, cloud services, and access to centralized resources and data centers. They are commonly used by businesses, government agencies, educational institutions, and service providers to interconnect their distributed operations and deliver services to customers and users within the metropolitan area.

Term	Definition
VLAN	VLAN stands for Virtual Local Area Network. A VLAN is a virtual grouping of devices within a network that logically segment traffic, regardless of the physical location of the devices on the network. Key characteristics of VLANs include: 1. **Logical Segmentation**: VLANs enable network administrators to logically segment a physical network into multiple virtual networks. Devices within the same VLAN can communicate with each other as if they were connected to the same physical network, even if they are physically located in different areas or connected to different network switches. 2. **Traffic Isolation**: VLANs provide traffic isolation between different virtual networks, preventing broadcast and multicast traffic from crossing VLAN boundaries. This helps improve network performance and security by containing traffic within specific VLANs. 3. **Flexibility**: VLANs offer flexibility in network design and management, allowing administrators to group devices based on logical criteria rather than physical location. This makes it easier to organize and manage network resources, accommodate changes in network topology, and implement security policies. 4. **Broadcast Control**: By isolating broadcast domains, VLANs help reduce network congestion and minimize the impact of broadcast storms, where excessive broadcast traffic can overwhelm network devices and degrade performance. 5. **Security**: VLANs can be used to enforce security policies by restricting access to resources based on VLAN membership. Access control lists (ACLs) and other security mechanisms can be applied to VLAN interfaces to control traffic between VLANs and enforce security policies. 6. **Scalability**: VLANs scale well with growing network requirements, allowing organizations to add new devices and services without the need for extensive changes to the physical network infrastructure.

Term	Definition
VPN	VPN stands for Virtual Private Network. A VPN is a secure and encrypted connection established over a public network, typically the internet, to enable remote users or branches to securely access resources and services on a private network as if they were directly connected to it. Key characteristics of VPNs include: 1. **Secure Communication**: VPNs use encryption protocols to ensure the confidentiality and integrity of data transmitted between the remote user or branch and the private network. This protects sensitive information from interception or tampering by unauthorized parties. 2. **Remote Access**: VPNs enable remote users, such as employees working from home or traveling employees, to securely connect to their organization's internal network and access resources such as files, applications, and internal websites. 3. **Site-to-Site Connectivity**: VPNs also facilitate secure communication between geographically dispersed sites or branches of an organization by creating encrypted tunnels over the public internet. This allows branches to securely exchange data and access shared resources as if they were on the same local network. 4. **Authentication and Authorization**: VPNs typically require users to authenticate themselves using credentials such as usernames and passwords, digital certificates, or multi-factor authentication methods before they can establish a connection. Access control policies can be enforced to restrict access to authorized users and resources. 5. **Scalability and Flexibility**: VPNs are scalable and flexible, allowing organizations to accommodate changing business needs and network requirements. They can support a wide range of devices and platforms, including desktops, laptops, smartphones, tablets, and network appliances. Types of VPNs: There are several types of VPNs, including: 1. **Remote Access VPN**: Used by individual users to securely connect to a private network from remote locations. 2. **Site-to-Site VPN**: Used to establish secure communication between multiple sites or branches of an organization. 3. **Client-to-Site VPN**: Similar to remote access VPNs but tailored for specific client applications or services.

Term	Definition
Man-in-the-Middle attack	A man-in-the-middle (MITM) attack is a security exploit where an attacker intercepts and potentially alters communications between two parties without their knowledge or consent. This type of attack can occur in various telecommunication channels, including phone calls, emails, instant messages, and data transmissions over networks. Key characteristics of a man-in-the-middle attack include: 1. **Interception**: The attacker positions themselves between the communicating parties, intercepting the data transmitted between them. This interception can occur in various ways, such as by eavesdropping on wireless networks, tapping into physical communication lines, or exploiting vulnerabilities in network protocols. 2. **Unauthorized Access**: The attacker gains unauthorized access to the communication channel, allowing them to eavesdrop on the conversation or data exchange between the legitimate parties. 3. **Tampering**: In some cases, the attacker may alter the intercepted data before forwarding it to the intended recipient, potentially modifying the content of messages, injecting malicious code, or manipulating transactions. 4. **Spoofing**: The attacker may impersonate one or both of the legitimate parties involved in the communication, creating the illusion of a direct connection between them while secretly intercepting and controlling the flow of data. 5. **Stealth**: Man-in-the-middle attacks are often carried out covertly, without the knowledge or awareness of the legitimate parties involved. Stealth allows the attacker to gather sensitive information or manipulate communications without raising suspicion. 6. **Mitigation**: To mitigate man-in-the-middle attacks, cryptographic techniques such as encryption and digital signatures can be used to protect the confidentiality and integrity of communications. Additionally, secure communication protocols, strong authentication mechanisms, and regular security audits can help detect and prevent MITM attacks.

13.2 Appendix B – MFN-2 User Survey

As described in Section 3.1.5, as part of this Business Case a survey was conducted of IT professionals responsible for provisioning and supporting MFN services for end-user agencies and organizations. This survey aimed to gauge user satisfaction and gather relevant feedback for the upcoming MFN-3 contract.

Survey Questions:

Please provide your responses to the following questions. All questions require a response. Please provide as much detail and specificity as possible.

1. Are there existing business processes for MFN-2 that you feel should be reviewed to improve capabilities and service delivery for MFN-3?
2. Are there any examples of state networks in other states that you would recommend we look at for "best practice" information?
    a. Is there a general tendency known to the CIOs from other state networks for networks to be based on a) Dedicated networking, or b) use of public/commercial network infrastructure?
    b. Do these best practices involve High Availability (HA)/High Reliability (HR) service layers?
3. Today, the MFN-2 contract is a single (bundled) contract where the MFN-2 core and local loop connections is the responsibility of a prime contractor. In this type of structure, offering end-to-end SLAs is not an issue.
    a. Should MFN-3 continue with the current structure where MFN-2 is a single contract with MFN-2 core and local loop connections as the responsibility of a prime contractor? Please explain your response.
    b. Should there be an unbundled procurement strategy where the MFN-3 core is awarded to a single prime contractor and local loop connections are awarded to multiple contractors under multiple contracts? In order to provide services, these multiple contractors would connect their facilities into the MFN-3 core provider's network. Please explain your response.
    c. What are the implications for your agency from separating the local loop connections from the MFN-3 core in regards to:
4. MFN-2's current pricing model is based on flat rates statewide and month-to-month pricing structure. Should MFN-3 continue with flat rate and month-to-month pricing structure? Please explain your response.
5. MFN-2's current physical resources (e.g., core routers, firewalls, Internet gateway router, tools, etc.) are dedicated and private for the exclusive use of the State of Florida agencies.
    a. Is it a requirement from your agency's perspective that physically dedicated resources be a requirement in the MFN-3 procurement?
    b. Do you believe appropriate network reliability, functionality and security can be obtained for your agency by provisioning MFN-3 from shared use of public/commercial network resources?
    c. What network would you choose if the overall pricing for a public/commercial network is lower than a private/dedicated network? Please explain your response.
6. Under the MFN-2 Contract, any customer sites migrating from MFN-1 to MFN-2 were not charged for any special construction if local loop facilities did not exist.

   a. Should MFN-3 be established the same or differently? Please explain your response.
   b. For any new sites installed on the current MFN-2 services, customers pay any special construction costs required to implement circuits for bandwidth above 12Mpbs, if local loop facilities are not available. If this threshold for exempting special construction costs were to change in MFN-3, what threshold would best serve your organization's needs? What special use cases, if any, may increase your bandwidth needs?
7. Is there additional or different technology beyond Multi-Protocol Label Switching (MPLS) that you foresee being required to support your agency's telecommunications needs? If so, what are they?
8. Currently under MFN-2, the vendor provides a centralized next generation firewall service (state firewall) protecting the state intranet. What, if any, challenges have you experienced with this centralized firewall model? Are there solutions you envision that could solve those challenges?
9. Questions related to the VPN architecture:
   a. What enhancements would your agency like added on VPN connectivity in the MFN-3 procurement?
   b. Do you have a need for Muli-factor Authentication options on rented VPN/firewall equipment?
   c. Do you have a need for active directory integration?
10. MFN-2 provides customers with a wide range of tools (Spectrum, CA-PA, CA-NFA, Remedy, ARCSIGHT-SEIM, Splunk, etc.) to monitor the health of the network.
   a. On a scale from 0-10, how frequently does your agency use these tools? Please list a rating for each tool, with "0" being not at all and "10" being daily.
   b. Do you use any alternative tools that provide similar functionality to the tools listed above? If so, which tools do you use, and what use cases are they in use for?
11. How many MFN-2 connections do you currently have within your agency? Within these connections, what is the breakdown between sites in rural areas compared to those in urban areas?
12. If a best-effort MFN-3 service were available at a lower cost, how many sites would you anticipate moving to best-effort service?
13. How important are SLAs to your organization in terms of current MFN-2 and future MFN-3 service delivery?
14. Which metrics for SLAs are most important to your organization, and why? Aspects for SLAs include, but may not be limited to, Uptime, Mean Time to Recover (MTTR), and Performance (jitter, packet loss, latency).
15. In your agency's experience, are there SLA criteria that are currently not measured that you would find useful?
16. Would your use of MFN-3 benefit from having a reduced SLA but more cost-effective service option? If so, on what percentage of your current sites would you consider leveraging such an option?
17. Are there services missing from the MFN-2 portfolio offering that would be helpful for your organization to achieve its goals?
18. Are there any other concerns, improvements or recommendations not listed in this questionnaire that you would like to see evaluated for potential inclusion in the MFN-3 procurement?

Following is a summary of the responses to each question:

1. **Review of MFN-2 business processes for MFN-3**: Most agencies expressed a need for improvements in order status updates, budgeting methods, and portal access. Some suggested enhancements in the relationship between MFN and Telco regarding service orders.
2. **Examples of other State networks to reference for "best practice" information**: The agencies that responded to the survey did not have familiarity with any other state networks.
    A. **Dedicated networking and use of public/commercial network infrastructure:** Some respondents have concerns and needs related to encryption and redundancy that does not rely on a single point of failure.
    B. **High Availability (HA)/High Reliability (HR):** Most respondents believe high availability and high reliability are requirement, including network devices, power supplies, and circuits.
3. **Contract structure**:
    A. **Should MFN-3 unbundle last mile and core contract:** Most respondents believe that a single vendor contract with better, more enforceable SLAs for installations and last mile problem resolution would be the simplest and most effective way to deliver services.
    B. **If unbundled should local loop be multiple vendors:** Most respondents like the option of unbundling the core and last mile allowing for multiple last mile providers. The consensus is that having multiple last mile vendors would allow for competition, innovation, increased reliability, improved resiliency, reduced cost, flexibility, and mitigate risk. While some still believe that this could lead to more effort to manage and the potential for vendor finger pointing.
    C. **Implications to agency separation of local loop and core:**
        1. **Ordering and billing processing:** Concerns that would need to be addressed in a multi-award contract would include, keeping a single bill, single trouble ticketing system, potential for increased network topology complexity and the need for agencies to be more technically capable, response time on delivery and repair of services, as well as additional workload.
        2. **Performance monitoring and SLAs:** Many respondents want to ensure that network monitoring and utilization is centralized. The theme of better SLAs continues in these responses and is a focus of respondents on any new contracts. The main sentiment from the respondents is to ensure that a multi award contract would not reduce performance or increase timeframes for service delivery or interruptions of service. While a direct relationship with last mile providers would be beneficial the overall network and contract must remain centrally managed**.**
        3. **Technology availability (fiber or only copper in certain areas):** All respondents prefer fiber to copper. Many would prefer it to be mandatory for many for improved reliability, increased bandwidth, and overall service improvements. However, they had concerns about higher construction costs for fiber only circuit delivery and availability.
4. **MFN-2 pricing model**: The responses were overwhelmingly in favor of maintaining it flat rate cost model. Benefits included flexibility, ease of budgeting, compatibility with the state's appropriation cycle, and the ability to meet fiscal year budget requirements. Additionally, the

model allows agencies to project billing dollars, especially for those with multiple sites. Overall, the consensus is that the current pricing structure strikes a balance between stability and adaptability.

5. **MFN-2 current network and security hardware (routers switches etc) are dedicated to FL agencies:**
    A. **Is it a requirement that physical resources be dedicated**: The consensus from respondents was that the infrastructure should be dedicated for FL agencies siting security and stability as the main reasons to maintain dedicated infrastructure.
    B. **Do you believe the appropriate level of reliability, functionality and security can be attained via shared public/commercial infrastructure**: The respondents all believe the appropriate functionality and security can be obtained via public/commercial network resources with the appropriate configurations and encryption.
    C. **If public/commercial network is lower cost that a private/dedicated network which would you choose**: The responses varied but were all centered around flexibility, cost and security as being key drivers in making the decision between options.
6. **Special construction costs**:
    A. **Should special construction be charged for sites with existing service that transition to same bandwidth**: All respondents agreed that special construction costs should not be charged by the vendor for providing service to existing sites at current bandwidth requirements.
    B. **What bandwidth threshold should be exempt from special construction fees for new installations**: Some agencies that utilize circuits under 12Mbps for most of their sites were not concerned with increasing the limit. However most agencies considered current and future bandwidth needs to all be higher than 12Mbps and would prefer the limit to be increased to bandwidth ranging from 25Mbps to 1Gbps.
7. **Technology beyond MPLS**: Beyond MPLS agencies are interested in mainly SD-WAN and additional encryption methodologies. Also a potential need for CPE capable of NNI (ISIS over SPBM) for use with Extreme Networks Fabric connectivity.
8. **Centralized firewall model**: Respondents found little to no major issues caused by the current centralized firewall. However, most respondents would like to see additional visibility, reporting, and logging access to the firewall logs and internet traffic logs. IP6 vs IPv4 readiness and potential review of the current firewall rules to ensure they are meeting the state's needs.
9. **VPN architecture**:
    A. **Enhancements**: The responses from the agencies that currently use MFN-2 VPN services requested improvements included better logging and reporting. They would also like the ability for Layer 7 rules and the option to allow for direct VPN to resources on the internet. Cost was a concern and a reduction in cost and time to deliver would be beneficial. One suggestion also was to change pricing from a per user model to a pool of licenses being available for use by anyone when needed.
    B. **Need for MFA**: Almost all respondents said that MFA for VPN is a must have to improve security on the VPN. Although some respondents do not want it as a separate service as it should work with an existing MFA service.

C. **Active directory integration**: Most of the respondents that use the service agree that AD integration would be a benefit.

10. **Monitoring tools**:
    A. **From 0-10 how frequently does your agency use these tools:** Out of all the MFN-2 contractually provided tools the respondents use CA-NFA the most and most use it daily. Some of the other tools are used by some of the respondents but on a much more limited basis. The consensus was that access to the tools is limited and difficult.
    B. **Alternate tools used:** Various tools are used by agencies internally for several different tasks. These tools include LogicMonitor, WhatsUp Gold, Dynatrace, Secure Works, LiveNX, Splunk, and Meraki. It was noted that a 3rd party MSSP could be helpful in the analysis of the security needs of MFN-3.
11. **Number of MFN-2 connections**: Number of connections vary by size of agency. They range from as low as 5 to over 500 and the locations are a mix of rural and urban areas.
12. **Reduced SLA but more cost-effective service option**: Most respondents would not be interested in a lower cost option that is less reliable however some would consider this depending on the specific needs of certain sites.
13. **Importance of SLAs**: All respondents cited SLAs are very of critical importance to their business and lack of adherence to them adversely impacts public safety.
14. **Important SLA metrics**: Uptime, MTTR, and performance were the most important SLA metrics for most agencies.
15. **Missing SLA criteria**: Some agencies expressed a need for new circuit install SLAs and better logging facilities.
16. **Use of MFN-3 with reduced SLA**: Most agencies did not prefer a reduced SLA for a more cost-effective service option.
17. **Missing services from MFN-2**: Some agencies expressed a need for SD-WAN, Starlink and better encryption. Training and professional services as well as making redundancy and encryption standard not additional costs were mentioned.
18. **Other concerns for MFN-3 procurement**: Some agencies expressed concerns about the time-consuming transition from MFN to MFN-2 and the need for full consulting services with dedicated per agency support with timely support. Cybersecurity and NOC support were also of concern.